UNISINOS

Programa de Pós-Graduação em

Computação Aplicada

Doutorado Acadêmico

Humberto Jorge de Moura Costa

FoG-Care: A Fog Computing and Blockchain Architecture for Global Sharing of Healthcare Data

São Leopoldo, 2022

Humberto Jorge de Moura Costa

FOG-CARE: A FOG COMPUTING AND BLOCKCHAIN ARCHITECTURE FOR GLOBAL SHARING OF HEALTHCARE DATA

Dissertation presented in partial fulfillment of the requirements for the degree of Ph.D. in Applied Computing from the Graduate Program in Applied Computing at the Universidade do Vale do Rio dos Sinos — UNISINOS

Advisor:
Prof. Dr. Cristiano André da Costa

Co-advisor:
Prof. Dr. Rodolfo Stoffel Antunes

São Leopoldo
2022

C837f Costa, Humberto Jorge de Moura.
FoG-Care : a fog computing and blockchain architecture for global sharing of healthcare data / by Humberto Jorge de Moura Costa. – 2022.
135 p. : il. ; 30 cm.

Dissertation (doctorate) — Universidade do Vale do Rio dos Sinos, Graduate Program in Applied Computing, São Leopoldo, RS, 2022.
Advisor: Dr. Cristiano Andre da Costa.
Co-advisor: Dr. Rodolfo Stoffel Antunes.

1. Blockchain. 2. Cloud computing. 3. Distributed systems. 4. Fog computing. 5. Global standards 1 (GS1). 6. Health. 7. Healthcare. 8. Health informatics. 9. Data. I. Título.

UDC: 004.77:64.024.8

Cataloging in Publication (CIP):
Librarian Alessandro Dietrich - CRB 10/2338

ATA DE BANCA EXAMINADORA DE TESE DE DOUTORADO Nº 16/2022

Aluno: Humberto Jorge de Moura Costa

Título da Tese: "FOG-CARE: A FOG COMPUTING AND BLOCKCHAIN ARCHITECTURE FOR GLOBAL SHARING OF HEALTHCARE DATA."

Banca: Prof. Dr. Cristiano André da Costa - Orientador
Prof. Dr. Rodolfo Stoffel Antunes - Coorientador (UNISINOS)
Prof. Dr. Cristiano Bonato Both - Avaliador (UNISINOS)
Prof. Dr. Weverton Luis da Costa Cordeiro - Avaliador (UFRGS)
Prof. Dr. Valderi Reis Quietinho Leithardt - Avaliador (Instituto Politécnico de Portalegre)

Aos cinco dias do mês de dezembro do ano de 2022, às 09h30 reuniu-se a Comissão Examinadora de Defesa de Tese composta pelos professores: Prof. Dr. Cristiano André da Costa – Orientador (por webconferência); Prof. Dr. Rodolfo Stoffel Antunes - Coorientador (UNISINOS) (por webconferência); Prof. Dr. Cristiano Bonato Both - Avaliador (UNISINOS) (por webconferência); Prof. Dr. Weverton Luis da Costa Cordeiro - Avaliador (UFRGS) (por webconferência) e Prof. Dr. Valderi Reis Quietinho Leithardt - Avaliador (Instituto Politécnico de Portalegre) (por webconferência) para analisar e avaliar a Tese apresentada pelo(a) aluno(a) **Humberto Jorge de Moura Costa** (por webconferência).

Considerações da Banca:

O trabalho constitui uma tese de doutorado. O candidato defendeu a proposta de forma adequada, respondendo as questões realizadas pela banca. Foram feitas sugestões pelos avaliadores que devem ser consideradas na versão final do texto.

Ocorreu alteração do título? (X)Não ( ) Sim
Indicar o novo título: .....

.....

.....

A Banca Examinadora, em cumprimento ao requisito exigido para a obtenção do Título de Doutor em Computação Aplicada, julga esta tese:

(X) APROVADA ( ) REPROVADA

Conforme Artigo 75 do Regimento do Programa o texto definitivo, com aprovação do Orientador, deverá ser entregue no prazo máximo de sessenta (60) dias após a defesa. O resultado da banca é de consenso entre os avaliadores. A emissão do Diploma está condicionada a entrega da versão final da Tese. A sessão da Defesa de Tese ocorreu integralmente por webconferência para atender às recomendações da OMS e Ministério da Saúde com relação ao Covid-19.

São Leopoldo, 05 de dezembro de 2022.

Orientador - Prof. Dr. Cristiano André da Costa

I dedicate this work to all who believe in education as a way of changing life and society.

If I have seen farther than others,
it is because I stood on the shoulders of giants.
— SIR ISAAC NEWTON

ACKNOWLEDGEMENTS

I want to thank all friends, family, supervisor, co-supervisor, study colleagues, professors and PPGCA staff. Without their support, this work would not have been carried out.

ABSTRACT

Due to recent advances in distributed systems and healthcare, patient data can be dispersed in distant locations. However, processing and transmission errors are more likely to occur as data sets become larger and more complex. Several solutions based on Cloud Computing have been proposed to manage health data. These solutions present many healthcare implementation challenges, such as scalability, data privacy, and global patient identification. Thus, Fog Computing and Blockchain present themselves as an alternative to reduce the complexity of managing health data and increase its reliability. Therefore, the main challenge to be faced is how health services can benefit from a computational architecture that supports standards for the global identification of assets and sharing of geographically distributed information, considering scalability, latency, and privacy. The scientific contribution is to propose an architectural model based on Blockchain and Fog Computing that meets these requirements and eventual limitations. The methodology consists of proposing and implementing a prototype of a healthcare software architecture called Fog-Care, evaluating performance metrics such as latency, throughput, and sending rate of blockchain smart contracts in a healthcare scenario of a global vaccination campaign. This software includes a globally unique identity model called ID-Care, which supports the global identification of unique individuals with various combinations of documents, biometrics, and the GS1 healthcare industry standard. The assessment is a use-case scenario based on an integrated vaccination campaign in the top 5 most visited tourist destinations globally. The performance evaluation demonstrated that the minimum latency takes less than 1 second to run, and this metric's average grows linearly. Also, the average latency of transactions is just a few seconds; even 100 simultaneous requests per peer are considered. Thus, its data-sharing issues of privacy and identification and the use of a model for a global id for healthcare can help reduce costs, time, and efforts, especially in the context of health threats, where agility and financial support must be prioritized. From the results, It is crucial to add more fog nodes, like one per state to support the increase of demand of transactions in a blockchain with comprehensive nodes dispersed, to support scalability; as the send rate increases, approximately half of the transactions are processed at that time, according to the throughput results; privacy can be supported and treated globally with blockchain with the writing of blockchain smart contracts that represent these features; the no mutation and integrity of the ledger in a healthcare global environment can help to protect the privacy of the patients; the unique and global identification of persons and resources is necessary and can be made with GS1 Standards properly; the use of a global identification architecture for health can generate several valuable suggestions in public health policies depending on the specifics of each country and the health data shared with the participants, being possible to implement better political decision-making and a more global coordinated healthcare strategy with faster and earlier results available.

Keywords: blockchain. cloud computing. distributed systems. fog computing. gs1. health. healthcare. health informatics.

RESUMO

Devido aos recentes avanços nas áreas de sistemas distribuídos e cuidados de saúde, os dados dos pacientes podem estar dispersos em locais distantes. No entanto, é provável que ocorram erros de processamento e transmissão à medida que os conjuntos de dados se tornam maiores e mais complexos. Diversas soluções baseadas em Cloud Computing têm sido propostas para gerenciar dados de saúde. Essas soluções apresentam muitos desafios de implementação no campo de cuidados de saúde, como escalabilidade, privacidade de dados e identificação global de pacientes. Assim, tecnologias como Fog Computing e Blockchain apresentam-se como uma alternativa para reduzir a complexidade do gerenciamento de dados de saúde e aumentar sua confiabilidade. Desta forma, percebemos que o principal desafio a ser enfrentado seria como os serviços de saúde podem se beneficiar de uma arquitetura computacional que suporte padrões para identificação global de ativos e compartilhamento de informações geograficamente distribuídas considerando escalabilidade, latência e privacidade. A contribuição científica é propor um modelo de arquitetura baseado em Blockchain e Fog Computing que atenda a esses requisitos e eventuais limitações. A metodologia consiste em propor e implementar um protótipo de uma arquitetura de software de saúde chamada Fog-Care, avaliando métricas de desempenho como latência, throughput e send rate de contratos inteligentes do blockchain em um cenário proposto de uma campanha global de vacinação. Este software inclui um modelo de identidade única global chamado ID-Care, que suporta a identificação global de indivíduos únicos com várias combinações de documentos, dados biometria e a utilização do padrão global do setor de saúde chamado GS1. A avaliação é um cenário de caso de uso baseado em uma campanha de vacinação integrada nos 5 principais destinos turísticos mais visitados do mundo. A avaliação de desempenho demonstrou que a latência mínima gasta menos de 1 segundo para ser executada, e a média dessa métrica cresce em progressão linear. Questões de compartilhamento de dados, privacidade, identificação e o uso de um modelo de identificação global para saúde podem ajudar a reduzir custos, tempo e esforços, especialmente no contexto de ameaças à saúde, onde agilidade e suporte financeiro devem ser priorizados. A partir dos resultados, podemos inferir que é crucial adicionar mais nós na Fog, como um por estado, para suportar o aumento da demanda de transações em uma blockchain com nós dispersos para suportar a escalabilidade; a latência média das transações é de apenas alguns segundos, até mesmo 100 solicitações simultâneas por peer são consideradas; a medida que a taxa de envio aumenta, aproximadamente metade das transações são processadas nesse momento, de acordo com os resultados do throughput; a privacidade pode ser suportada e tratada globalmente com blockchain através da escrita de contratos inteligentes de blockchain que representam esses recursos; a ausência de mutação e integridade do ledger do blockchain em um ambiente global de saúde pode ajudar a proteger a privacidade dos pacientes; a identificação única e global de pessoas e recursos é necessária e pode ser feita com os padrões GS1 adequadamente; a utilização de uma arquitetura global de identificação para a saúde pode gerar várias sugestões úteis nas políticas públicas de saúde dependendo das especificidades de cada país e dos dados de saúde compartilhados com os participantes, sendo possível implementar melhores decisões políticas e uma estratégia de saúde coordenada com resultados mais rápidos e previamente disponíveis.

Palavras-chave: blockchain. computação na neblina. computação na nuvem. cuidados com saúde. gs1. computação na saúde. saúde. sistemas distribuídos.

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CDU	Central Decontamination Unit
COVID-19	Corona Virus Decease
CPID	Component/Part Identifier
CPU	Central Processing Unit
CSV	Comma-separated Value
ECG	Electrocardiography
EDI	Electronic Data Interchange
EHR	Electronic Health Records
EPC	Electronic Product Code
FAPERGS	Fundação de Amparo à Pesquisa do Estado do Rio Grande do Sul
FNC1	Function 1 character
GCN	Global Coupon Number
GDTI	Global Document Type Identifier
GIAI	Global Individual Asset Identifier
GINC	Global Identification Number for Consignment
GLN	Global Location Number
GMN	Global Model Number
GRAI	Global Returnable Asset Identifier
GS1	Global Standards 1
GSIN	Global Shipment Identification Number
GSRN	Global Service Relation Number
GTIN	Global Trade Item Number
HIBCC	The Health Industry Business Communication Council
IFRS	Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul
IoT	Internet of Things
PHR	Personal Health Records
QOS	Quality of Service
SSCC	Serial Shipping Container Code
TXT	Text File
UNISINOS	Universidade do Vale do Rio dos Sinos
URI	Uniform Resource Identifier
XML	Extensible Markup Language

CONTENTS

1 INTRODUCTION

Today, technology can significantly benefit healthcare. The safety and quality of health care considerably affect the use of health information technology in institutions, and hospitals (AHMADI et al., 2021). Healthcare applications usually require data-intensive computing operations (VERMA et al., 2022). Due to recent advances in the Internet of Things (IoT) and distributed computing, modern computers can quickly process a large volume of patient data. Therefore, in healthcare, this data is often dispersed in various forms, locations, and structures such as hospitals, universities, government authorities, clinical reports, medical certificates, wearable body sensors, and so on (SAHOO; MOHAPATRA; WU, 2016).

Cloud computing is an architectural model that provides convenient network access to a set of configurable computing resources that are fast for delivery and roll out with low management effort or service provider interaction (MELL; GRANCE et al., 2011). Therefore, resources such as CPU and storage are provided as general utilities that users can rent and release on demand (ZHANG; CHENG; BOUTABA, 2010). Considering the advantages of integration and the growth in cloud computing, several research projects in the health area have been carried out. In recent years, various platforms, protocols, and systems have emerged to address the challenges of cloud computing and its constraints (DARWISH et al., 2019). Despite the benefits of this technology, for many healthcare applications, a simple sensor-based cloud architecture may not be feasible (KRAEMER et al., 2017). For example, healthcare applications are considered latency sensitive. They often process vital data that is monitored by IoT devices. Also, to design this kind of real-time healthcare application, it is necessary to solve the latency drawback (MOURADIAN et al., 2017). An important issue is that conventional IoT systems still have several limitations. Some of them are related to distributed computing issues such as context awareness, reliability, communication bandwidth, accessibility (GIA et al., 2018), large-scale processing and storage (MEHMOOD; SAJJAD; BAIK, 2014), various frameworks (LV; CHIRIVELLA; GAGLIARDO, 2016), (HASHEM et al., 2015) generation and transmission errors.

One possible approach to dealing with cloud computing and analytics problems in healthcare systems is Fog Computing (BONOMI et al., 2012). In recent years, researchers have been actively working in this area. Fog is a figure of speech for computing devices interconnected between the cloud (servers) and the ground (computing devices). Fog expands the cloud computing paradigm to the edge of the network (BONOMI et al., 2014). Fog Computing presents itself as an alternative to reduce the complexity of managing health data, consequently increasing its reliability. To that end, it is crucial to understand the associated challenges, issues, and open questions.

1.1 Motivation

In a healthcare environment, due to a large number of interactions between health professionals, hospitals, and general practitioners, and considering a large number of interactions during the treatment of a patient, a delay in authentication and consequently in the use of resources and increase of costs for the medical parties involved may occur. (SWAN, 2015). Healthcare companies and related professionals say the high cost of healthcare is one of the most important issues for governments (ALAM et al., 2019).

All over the world, with the increase in healthcare expenses and the occurrence of many diseases, it has become a necessity to focus on the person-centered environment, not just the hospital (VERMA; SOOD, 2018a). Cloud-based healthcare architecture is a potential scheme to improve accessibility to correct healthcare data and reduce medical errors. It has been chosen by many medical organizations to receive, store, and manage the massive patient data from electronic health record systems (SAHOO; MOHAPATRA; WU, 2018). With this technology-based approach to healthcare, there is a possibility to be an excellent opportunity to improve the quality and efficiency of medical care, increasing patient well-being (MORAIS BARROCA FILHO; AQUINO JUNIOR, 2017).

1.2 Problem

In a healthcare environment, low latency is a desirable metric 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 (NúñEZ-GóMEZ; CAMINERO; CARRIóN, 2021), (ELMISERY; RHO; ABORIZKA, 2017). In addition, hospital policies do not allow the storage of patient data on external network environments due to elevated risks of patient data leaks (KRAEMER et al., 2017). For instance, the integrity and authenticity of the data can be enhanced with the use of blockchain technology to exchange medical records (ALHADHRAMI et al., 2017). Blockchain technology is a shared data structure related to each other in the form of a chain, responsible for storing all transactional history, and it can provide sturdiness against failures and data exposure(NAKAMOTO, 2008). The Blockchain acts as a decentralized architecture to record the data, in which a simple unit of the block is composed of a header, a transaction, and its counter (DWIVEDI et al., 2019). Therefore, by its nature, Blockchain may protect healthcare data from potential data loss, and guarantees that any record previously inserted into the chain will not be altered, helping to meet the requirements for storing healthcare records, such as the integrity and validity of patients' data (AGBO; MAHMOUD; EKLUND, 2019).

Additionally, many organizations create their service system to differentiate distinct entities in a healthcare system (GS1, 2020). The lack of standard identification of patients and assets can increase costs or cause several errors. Furthermore, as health data sets become larger and

more complex, processing and transmission issues are more likely to occur (MOURA COSTA et al., 2020a). A patient on vacation can visit several countries in the same travel, but in each location, he or she may probably have multiple health data, and different identification codes (SMITH; NACHTMANN; POHL, 2012). One possible approach is to use available standards for developing healthcare software solutions, like GS1 Standards. This international, non-profit global organization develops and implements standards to improve supply chain management in several industries, including healthcare and transportation (GS1, 2020). However, there currently needs to be an implemented official solution for the unique global identification of patients. In addition, in many healthcare monitoring systems, cloud computing servers have been used to store and process a vast amount of data collected (GIA et al., 2015).

1.3 Research Question

In the current healthcare applications, patients have their health information spread across multiple systems, hospitals, networks, and potentially countries. Many fragmented medical records of the same patient are kept in different institutions with their own snapshot of the patient's health. Several challenges need to be addressed, like the scalability of geographically dispersed traffic data. A large amount of data being exchanged between hospitals with different locations can cause delays, making data exchange unfeasible. In the healthcare environment, there are several items, such as exams, diagnoses, prescriptions, and documents, which can be shared to serve the patient better but are made unfeasible by the lack of standardization and identification. Budget constraints of governments, hospitals, and entire healthcare systems demand that the user is constantly optimized and without waste. A common problem is how to locate healthcare assets and resources globally. More recently, with the COVID-19 pandemic, mechanical and digital respirators have become extremely important. The rapid location of the healthcare system of idle respirators in hospitals in specific areas can be reallocated to those who need them most urgently. The brands, models, and functionalities can be different, and even checking if specific equipment has the necessary technical specification, important time can be lost in the care of critical patients. Another concern is the privacy of this data. As many health professionals will access electronic health records, and this data may be shared, there are possibilities of data leakage (concerns about privacy and integrity) and possible rework.

Based on the gaps identified in the state-of-the-art, we propose the following research question:

How can healthcare services benefit from a computer architecture that supports standards for the global identification of assets and sharing of geographically distributed information considering scalability, unique identity, and privacy?

1.4 Contributions

The main contribution of this work is to propose a solution that integrates a distributed health system architecture within Fog Computing and Blockchain in a way that considers the challenges of dealing with scalability, privacy, and a unique global identity of assets. This proposal is based on the results of a systematic literature review that highlights the need for low latency access, scalability, respect for data privacy and integrity, and the ability to identify and share data on a large scale. Blockchain can be essential in supporting privacy. The GS1 technology for use in the globally unique identification of assets, patients, and healthcare professionals addresses the integration of a globally scalable architecture using a well-known data standard.

We also define a fog computing architecture using Blockchain that considers the specifics of healthcare and the uniqueness of assets and discovers the challenges and open questions involved, contributing to the computing area. In addition, it comprises the following secondary contributions:

Scientific Contributions:

- Produce a systematic review of the literature on Fog Computing and healthcare;
- Propose a taxonomy to represent the main discoveries and challenges in the area of fog computing applied to healthcare;
- Evaluate and validate the performance of the proposed architecture;
- Apply the proposed architecture in a global healthcare environment case study.

Technical contributions:

- Develop a prototype for the proposed fog computing architecture, including global asset identification and use of Blockchain, considering scalability, privacy, and latency requirements.
- Develop a mobile client application to support the proposed architecture;

1.5 Study Organization

This proposal dissertation is divided into seven chapters. The remaining of this proposal is organized as follows. In the second chapter, background, we describe the main concepts of fog computing blockchain and GS1 standards. In the third chapter, Related Work, we research the articles regarding Fog Computing and healthcare. In the fourth chapter, FoG-Care Model, We present the model, taxonomy, and architecture proposed. The fifth chapter is the Materials and Methods, which describes the method, evaluation, and case study of this work. The results and discussion are shown in the sixth chapter, Results and Discussion. In chapter Conclusion, we present the conclusion and future directions.

2 BACKGROUND

This chapter describes the technologies of Cloud Computing, Fog Computing, Blockchain, and Identification Standards in healthcare. These technologies made up the architecture proposed in this dissertation. They were chosen based on the proposed value to contribute to the objectives of this work and were obtained from a literature review related to technologies applied in the healthcare area.

2.1 Cloud Computing in Healthcare

Cloud computing can provide ubiquitously, on-demand, and convenient network access to computing resources (such as servers, storage, networks, applications, and services), which can be shared and provisioned quickly, with minimal interaction effort or service provider management (MELL; GRANCE et al., 2011). These platforms possess characteristics of both clusters and Grids, with particular attributes and capabilities, such as strong support for virtualization and dynamically composable services with web service interfaces. As a result, such environments enable the creation of third-party, value-added systems by leveraging compute, storage, and application services while abstracting the required hosting infrastructure (BUYYA et al., 2009).

In many healthcare monitoring systems, remote cloud servers have been used to store and process a vast amount of data collected from sensor nodes (GIA et al., 2015). However, there are many challenges regarding access latency, location definition, and large data transmissions. There is an increased probability that a single error in the data analyzed may lead to imprecise treatment decisions and crucially affect the life of a human being (GIA et al., 2015).

In the cloud environment, cloud providers support different infrastructures and architectural designs to improve the quality of their services. The heterogeneity of hardware and architecture between mobile devices and cloud servers makes it challenging to deploy cloud resources and services on mobile devices directly and leads to several problems, as detailed below (SANAEI et al., 2013).

- Unbalanced quality and performance: the variation in computing resources and their implementations diversifies the performance and quality of cloud services.

- Data integrity and management: the increase in the number of data warehouses distributed geographically on a large scale and the lack of similarity of data structures makes data management difficult.

- The integration of large distributed data and the provision of virtually unified storage for mobile users is becoming more difficult with the increasing heterogeneity (SAKR et al., 2011).

- Interoperation: Data interoperation is the ability to connect heterogeneous systems (wired or wireless), understand geographic information resources, and exchange data between/across two or more heterogeneous systems (BLAIR et al., 2011). The absence of uniform interface standards and platforms has created problems in data integration and interoperation due to the differences between cloud and mobile infrastructures, such as the existence of cables connected to wireless network hardware systems.

  These problems must be managed to avoid impacting the needs of healthcare computer software, as demonstrated in the next section.

2.2 Fog Computing in Healthcare

For many healthcare applications, a simplified cloud architecture may not be feasible. In some cases, hospital policies do not allow patient data storage on external network environments due to elevated risks of patient data leaks (KRAEMER et al., 2017). One possible approach to addressing the gap between sensors and analytics in healthcare applications is fog computing. NIST defines Fog Computing as a layered model for enabling ubiquitous access to a shared continuum of scalable computing resources (IORGA et al., 2018). The original concept of fog computing was coined by industry (BONOMI et al., 2012) as a metaphor for the idea that Fog is a location between the cloud (data centers) and the ground, where devices belonging to users are located.

Mokhtari defines Fog Computing as a technology that provides a scalable solution for cloud computing, which provides storage and computation close to the end (MOKHTARI; ANVARI-MOGHADDAM; ZHANG, 2019). The application of Fog computing principles can benefit a large number of computing tasks in healthcare (KRAEMER et al., 2017). For instance, there is an increased probability of processing and transmission errors as health datasets become larger and more complex, and this may lead to inaccurate treatment decisions (GIA et al., 2015).

Since Fog can provide storage and computing services closer to the end devices, it can aggregate, process, and store a massive amount of information, enabling real-time analysis. Since medical sensors generate data frequently, 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 (ANDRIOPOULOU; DAGIUKLAS; ORPHANOUDAKIS, 2017).

In other words, it is a scenario where a large number of ubiquitous (wireless and sometimes standalone) heterogeneous and decentralized devices communicate and potentially cooperate. The network performs storage and processing tasks without the intervention of a third party. Fog computing provides storage and computation closer to the end devices, being a scalable solution for cloud computing (MOKHTARI; ANVARI-MOGHADDAM; ZHANG, 2019). These tasks may be to support essential network functions or new services and applications that run in a sandbox environment. Users who make part of their devices available to host these services

receive incentives to do so (VAQUERO; RODERO-MERINO, 2014).

More recently, Iorga et al. (IORGA et al., 2018) defined Fog Computing as a layered model to allow ubiquitous access to a shared continuum of scalable computing resources. This idea facilitates the deployment of latency-aware distributed systems and services, and it is based on physical or virtual fog nodes located between smart devices and centralized services.

Conventional IoT systems still have several limitations in terms of latency, reliability, communication bandwidth, and accessibility (GIA et al., 2018). Healthcare applications are also latency-sensitive. They process vital data (e.g., heart rate and glucose level) that are monitored by IoT devices (e.g., Body Area Network). Moreover, they send real-time notifications (e.g., heart attack alerts to family members). Consequently, researchers increasingly rely on the Fog when designing such applications to address the latency drawback characteristics of the cloud (MOURADIAN et al., 2017). The technology-based approach to healthcare is an unprecedented opportunity to improve the quality and efficiency of medical treatment and consequently improve patient wellness, as well as be a better application of government financial resources (MORAIS BARROCA FILHO; AQUINO JUNIOR, 2017). For instance, since Fog can provide storage and computing functionality closer to the end devices, it can aggregate, process, and store a vast amount of information, enabling real-time analysis. Because medical sensors generate high-frequency data, the real-time analysis performance can be improved, providing intelligent data analysis and decision-making according to local policies and the network resources available to the end users (ANDRIOPOULOU; DAGIUKLAS; ORPHANOUDAKIS, 2017).

Many technological challenges must be overcome in healthcare. 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 (MELL; GRANCE et al., 2011). Solutions based on Cloud Computing, for instance, are widely proposed to manage healthcare data. However, such solutions need to address issues such as network latency, support different kinds of internet connections and simultaneously deal with large volumes of data (MOURADIAN et al., 2017). Furthermore, the patient data sometimes must be processed in real-time, contributing to an increased probability of processing and transmission errors as health datasets become larger and more complex (GIA et al., 2018).

In this context, Fog Computing presents itself as an alternative to reduce health data management complexity, consequently increasing its reliability (KRAEMER et al., 2017). Fog Computing is a technology that provides a scalable solution for cloud computing, which provides storage and computation close to the end (MOKHTARI; ANVARI-MOGHADDAM; ZHANG, 2019). In other words, it can enable ubiquitous access to a shared continuum of scalable computing resources (IORGA et al., 2018).

Since Fog can provide storage and computing services closer to the end devices, it can aggregate, process, and store a massive amount of information, enabling real-time analysis. Since

medical sensors generate data frequently, 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 (ANDRIOPOULOU; DAGIUKLAS; ORPHANOUDAKIS, 2017). Fog computing is a trend in the cloud computing environment. Increasingly, applications are cloud intensive. While hardware has dramatically increased its capacity, healthcare applications need the information to be obtained as quickly as possible. Fog computing can help substantially with this. It can reduce the latency of these applications, enabling medical services in real-time and in a massive way, with the possibility of positively impacting the poorest population, which still does not have access to quality healthcare worldwide. Based on Dastjerdi et al. (DASTJERDI et al., 2016), the key features of the Fog Computing paradigm are:

- Low latency - due to the close location of fog nodes to on-premise physical devices, allowing for a much quicker response time and data analysis.
- Rich and heterogeneous support for the end user – due to the edge devices' proximity to computing nodes.
- Multi-tenancy - due to highly virtualized distributed platforms.
- Support of mobility - due to immediate communication between fog applications and mobile devices.
- Real-time interaction - various fog applications involve real-time processing rather than batch processing.
- Context awareness - due to devices and having information and knowledge of their environment.
- Wide geographical distribution - due to the largely distributed deployment, Fog Computing can provide high-quality streaming services.
- Seamless interoperability and improved federation - for better communication among devices from different providers and domains.
- Support analytics in real-time - due to ingesting and processing data close to end devices.
- Heterogeneity support - due to different forms of fog nodes and their deployment.
- Support for many industrial applications - due to real-time processing and analysis.

The use of Fog Computing in this work is related to scalability support, a relevant requirement discovered in the current scientific literature. The possibility of transmission errors and the likelihood of data processing delay remains an issue as healthcare datasets become more complex and larger, and support for healthcare applications in integrated sharing and global data distribution increases. (AWOTUNDE; BHOI; BARSOCCHI, 2021).

2.3 Blockchain in Healthcare

Another technology that has been widely proposed to address privacy issues in healthcare is Blockchain. With this technology, it is possible to ensure the integrity and traceability of shared data while supporting privacy in a decentralized environment commonly found in healthcare.

The Blockchain consists of a Peer-to-peer (P2P) distributed ledger database for transactions without the necessity of a central authority or a third-party verification (CONOSCENTI; VETRO; DE MARTIN, 2016). The key benefits included in blockchain technology applied to healthcare can be decentralized management, immutable audit trail, data provenance, robustness and availability, and improved security and privacy. Blockchain can also improve medical record management, enhance the insurance claim process, accelerate clinical/biomedical research, and advance biomedical / healthcare data ledge (REJEB; BELL, 2019).

A Blockchain is formed by sets of chained blocks and every block includes a hash of the previous block. The genesis block is considered the first block in a Blockchain, and it is hard-coded into the software and is the only one that does not refer to a previous block. This technology is also considered a peer-to-peer (P2P) distributed ledger technology for a new generation of transactional applications that establishes transparency and trust. The main concepts associated with Blockchain are (TASATANATTAKOOL; TECHAPANUPREEDA, 2018):

- **Decentralization:** The blockchain stores data across the network.
- **Transparency:** Everyone in the node can view the ledger that shares the amount decentralized network.
- **Miner:** Transaction verification
- **Consensus:** A v method is used to verify the transaction.
- **Forks:** The problem that arises when the node is used for a different version of Blockchain
- **Hash:** One-way hash function to check the integrity of a transaction or message.
- **Node:** The ledger in the Blockchain system.
- **Timestamp:** A date and time in the computer system used as an electronic time stamp for the transaction.

The Blockchain forms the underlying fabric for cryptocurrencies such as Bitcoin and is a design pattern consisting of three main components: a distributed network, a shared ledger, and digital transactions.

The main blockchain characteristics include:

- Distributed Network Blockchain is a decentralized P2P architecture with nodes consisting of network participants. Each member in the network stores an identical copy of the Blockchain and contributes to the collective process of validating and certifying digital transactions for the network.

- Shared Ledger Members in the distributed network record digital transactions into a shared ledger. To add transactions, members in the network run algorithms to evaluate and verify the proposed transaction. If a majority of the members in the network agree that the transaction is valid, the new transaction is added to the shared ledger. Changes to the shared ledger are reflected in all copies of the Blockchain in minutes or some cases, seconds. After a transaction is added edit is immutable and cannot be changed or removed. Since all members in the network have a complete copy of the Blockchain, no single member has the power to tamper or alter data.

Different types of data are being captured and stored in health centers. In healthcare, a common approach due to security and integration properties is using Blockchain decentralized technology to support sharing data such as Electronic Health Records (EHR), Personal Health Records (PHR), or other health data. Throughout a person's medical history, Electronic Health Records (EHR) provide a medical representation of that person to document certain information regarding some aspect of the patient's health status. As an extension of EHR (ROEHRS et al., 2019), the PHR is the representation of some information regarding health, such as wellness, development, and welfare which standalone or integrates health information from multiple sources and for which the individual, or their authorized representative, manages and controls the PHR content and grants permissions for access by or sharing with other parties (ISO, 2017). These standard technologies are most of the time used to view the complete health history of a given patient. However, they are generally maintained centrally by healthcare organizations, making integration between healthcare institutions more difficult. (QUAINI et al., 2018).

2.4 Identification Standards in Healthcare

Many healthcare organizations develop their own naming/service system to differentiate distinct entities within a healthcare system (GS1 HEALTHCARE, 2022). The lack of standard location identification leads to increased costs by causing product delivery errors and complicating the rebate process (TEMPLETON, 2010). One example is the problem where a single location may have multiple names and different identification codes (SMITH; NACHTMANN; POHL, 2012). To deal with these concerns, GS1 Global, an organization formed by a global community of volunteer users, such as stakeholders in the health supply chain, including manufacturers, distributors, hospitals, solution providers, and 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 (GS1, 2020). The advantages of these standards can be Ease of Use and Usefulness, Product Identification, Accurate and Reliable Tracking, Information Accuracy, and Information Availability (KRITCHANCHAI; HOEUR; ENGELSETH, 2018).

The complex nature of healthcare supply chains has intensified the need to share accurate and timely information about products and locations. The information disconnect and the rising costs of products in the healthcare supply chains call for employing effective supply chain management practices.

The reality is that managing inventory is a difficult task for hospitals, instrument manufacturers, and distributors alike. It is a cumbersome, resource-intensive process that is complicated by the fact that an instrument tray's visibility is critical to patient safety and the efficiency of a CDU. Patient safety benefits: (JAYARAMAN et al., 2011)

- Robust traceability of instrument sets with audit trails for quality assurance are electronically accessible;
- Instrument sets can be located quickly in emergencies;
- Warnings are provided if a step is skipped in the decontamination process;
- Links between patients, instrument sets, and the decontamination process are established Efficiency benefits:
- Ability to analyze staff productivity to improve;
- Ease of reporting both during and post-event;
- Automated validation and streamlined processes;
- Inventory visibility available in real-time;
- Automatic generation of setlists when the GS1 code is scanned, reducing administrative work;
- Improved communication between CDU and staff, ensuring sets are ready where and when needed;

In GS1 Standard, the Global Trade Item Number (GTIN) is used to identify trade items worldwide uniquely. A trade item is any item (product or service) upon which there is a need to retrieve predefined information that may be priced, ordered, or invoiced at any point in any supply chain. This includes individual items and all their different configurations in different types of packaging.

In the GS1 Standard, the Global Trade Item Number (GTIN) uniquely identifies trade items worldwide. It is any item (product or service) that is necessary to retrieve predefined information

that can be priced, ordered, or invoiced at any point in any supply chain. This includes individual items, as well as all their different configurations in different packaging types. Safer surgery saves lives: GS1 identification and bar code standards deployed in the Irish Health Service Executive's (HSE) Central Decontamination Units (CDUs)

Mandatory identifiers

- All GS1 standards will incorporate GS1 identification standards as mandatory identifiers exclusive of all other mandatory identifiers.
- Non-GS1 identifiers Non-GS1 identifiers may only be used with GS1 standards as additional identifiers (not alternates). Implementations using non-GS1 identifiers as primary identifiers are not compliant with GS1 standards.
- GS1 Company Prefix The GS1 Company Prefix is used exclusively within GS1 identification standards that may be expressed in GS1-approved barcode applications, in GS1 EDI messages, for global data synchronization, network registration, and in EPC Tags within the header values reserved for the GS1 system.
- Carrier independence GS1 identification keys are defined and utilized per GS1 definitions independent of the data carrier (e.g., barcode, radio frequency identification (RFID), business message).
- GS1 business messages GS1 business messages or GS1 standards-based applications use GS1 identification keys for identification exclusive of GS1 data carrier features. Examples of data carrier features include the use of:
- Modulo 103 GS1-128 symbol check character to secure data capture.
- Function 1 Symbol Character (FNC1) in the second position of GS1-128 barcode or an Electronic Product Code (EPC) header value to discriminate between GS1 data content and data carrier overhead.
- Separator characters or EPC parsing values to parse a decoded data string into significant data parts.

The GS1 identification standards can be visualized in Table 1.

The above technologies were selected for this work based on several challenges discovered in the literature review. Cloud Computing and Fog Computing are considered good strategic choices to deal with the vast amount of data generated by healthcare patients and can provide real-time solutions with low latency and better reliability. EHRs and PHRs are almost stored on centralized databases in which medical data remains largely non-portable. The centralization of this approach may increase the security risk and require that the parties trust a single authority in the case of sharing data. EHR / PHR carries many challenges, such as completeness, accuracy, complexity, and bias (HRIPCSAK; ALBERS, 2013). Furthermore, centralized

Table 1 – GS1 Identification Standards.

ID Key	Used to Identify	Example
Global Trade Item Number (GTIN)	Products and services	Can of soup, chocolate bar, music album
Global Location Number (GLN)	Parties and locations	Companies, warehouses, factories, stores
Serial Shipping Container Code (SSCC)	Logistics units	Unit loads on pallets, roll cages, parcels
Global Returnable Asset Identifier (GRAI)	Returnable assets	Pallet cases, crates, totes
Global Individual Asset Identifier (GIAI)	Assets	Medical, manufacturing, transport, and IT equipment
Global Service Relation Number (GSRN)	Service provider and recipient relationships	Loyalty scheme members, doctors at a hospital, library members
Global Document Type Identifier (GDTI)	Documents	Tax demands, shipment forms, driving licences
Global Identification Number for Consignment (GINC)	Consignments	Logistics units transported together in an ocean container
Global Shipment Identification Number (GSIN)	Shipments	Logistics and units delivered to a customer together
Global Coupon Number (GCN)	Coupons	Digital coupons
Component/Part Identifier (CPID)	Components and parts	Automobile parts
Global Model Number (GMN)	product model	Medical devices

GS1 General Specification (STANDARDS, 2022).

databases cannot ensure security and data integrity, regardless of identification and controlled access requirements. By the force of law, centralized health databases are legally a requirement and necessity in most countries worldwide. Therefore, they require an added technology layer to improve their portability and security, so Blockchain technology is considered a solution. Finally, several healthcare data standards exist, but integration takes time to implement. They were considering implementing GS1 Standards because the large organizations' support provides interoperability that can be implemented with open and internationally recognized standards. Thus, patients often move between health institutions to avoid repeated and missing patient data. Their database may contain only part of their data, resulting in a complex problem of sharing and fragmentation of the data. One of the objectives of this work is to contribute solutions that consider the complexities, needs, and limitations of the healthcare area in applied computing in an integrated way.

3 RELATED WORK

We made a systematic literature review regarding Distributed Computing technologies applied to healthcare, Blockchain technologies applied to healthcare, and global identification technologies applied to healthcare. It was considered as a basis for the development of the proposed objectives and the implementation of possible solutions. Based on this work, an article was published in the Journal of Health and Technology under the name of Fog computing in health: A systematic literature review (MOURA COSTA et al., 2020a).

3.1 Related Work on Distributed Computing Applied to Healthcare

3.1.1 Selected Articles

This work presents a systematic literature review designed to provide a research overview of Fog Computing being applied to the health area. We propose to verify and quantify research evidence on these topics (BUDGEN; BRERETON, 2006). We used this literature review approach because our goal is to summarize the technology regarding fog computing being applied to health and identify promising directions, which does not require an in-depth analysis and synthesis. Moreover, to increase the reproducibility of our results, we follow the well-documented study protocol proposed by Biolchini et al. (BIOLCHINI et al., 2005).

The method that we did the systematic literature review was based on the original work of Kitchenham (KITCHENHAM, 2004), which defines the following activities:

1. **Research questions:** introduces the research questions investigated;
2. **Search strategy:** outline the strategy and libraries explored to collect data;
3. **Article selection:** explain the criteria for selecting the studies;
4. **Distribution of studies:** present the chronological distribution of the studies;
5. **Quality assessment:** describe the quality assessment of the selected studies;
6. **Data extraction:** compare the selected studies and research questions.

The following sections describe how we performed this process.

3.1.2 Research Questions

One of the essential processes of any systematic review is the selection of research questions (KITCHENHAM, 2007) (PETTICREW M, 2006).

Table 2 – Research questions proposed.

Id	Issue
GRQ01	How would the **taxonomy classification** relative to the intersection of fog and health area should be?
GRQ02	What are the **main challenges and open questions** relative to the intersection of fog computing and health area?
SRQ01	What are the **main types of applications or services** relative to the intersection of fog and health area?
SRQ02	What technologies are commonly used in **device layer** relative to the intersection of fog and health?
SRQ03	What technologies are commonly used in **fog layer** relative to the intersection of fog and health?
SRQ04	What technologies are commonly used in **cloud layer** relative to the intersection of fog and health?

In this way, we map and classify the technologies related to Fog Computing and healthcare, such as the characteristics, challenges, issues, and solutions that are today considered and the existence of possible research opportunities.

We separate the questions into general research questions (GRQ) and specific research questions (SRQ). The goal of general research questions is to address broader concerns about fog computing applied in the healthcare field of study. In turn, the specific research questions explore particular challenges, focusing on the architecture of Fog Computing technologies applied to healthcare.

Therefore, we formulate two general research questions, one focused on a taxonomy for Fog computing applied to healthcare and the other dealing with respective research challenges. Also, we created four specific research questions. The first concerns applications and services, and the remaining three regard technologies used in fog, cloud, and client layers, respectively. Table 2 describes all the research questions studied.

3.1.3 Search Strategy

The main objective of the search strategy was to find relevant works regarding Fog Computing and Health Care. We defined the search scope and keywords according to the work of (KITCHENHAM, 2004). This way, we selected all the words related to the research topic for more accurate results. We also applied the PICOC (population, intervention, comparison, outcome, and context) method from Petticrew (PETTICREW M, 2006) as a guideline to define the strategy.

The search strategy consisted of constructing keywords for querying related works in fog computing and health care. The variants and synonyms, such as “healthcare” and “health” were also considered as keywords. Following, we present the resulting search string used to select

articles.

(“fog computing”) and (“health” or “healthcare”)

We used the following terms to better filter studies in line with our focus: “health”, “fog computing” and “healthcare”. We analyzed the context of fog and healthcare information coverage in terms of standardization, information grouping, security, and Privacy. The data were obtained from electronic databases by applying the created keywords in the search scope phase.

3.1.4 Article Selection

To select the articles, we removed all those that were not relevant to fog computing and healthcare topics. Thus, we removed articles that did not report the fog explicitly. To use the exclusion criteria, we use the population terms and intervention criteria as follows:

- **Exclusion criterion 1:** article does not address “fog” or related acronyms (population criterion I).

- **Exclusion criterion 2:** article does not address “health” or “healthcare” or related acronyms (intervention criterion II).

The steps of the filtering process are as follows:

1. impurity removal;

2. filter the title and abstract;

3. removal of duplicates;

4. filter the entire text content;

5. article must have a minimum of 6 pages.

First, we have removed the impurities of the search results. These include, for example, conference abstracts correlated to the search keywords, academic thesis or dissertation, books, or articles not related to fog and healthcare research fields.

Second, we excluded articles in the title and abstract that did not mention the fog Computing and healthcare terms. Third, we have grouped the remaining articles and removed the duplicates. Fourth, we carefully read the articles looking for architectures related to computing and healthcare. Those articles deemed not relevant to our focus were removed from the corpus. Finally, we only kept six pages or more articles.

3.1.5 Quality Assessment

This criterion was proposed to verify that the article is a relevant study necessary to evaluate the quality of the selected works (KITCHENHAM, 2004). We assessed the selected articles considering the research purpose, contextualization, literature review, related work, methodology, outcome, and conclusion according to objectives and indication of future studies. We present the quality assessment in Table 3.

Table 3 – Quality criteria used to analyze the articles.

Criteria	Description
CR01	Purpose of the research is clear.
CR02	Related work is presented with the main contribution.
CR03	Have an architecture proposal
CR04	Have research results.
CR05	conclusion are linked to the research objectives.
CR06	Future work, improvements, or further studies are recommended.
CR07	Literature review or background are described effectively.

3.1.6 Data Extraction

In order to get information about the studies and the sections where we found answers to general and specific research questions, an evaluation form for the selected articles was developed, as shown in Table 4.

Table 4 – Article sections related to proposed research questions.

Section	Description	Research Question
Title	Title of specific article	GRQ01, GRQ02
Abstract	Summary of paper	GRQ01, GRQ02
Keywords	Words of the text content	All research questions
Introduction	Issue to be addressed	All research questions
Background	Concepts and is related to the proposal	All research questions
Methods	The scientific methodology	All research questions
Results	Evaluation outcome	All research questions
Discussion	Data quantified compared with the literature	GRQ02, SRQ01-SRQ04
Conclusion	Findings related to objectives and hypotheses	GRQ02, SRQ01-SRQ04

3.1.7 Recruitment

We present the outcomes correlated with the research topic from the 44 articles studied. We try to answer each research question proposed in the following subsections through the

synthesis of information elaborated. As an outcome, we have also proposed a new taxonomy, a renovated overview of the key challenges and issues, and an updated survey on data types, patterns, user types, profiles, and entry techniques for the Fog Computing and healthcare field of study.

3.1.8 Conducting the Search Strategy

We have selected the following electronic databases as our research scope: Google Scholar, ACM, IEEE, Science Direct, Elsevier, and Springer. These online databases cover the most significant journals and conferences within the computer science and healthcare area. We employed Manual filtering to eliminate duplicate results from different databases in the study selection. To limit our search, we have set the search range from 2008 to 2018.

3.1.9 Proceeding With Article Selection

Figure 1 describes the selection process, demonstrating how the filtering process works. We found 1070 papers in the preliminary search before using the exclusion criteria; of these, 843 (78.79%) papers were considered impurities. After applying a filter by title and abstract, 115 (10.75%) was irrelevant. Therefore, 8 (0.75%) articles were considered duplicates and very similar. Next, exclusion criterion 2 was used for the text content and excluded 24 (2.24%) articles. Finally, all 36 (3.36) articles with six pages or less were dropped. Therefore, the final selection was 44 articles (4.11%). Table 20 (Appendix A) describes the final corpus of articles. Additionally, in Figure 2, we provide a list of articles per year grouped by their respective publishers.

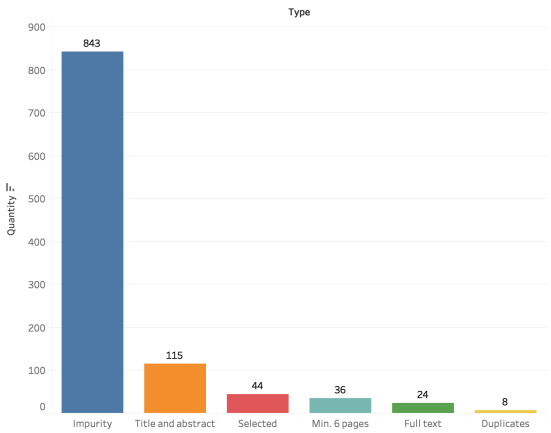

Figure 1 – Number of articles removed by the filter.

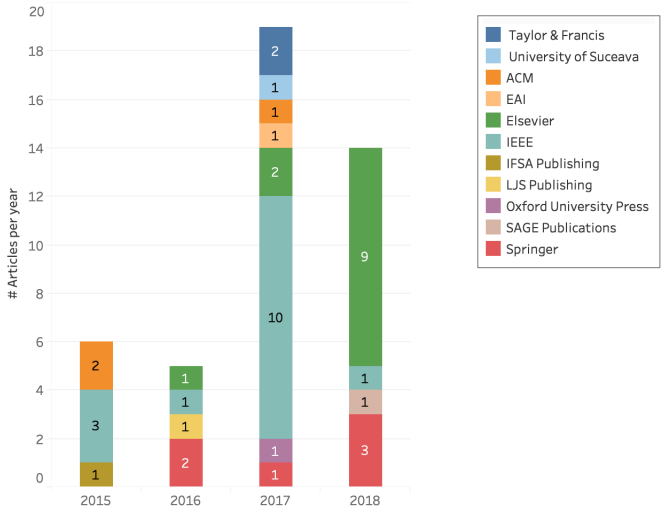

Figure 2 – Number of articles per year grouped by publishers.

3.1.10 Data Extraction and Answers to the Research Questions

Now, we answer, in this section, the proposed research questions. General Research Questions (GRQ) and Specific Research Questions (SRQ) are addressed.

GRQ1: How should the taxonomy classification be relative to the intersection of fog and health area?

We have investigated several recent questions in Fog Computing and healthcare. Therefore, we have been able to develop a taxonomy to gather and organize the various possibilities of architectures to be used. The proposed taxonomy is described in Figure 3.

These groups have been inspired by the article "The NIST definition of fog computing" (IORGA et al., 2018).

GRQ2: What are the main challenges and open questions relative to the intersection of Fog Computing and the healthcare area?

We have made a study of the main challenges, open questions, aspects, and common concerns related to the use of fog Computing intersecting with health areas. We present the results in Table 21 (Appendix B). Enumerating these challenges is fundamental to being aware of the research topics currently widely studied by the academic community. The selected challenges are Data Management, Scalability, Interoperability, Security, and Privacy, as we can visualize in Figure 4 and describe textually below.

Data management means how the cloud integrates data from multiple sources, captures the data from many fog nodes, and stores the data safely and securely. Scalability is the ability of a network, system, or process to deal with an increasing amount of work or its potential to be increased to adapt to that growth(BONDI, 2000). Interoperability is typically considered as the ability to quickly move workloads and data from one cloud provider to another or between private and public clouds (LEWIS, 2013). Security and Privacy are always considered in the

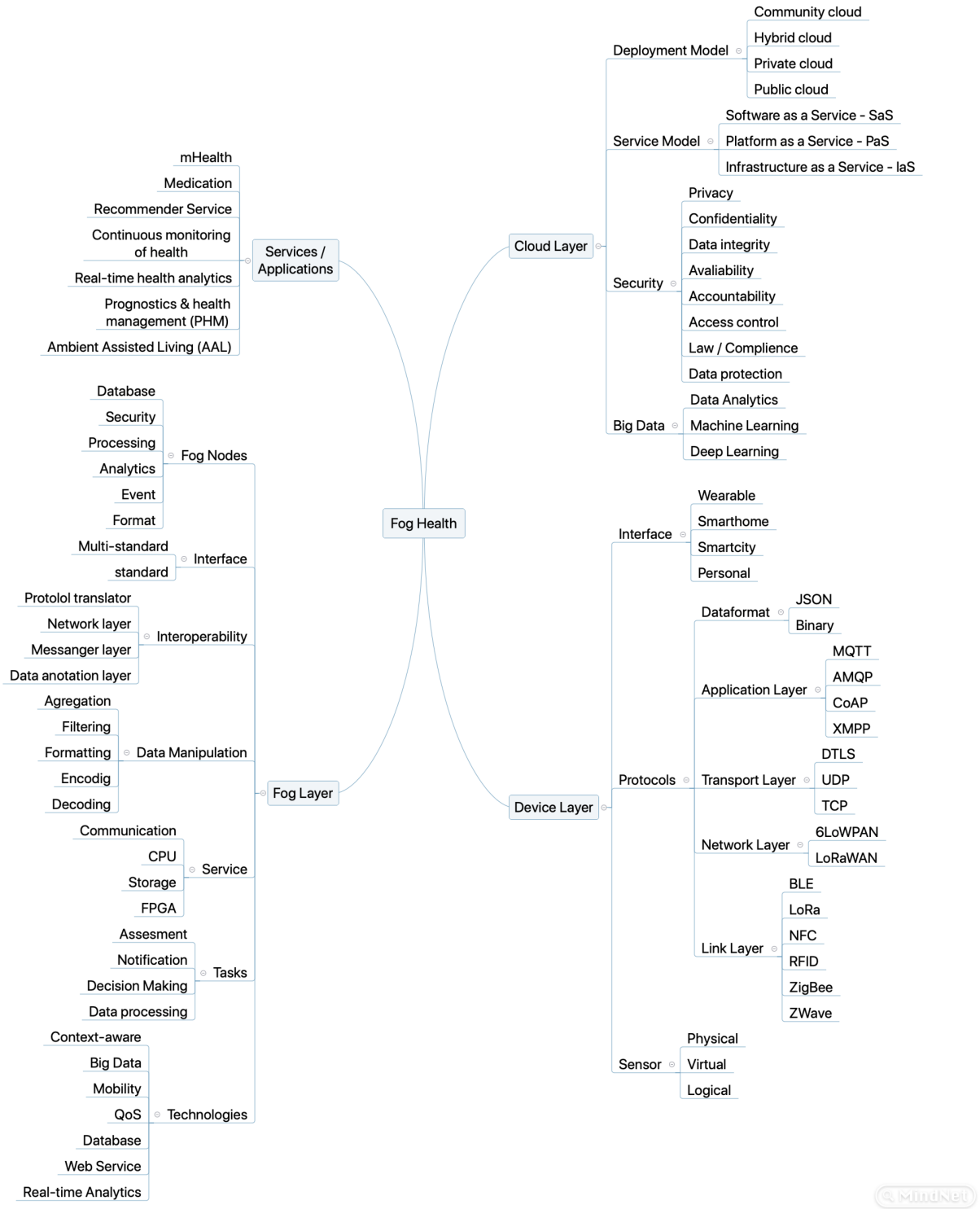

Figure 3 – Proposed taxonomy.

context of computing and information security in this work.

For question GQ2, we tried to find out the main challenges and questions of using Fog computing applied to the healthcare area. The overviewed challenges found in most articles are related to the question of security (40 articles) and Privacy (26 articles). Thus, interoperability of the system was the next big challenge, followed by the problem of scalability (19 articles) and data management (111 articles).

SRQ1: What are the main types of applications or services relative to the intersection of fog and health area? The types of applications are considered important because the classification in groups should help the researchers focus on a topic or a group of topics of investigation. The main types of applications selected are: mHealth, Medication, Recommender Service, Real-time health analytics, Continuous monitoring of health, Prognostics & health management (PHM) and, Ambient Assisted Living (AAL), and are summarized in Table 22 (Appendix C) and Figure 4.

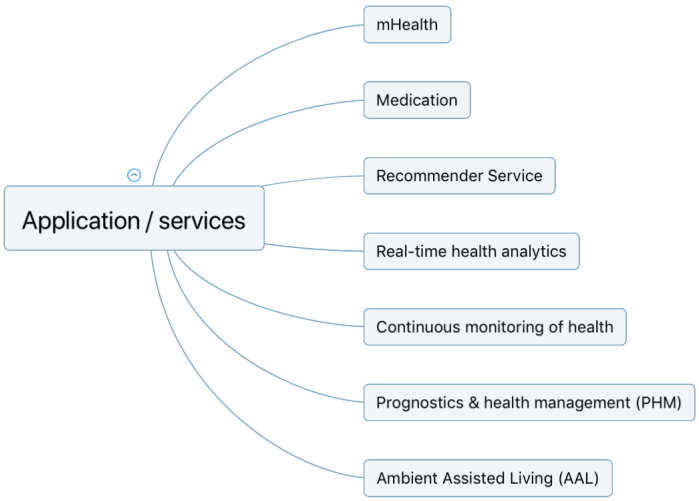

Figure 4 – Subset of proposed taxonomy.

The m-Health type of application consists of health applications that use mobile devices. Medication is an application considered usually to support the process of a doctor medicating a patient. A recommender service is an application that can suggest some service or information for a person in this context applied in the health area. A real-time health analytic application can process and analyze health data in real-time. Continuous monitoring of health consists of applications that have the function of supporting this type of monitoring of a patient. Prognostics & health management applications help doctors predict a patient's health and manage them. Finally, the Ambient Assisted Living application is which can enable the elderly and people with some limitations to be assisted in their daily routine independently and safely (OLIVEIRA et al., 2018). With question SQR1, we tried to set a general classification of application categories. We observed that real-time data analytics is a great representative (10 articles).

The m-Health (8 articles) and Ambient Assisted Living (8 articles) applications appear commonly in the selected papers. The Medication application type (7 articles) and Continuous monitoring of health (6 articles) are also standard solutions using fog computing. Other types of applications, such as Recommender Service (1 article) and Prognostics & Health Management (2 articles), have been identified.

SRQ2: What types of technologies are commonly used in the device layer relative to the intersection of fog and health?

The device layer is the closest layer from the perspective of a user. This taxonomy consists of the following groups: interface protocols and sensors, as listed in Table 23 (Appendix D) and 5. The application's environment forms the interface group: Wearable / Anywhere, Smart home, or Smart City. The protocols group is related to Data Format and Application Layer. The date format can be plain text or binary. In most cases, these text formats are JSON, XML, and CSV, allowing a person to read them without concerns. Transport Layer, Network Layer, and Link Layer consist of know protocols for each. The Sensor can be Physical, Virtual, or Logical types.

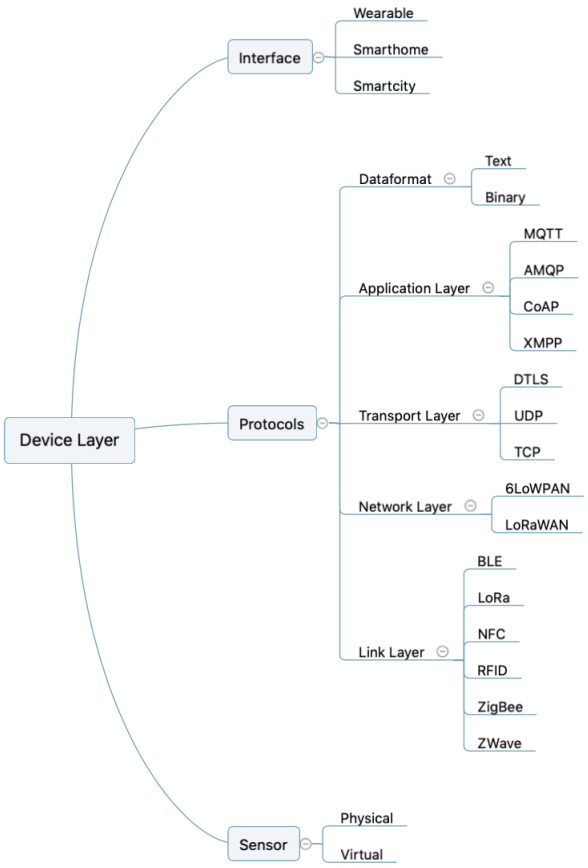

Figure 5 – Device Layer subset of proposed taxonomy.

In the device layer, we have identified a significant number of wearable (38 articles) and personal (35 articles) interfaces, showing us that smart cities and smart homes are the minority.

In the group of protocols, in the application layer, we have found that MQTT is predominant. And TCP, for the transport layer, within the 6LoWPAN network protocol. In the link layer, RFID (15 articles) and ZigBee (12 articles) are cited regularly. Finally, the physical sensors (30 articles) are commonly used.

In terms of interface, hospitals, clinics, smart homes, and sensors are the most common of them(FARAHANI et al., 2018). Hospitals regularly rely on advanced technologies in order to run their operations smoothly. One advantage of the clinic interface in IoT is that doctors can virtually access the lab reports of their patients before they visit, and clinic receptions can check the insurance coverage in real-time. Smart homes can reduce the Number of visits to hospitals and clinics, especially for patients who are elderly with chronic conditions or disabilities, it becomes vital to establish a technical infrastructure in their homes.

The sensors, for instance, medical devices with a wired / wireless interface, can be used in the eHealth ecosystem. Generally, to track patients' physical wellness and digitally monitor their health, collecting user's data from various sensors, i.e., health sensors, environmental sensors, and location sensors (SOOD; MAHAJAN, 2018a). Besides sensors, which produce data, actuators can consume it in the form of commands to generate physical outcomes (CERINA et al., 2017).

Some of the most common data captured by sensors from health applications are respiratory rate, heart rate, blood pressure, body temperature, blood glucose, electrocardiogram (ECG), electroencephalogram (EEG), user's personal, environmental, meteorological, social contact and health-related data (MANOGARAN et al., 2018) (SOOD; MAHAJAN, 2018b) (KHALID; SHAHBAZ; FAYYAZ, 2016) (SOOD; MAHAJAN, 2017). Generally, the data is transmitted for being processed in a fog environment via consumption APIs. (NASTIC et al., 2017)

The data generally is managed by acquisition, and transmission phases (SAREEN; GUPTA; SOOD, 2017) (VERMA; SOOD, 2018a) (VERMA; SOOD, 2018b) (KHALID; SHAHBAZ; FAYYAZ, 2016). The use of mobile devices to acquire data from medical sensors is common (UNGUREAN; BREZULIANU, 2017). For connecting a network of IoT sensors to the Internet through a smartphone, a model can take advantage of the 6LoWPAN protocol (ABIDEEN; SHAH, 2017). Stores data for a short period and implements some pre-processing techniques (AZIMI et al., 2016). Data acquired by these IoT devices are heterogeneous as it comprises numeric and non-numeric values (BHATIA; SOOD, 2018). The data format from mobile apps is generally serialized as a text string posted to the server.

Another strategy used is that some parameters are collected in textual, graphical, and numeric form and converted into an acceptable format by fog nodes before sending for further analysis in the cloud layer (VERMA; SOOD, 2018b). On the server side, data must be deserialized, stored in a database, and shown to the user through a web interface (MASSIMO CANONICO STEFANIA MONTANI, 2017). One common approach is using context-aware, and ubiquitous computing in the device layer (BHATIA; SOOD, 2018) (VERMA; SOOD, 2018b). For example, the emergency call considers device capabilities (e.g., TV, tablet, PDA). End-users

profile (e.g., disabled person hearing, vision, and cognitive impairments), advanced features such as automatic routing for end-users language preferences, automatic routing of emergency calls, emergency services mapping, location information retrieval, and support for people with disabilities (MARKAKIS et al., 2017). Therefore, communication protocols can be used, such as Bluetooth, Wi-Fi, ZigBee, or 6LoWPAN. (RAHMANI et al., 2018) Smart wearables and smartwatches acquire data about the person's vital health signs, and bio-sensors are embedded in the ambient environment of a person (BHATIA; SOOD, 2018).

One crucial issue is that wearable sensors possess limited memory and computing resources. Consequently, these cannot accumulate the data acquired in real-time. For accumulating the data resulting from continuous monitoring of patients, fog data architecture has services providing flexible software routines that perform on-demand, real-time accumulation of data, processing of data for extracting clinically relevant features, or mining pattern in acquired data (DUBEY et al., 2015).

SRQ3: What types of technologies are commonly used in the fog layer relative to the intersection of fog and health?

The fog layer is the central part of this taxonomy. The following groups form it: Interoperability, Data Manipulation, Technologies, Fog nodes, Interface, Service, and Task, as listed in Table 24 (Appendix E) and Figure 6. The interoperability represents how the fog can operate between different types of protocols. The included items are the Protocol translator, Network layer, Messenger layer, and Data Annotation layer. The Data Manipulation consists of operations and transformations that can be applied to data: Aggregation, Filtering, Formatting, Encoding, and Decoding. The Technologies items are represented by the Context-aware, Mobility, Big Data, QoS, Database, Web Service, and Real-time Analytics items.

The Fog Nodes are sometimes characterized as: Database, Security, Processing, Analytics, Event, and Format. The interface can be multi-standard or standard interfaces. Multi-standard interfaces are compatible with various PAN and WSN protocols (such as RFID, BLE, Zigbee, Wi-Fi, 3G/4G, and Ethernet), wired protocols (such as Ethernet), as well as different serial protocols (such as UART, SPI, and USB) (FARAHANI et al., 2018). Thus, standard interfaces support only one protocol. The resource means the use of a strategy of Communication, CPU, or storage, as well. Finally, the item Tasks represent the Assessments, Notifications, Decision Making, and Data Processing that can be used in a Fog. The leading technologies commonly in the device layer are described in Table 23 and Figure 5.

The fog layer concentrates on the high complexity of taxonomy. In terms of interoperability, the network layer (37 articles) is a hot topic. For data manipulation, Aggregation(10 articles), filtering (8 articles), and Encoding (8 articles) are widely used. Real-time analytics (24 articles), Big Data (31 articles), and Mobility (26 articles) applications are technologies commonly used with fog computing applied for health. For the fog nodes, security (35 articles), processing (37 articles), and analytics (28 articles) are highly cited in the articles. The communication service (39 articles) of the fog is an issue. The CPU (14 articles) and storage (37 articles) are also very

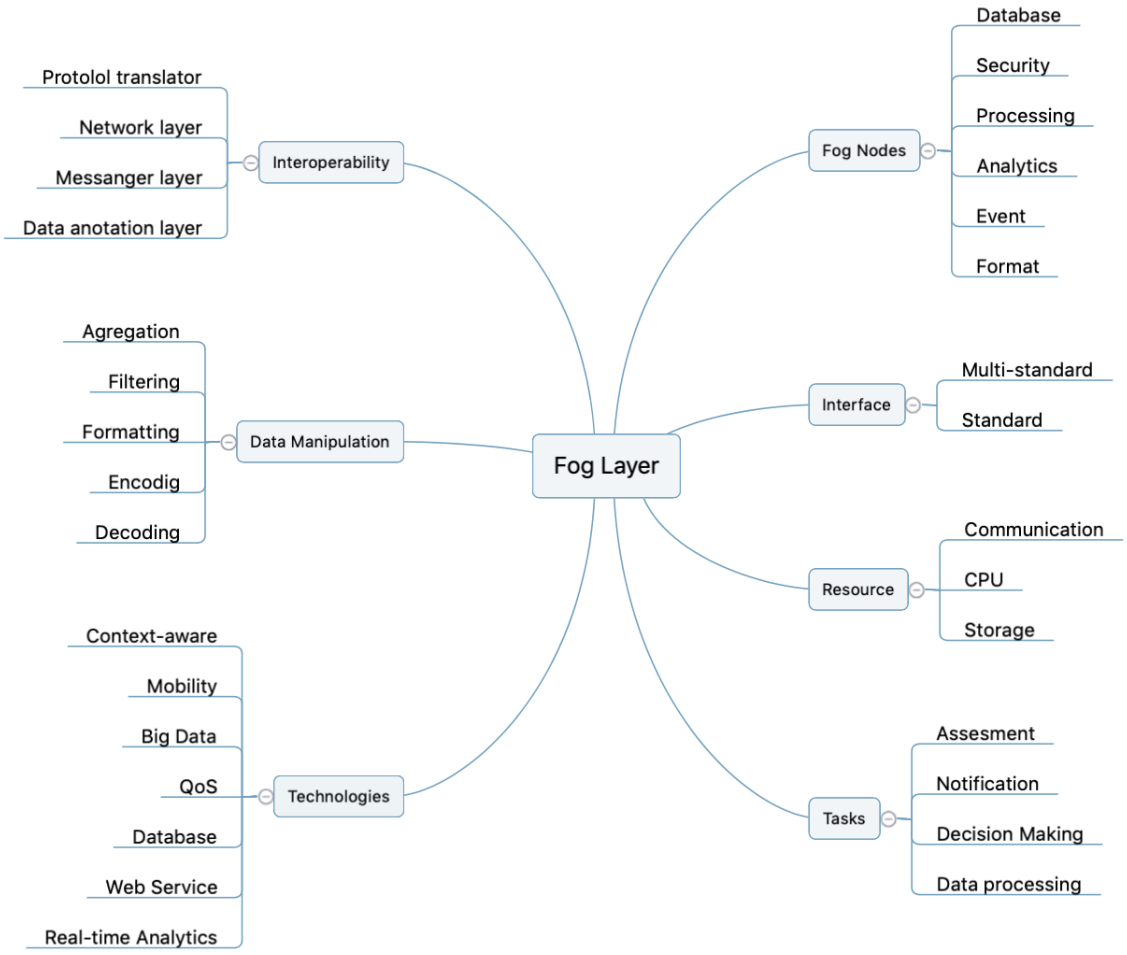

Figure 6 – Fog Layer subset of proposed taxonomy.

used in its solutions. Finally, decision-making (22 articles) and data processing (21 articles) tasks are widely needed.

Fog computing has the potential to offer services such as low latency, location awareness, quality of service assurance, and immediate notification services for real-time applications (SOOD; MAHAJAN, 2018a). In the fog computing approach, the fog node is a network edge device that can be depicted as an enhanced access point such as a multilayer switch or router, which is equipped with networking and computing capabilities to facilitate the execution of dynamic runtime self-reconfiguration mechanisms (ELMISERY; RHO; ABORIZKA, 2017).

Fog computing can be suitable for supporting human health monitoring WBAN-based systems, which have features of low energy, low bandwidth, and low processing power and include hardware-constrained nodes. To this end, combining the WBAN-based system, cloud computing, and fog computing can be a sustainable solution for challenges in the current IoT healthcare systems (GIA et al., 2015). In one possible approach, the Fog device notifies the Edge device of its intention to read data and then begins to transmit read requests cite masouros2017. One of the potential areas that fog computing could be useful is the eHealth one. In this area, we can use fog nodes to speed up the real-time processing in an emergency case and the cloud platform to maintain the patient history available for a long time (FRATU et al., 2015).

One crucial question is interoperability. IoT eHealth enables different technologies to work together seamlessly without concerning the complexity of technology integration (FARAHANI et al., 2018). Interoperability plays a vital role in the success of Health-IoT systems (RAHMANI et al., 2018). In terms of Big Data, IoT eHealth can effectively process, analyze, and manipulate data of multi-scale, multi-modal, distributed, and heterogeneous datasets produced by connected sensors in a fair amount of time. Therefore, valuable, actionable information can be extracted from health data (FARAHANI et al., 2018).

One issue is the ability to personalize and tailor content/service: IoT and big data analytics can vastly expand the possibilities to fulfill the necessity of personalized healthcare and treatments. In terms of fog nodes, one advantage is analyzing the time-sensitive data and making the highly time-sensitive decision on the fog nodes (FARAHANI et al., 2018). In a fog environment, CPU, Storage, and Communication are resources commonly used for optimizing the processing of data (CERINA et al., 2017). Data classification components can help to categorize users' health and other data that can be processed by an algorithm of Machine Learning (SOOD; MAHAJAN, 2018a). Data filtering or pattern recognition can be implemented with fog for the most efficient way of employing hardware-accelerated algorithms (CERINA et al., 2017). Furthermore, to employ FPGAs in the fog at both infrastructure and application levels, highlighting how the most recent FPGA programming paradigms could be exploited to provide rich Fog applications with maximum power efficiency (CERINA et al., 2017).

The rapid development of IoT-based healthcare applications is followed by Privacy and security risks. Since private data regarding health are especially sensitive, they must be protected appropriately. The necessity of generation, processing, and sharing health-related data with the

appropriate level of security and Privacy is an important goal that must be accomplished. Therefore, the security and privacy issues of IoT-driven healthcare systems. Privacy - Fog nodes at the network's edge usually gather sensitive data generated by sensors and end devices, particularly in healthcare applications.

Fog computing enables the analyzing and processing of data at the edge and thus minimizes the transmission of sensitive data to the cloud, which contributes to privacy preservation. Storing data in the Fog layer contributes to better protection of data. In order to protect data privacy, sensitive data from end-users must be encrypted before outsourcing it to the Fog node. Various privacy-preserving techniques (e.g., differential privacy, homomorphic encryption) can be applied between the fog and the cloud to preserve data privacy (ABIDEEN; SHAH, 2017).

Data privacy, usage privacy, and location privacy are pressing challenges that must be considered and accomplished. Authentication – The Fog level holds the potential to enable authentication in IoT devices or the appliance of lightweight encryption algorithms between Fog nodes and IoT devices to improve authentication. Networking security – Fog nodes deployed at the edge of the network bring numerous challenges regarding network management. The solution for overcoming challenges related to the implementation and management, alongside increased network scalability and decreased costs, can be found in the employment of SDN (Software Defined Networks). Attack detection – Fog computing enables the improved detection of unusual behavior or malicious attacks on both the IoT device and the Cloud sides.

Attack detection on the Fog node side can be performed by monitoring and analyzing log files, access control policies, and user login data. In this way, fog nodes can identify threats or attacks faster and mitigate them before they are passed through to the system. On the fog network side, malicious attacks such as denial-of-service (DoS), and port scanning, among others, can be detected. Challenges to implementing attack detection in the geo-distribution, large-scale, high-mobility fog computing environment and simultaneously satisfying the low-latency requisite. Access control -fog level facilitates the adoption of many standard access control models and creates an opportunity for designing new access control models. A policy-based resource access control in Fog computing can be developed to support secure collaboration and interoperability between heterogeneous resources. However, the access control design spanning end user-Fog-Cloud, satisfying designing goals, and resource constraints are challenging (MAKSIMOVIć, 2018).

Security services between Fog and Cloud computing can be used for protecting and preventing big data from intruders and unauthorized access. One approach is storing big data in different cloud data centers based on data classification and functions. For example, the data is in Sensitive, Critical, and Normal focus. Hence, the proposed system initially classifies the data according to the data type. This variety of data is stored in different cloud data centers and retrieved based on the importance (MANOGARAN et al., 2018). Security can be considered one of the essential requirements in Health-IoT applications on the ground that unsecured systems can have severe vulnerabilities to provide a high level of security (RAHMANI et al., 2018).

For security and Privacy, the various fog nodes can cooperate to achieve Privacy by encrypting collected health profiles. They could use homomorphic threshold encryption to permit particular operations to be performed on encrypted data without needing prior decryption and then submit these encrypted aggregates to the cloud (ELMISERY; RHO; ABORIZKA, 2017). The deployment, scheduling, elasticity, and basic reasonable defaults for the quality of service (QoS) are core runtime mechanisms to support executing the actions initiated by the fog layer (NASTIC et al., 2017). In some approaches, the sensor can be connected to the LoRaWAN gateway so that the information generated by these end devices can be sent directly to the Fog nodes (KHAREL; REDA; SHIN, 2017a). On the network layer, this model capitalizes the advantages of the 6LoWPAN Border Router (6LBR), which is used with the Wi-Fi interface (ABIDEEN; SHAH, 2017) with the fog. Two important principles of fog computing are distributed analytics and edge intelligence (CAO et al., 2015).

The work of (ALSHIKY; BUHARI; BARNAWI, 2017) proposes to manage and share EHRs among multiple fog nodes maintaining the cloud. The low capabilities of storage and computing of fog nodes are considered, focusing on decreasing the storage and processes in fog nodes to attend to the availability of the fog to increase its performance and effectiveness. Processing data in the fog layer can be supported by Data filtering, Data compression, and Data Analysis. In Data Filtering, Receiving data from various sensors makes it essential to implement appropriate pre-processing at the edge before any more advanced processing, such as data analysis, is performed. Bio-signals (e.g., ECG, EEG, and EMG) collected from users' bodies are the primary sources of information for assessing patient health status. Data compression can be used to reduce communication latency and energy consumed during a transaction. Data Analysis can assist the system in detecting and predicting emergencies. For instance, in the case of fall detection for older people, the fog layer can locally offer fall-detection-related processing rather than sending parameters to a cloud and waiting for the responses. Consequently, the system reacts to an emergency faster and more reliably and implements real-time responses. In addition to the system's sensitivity, utilizing data analysis in the fog layer enables the system to minimize the processing latencies of critical parameters (RAHMANI et al., 2018). The mining Layer performs the task of information extraction from the cloud database. Various data sets are stored in the form of temporal instances. Therefore in the current scenario, information mining is performed by Temporal Mining Technique. Fog-based severity analysis Information mined from the data comprises a pattern of events in terms of temporal instances.

These include events belonging to the severity class and non-severity class. Therefore, they must be analyzed over the severity scale. Performing severity analysis of time series pattern for various events will 1) determine the effects on the health of the person in the ambient office environment, 2) provides an insight into the context of the person in terms of the level of severity, 3) aids in efficient decision making concerning health-oriented problems. Based on these aspects, severity analysis for various events is performed using a probabilistic parameter termed as Severity Index (BHATIA; SOOD, 2018). For connectivity, the edge user's device can

be connected to health centers via LoRa, and hospitals are connected to health centers via the Internet or just LoRa. In the proposed system, the edge users are equipped with wearable devices, WBS, medical devices, or sensors. Depending on the device type, they can sense various health measurements (KHAREL; REDA; SHIN, 2017b).

In the work of (AZIMI et al., 2017) is proposed a hierarchical health system within subsets of shared health data between the centralized part in the cloud and the distributed part in the fog nodes. The main idea of this approach is to improve health monitoring services at the edge by reducing response time and improving availability.

SRQ4: What types of technologies are commonly used in the cloud layer?

The Cloud Layer of the taxonomy consists of the following groups: Service Model, Deployment Model, Security, and Big Data, which are described in Table 25 (Appendix F) and Figure 7.

This layer is the heavy-weight part of the architecture. This layer justifies creating a fog strategy, generally because of the low latency, dealing with massive data, or low bandwidth found there. In terms of the service model, the studied alternatives are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The Deployment Model is composed of community Cloud, hybrid cloud, private cloud, and public cloud. Security is divided into Privacy, Confidentiality, Integrity, Availability, Accountability, Access Control, Law / Compliance, and Data Protection. Finally, the Big Data group consists of Data Analytics, Machine Learning, and Deep Learning Applications.

The results found in the cloud layer show us that the service model most used is Software as Service - SaS (9 articles), with a predominance of public (5 articles) and private cloud(4 articles). The main security topics are Privacy (27 articles) and availability (21 articles) and questions related to Access Control (8 articles) and law/compliance (12 articles). Data analytics are well required in terms of Big Data (20 articles). Machine learning (18 articles) also is cited regularly. However, only one citation of Deep learning (1 article).

Cloud computing can be categorized into three service models. IaaS, PaaS, and SaaS. The difference between them is the focus of the application. In the IaaS service model, the infrastructure does not depend on the hardware being executed. In PaaS, users are provided with an underlying software and services platform to develop and use software applications without software installation. In the SaaS service model, the focus is on being able to use software applications that they do not need to install on their computers, offering them as a service over the Internet.

Cloud computing can be categorized into four deployment models: public cloud, private cloud, community cloud, and hybrid cloud. People buy or rent resources from specific service providers in the public cloud model. In the private cloud, the asset is owned or rented by the company. In community clouds, some closed communities share the resources of the cloud between them. Finally, the hybrid cloud is characterized by being formed by two or more deployment models. (AL HAMID et al., 2017).

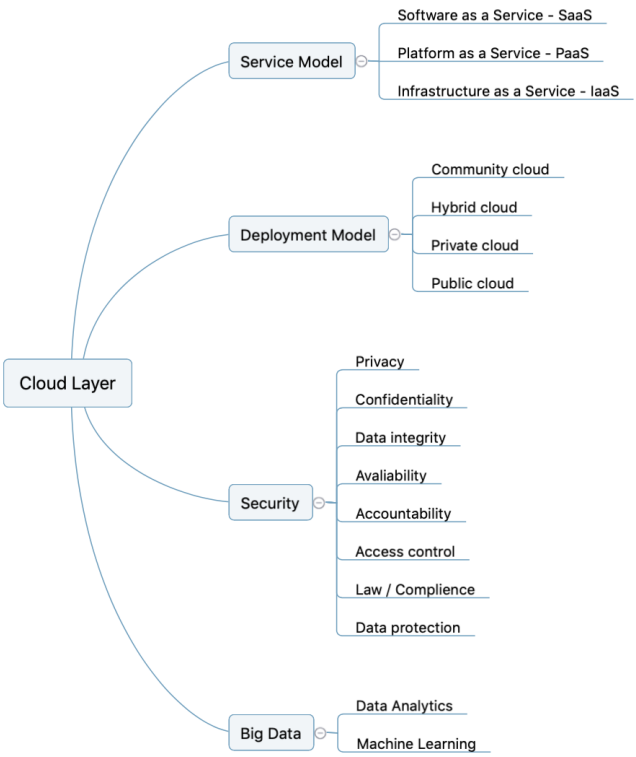

Figure 7 – Cloud Layer subset of proposed taxonomy.

IoT and cloud-based applications generate a considerable amount of data, making it difficult for the cloud system to process it in real time due to communication overhead. Cloud computing cannot provide low latency, location awareness, and high quality of service for real-time applications (SOOD; MAHAJAN, 2018a). One possible approach for the security of the cloud in a healthcare environment is increasing reliability and security with flexible policies for data transfer and encryption (CERINA et al., 2017).

In the work of (GIA et al., 2015), distributed databases contain static look-up storage, general-purpose storage, and synchronized storage. The static look-up storage contains static and essential data required for several services and algorithms (e.g., security with username and password, references for data accessing, and access management); therefore, the static database is kept intact for all cases except for the case of system administrators. The general-purpose storage, which stores high data rate input data, is used for the Fog Computing service and the graphical user interface. This fog server follows near-edge technology to connect health monitoring devices in a smart healthcare application (MANOGARAN et al., 2018).

For security proposes, usually, the architecture uses security terminologies such as the public key and private key, encryption, and decryption, cryptography identity access management, and KI certificate authority for securing data and applications in the cloud (MANOGARAN et al., 2018). In the study of (ELMISERY; RHO; ABORIZKA, 2017), the cloud healthcare recommender service interacts with the fog node to obtain a secret key for accessing the globally

concealed profile, and then it performs different filtering techniques on the group profile, which returns a list of personalized lifestyles that are correlated with such a profile. Since this list is encrypted with the distributed threshold cryptosystem, a private key needs to be reconstructed by the fog nodes. The fog node sends back the decrypted list on the reverse path to the personal gateway of the patient.

In a cloud environment, a user profiling algorithm (AL HAMID et al., 2017) can help determine whether a user is legitimate based on specific parameters, such as the user-search behavior, amount of downloaded data, nature of operations, division of tasks, and IP address. Knowing how a legitimate user deals with his / her cloud data based on these parameters will help determine whether or not the user is malicious (MASOUROS et al., 2017). There are three types of user profiling, each with different advantages and disadvantages based on the techniques used. The type we will use in our system is the hybrid user profile, a combination of explicit and implicit user profiles. The detailed user profile typically contains high-quality information because it is gathered from the user him/herself. However, it requires a lot of effort from the user to update his/her profile information.

On the other hand, the implicit user profile is automatically updated with minimal effort; however, a large amount of interaction between the user and the content is required before an accurate user profile can be created. Thus, combining the two types into a hybrid user profile should reduce the weak points and enhance the strong points of each technique used to monitor the cloud data access and detect any unusual data access pattern.

Data Collection Component (SAREEN; GUPTA; SOOD, 2017), in a traditional way, once the data is collected and processed by the Fog servers, it is transmitted to the cloud for in-depth analysis. Cloud storage provides a smooth, flexible, and secure way to share information among users, doctors, hospitals, and governmental agencies. Generally, all data on a central server can be accessed only after a prior authentication. Security issues appear at two points when transmitting data to the central server. The first point regards the data transmission by the mobile device (UNGUREAN; BREZULIANU, 2017). The primary function of a Server layer is to provide storage and critical analysis of the data. The data can be stored and managed through a database from where it can be further utilized to generate periodic reports (ABIDEEN; SHAH, 2017).

In most Cloud layer infrastructures, simple but efficient scaling and smooth integration with existing systems are designed without exposing the technical details of our system's lower layers. For example, the work of (MASOUROS et al., 2017) developed a RESTful web service using the Java Servlet API to receive data from the Fog layer and manage the database transactions of our server. User, health status classification, is essential for deciding various medical diagnoses. This component provides an initial diagnosis to users. Long-time result processing and storage encompass cloud deployment (KHALID; SHAHBAZ; FAYYAZ, 2016). This architecture is responsible for storing large amounts of data and processing output streams to analyze data collected over a long period.

3.1.11 Limitations

This research is limited to aspects related only to Fog computing applied to healthcare. In this sense, this paper focuses only on articles that address the characteristics of fog computing architectures directly related to healthcare, disregarding models within pure cloud computing or articles on fog computing without healthcare context. The search for articles was limited to the following scientific databases: ACM, Google Scholar, IEEE, Science Direct, Elsevier, and Springer. Finally, this paper sought to answer the research questions for an overview of the current literature on Fog Computing applied to healthcare. It is based only on scientific articles and does not address commercial or technological solutions.

3.2 Partial Considerations

Several challenges were selected and highlighted in this study. In Table 26 (Appendix G), we summarize the main challenges and main gaps found. The main challenges were classified as follows: interoperability, Privacy, security, unique identity, scalability, and mobility. The interoperability challenge is related to issues such as connecting heterogeneous networks, involving different protocols and networks, and how to manage and exchange data among healthcare institutions. Privacy refers to preventing data leakage in the healthcare area and the necessary access controls. The security challenge is data integrity and process accountability. A unique identity is regarding some problems of data integration problems such as a patient who can be identified by hospitals or healthcare institutions with multiple IDs and being the same person. Fragmentation of data can be a significant problem of this issue. Scalability is another critical challenge because, as the data grows, we may experience latency problems and be unable to support real-time operations. Finally, mobility is a significant challenge. Healthcare professionals and patients need relevant information multiple times, and quick and correct information can save lives.

Based on the survey carried out through the systematic literature review, several gaps and challenges were found to be analyzed for this work. These primary challenges are interoperability, Privacy, security, unique identity, scalability, and mobility. These are described in more detail in Table 26 and are summarized in Figure 8 as well. Although all the main challenges are essential, we decided to focus on three: scalability, unique identity, and Privacy. They are explained in the next Chapter.

In the current literature, privacy (LEITHARDT et al., 2020), single identity (VOHRA; JAIN, 2011), and scalability (MOURA COSTA et al., 2020b) are widely known as issues to be addressed in a distributed healthcare software architecture. These concerns are directly related to latency, Privacy, and globally unique identification, whether the item uses a globally unique identification number or a more local or unspecified location.

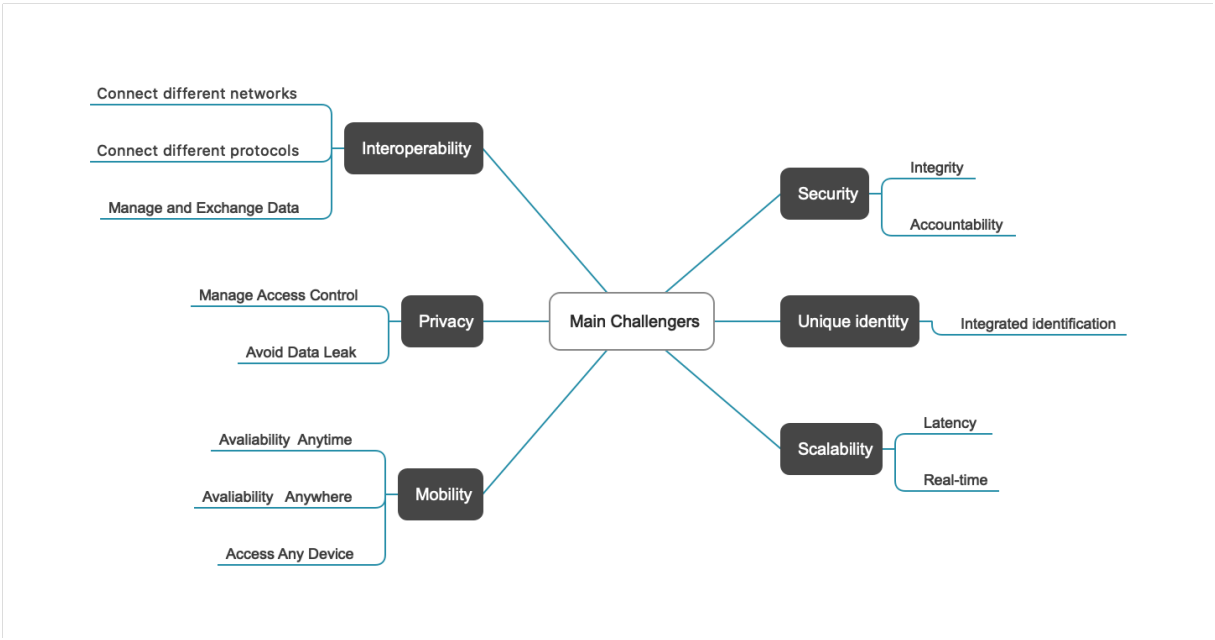

Figure 8 – Main challenges/gaps and problems to solve.

4 FOG-CARE MODEL

In this chapter, we present the FoG-Care model. The main objective of this model is to address the health challenges previously identified and considered important by the scientific community in related works. The source code is available on GitHub and cab be downloaded at https://github.com/humbertomoura/fog-care. This chapter is divided into four sections: Design Decisions, Fog-Care Model Overview, Fog-Care Model Architecture, and Global Identification. The first section explains the design decisions taken, and the following section presents the model and architecture proposed, including its objectives, and a description of its components and interactions, then the third one lists the components of the architecture and the last one presents a global identification perspective of the proposed model.

4.1 Design Decisions

The literature review studied demonstrated that the main healthcare architectures found do not propose solutions that include concerns of gain in scale (scalability) from a wide dispersed network, and do not apply privacy features while considering the issues of patient uniqueness, and support for globally distributed health data sharing capabilities. To deal with these issues, we propose that the scope of this work should highlight three main challenges identified in robust healthcare models: **unique identity**, **scalability**, and **privacy**. The reason for this choice is that the architectures found in the literature review do not propose solutions that include scalability and privacy, considering the issues of the uniqueness of assets, such as patients, and the concerns of scale gain from an integrated point of view, supporting distributed location sharing features. The use of Fog-Care architecture can be made by a mobile application or web service API. The design decisions of the main features are detailed as follows:

- **Unique identity:** There are two known alternatives for the unique identification of health assets. The Health Industry Business Communication Council - HIBCC (THE HEALTH INDUSTRY BUSINESS COMMUNICATIONS COUNCIL, 2022), and the GS1 (GS1, 2020). The HIBCC system, created in 1983, provides unique identifiers for healthcare locations - HIN and Labeler Identification Code - LIC for healthcare assets but is primarily restricted to the US market (JAYARAMAN et al., 2015). The other alternative, the GS1 Standards, was developed by an international non-profit organization that develops and implements standards to improve supply chain management in more than 23 industries, including retail, healthcare, consumer electronics, and transportation. The choice of GS1 standards was due to the possibility of solving the global naming problem with a scalable global solution.

- **Scalability:** Processing, storing, and sharing public health data requires scalable infrastructure (BARIK et al., 2017). The strategic choice for support scalability in the model

was Fog Computing. The Fog has essential characteristics such as low latency, contextual location awareness, geographical distribution, heterogeneity, interoperability, federation, and real-time interactions (IORGA et al., 2018). The low latency can be 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. Geographical distribution is important because healthcare applications can demand widely but geographically identifiable, distributed deployments with access points geographically positioned along with a wide scope area. Heterogeneity and interoperability support collect and process data of different form factors acquired through multiple network communication capabilities. Healthcare applications usually need real-time interactions rather than batch processing for a quick and urgent response.

- **Privacy:** 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 (YUE et al., 2016). The proposed approach to address the privacy problem is to implement a model based on blockchain technology. It is a tamper-evident, and tamper-resistant digital ledger 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 (YAGA et al., 2019). Deploying healthcare data in a blockchain can provide several benefits, such as complete, consistent, timely, accurate, and easily distributed data and agreements without the involvement of a trusted mediator. Another essential feature is to avoid performance bottlenecks or a possible single point of failure and allow patients to control their data. Changes in the blockchain healthcare data are visible to all members of the blockchain network, and all data insertions are immutable, but the privacy of the patient's data is protected by authorization access allowed by the patient. In addition, any unauthorized changes can be detected easily (ESPOSITO et al., 2018).

This list of challenges emerged from several secondary contexts identified in the literature: Health Facilities, Persons, Assets, Technology, Health Data, and Application (Figure 9).

- **Health Facilities** are any building or place designated for the hospitalization and treatment of a sick or injured person. Hospitals can belong to a certain complex, a group of hospitals managed by the same organization. Generally, they can contain hospitals of each specialty and are located in the same geographic location. Clinics are health centers where you can receive routine preventive care or visit your doctor. A clinic is an institution smaller than a hospital that aims to serve patients who need simple procedures and short stays. Medical laboratories are places where clinical pathology tests are performed on clinical specimens to obtain information about a patient's health to aid in diagnosing,

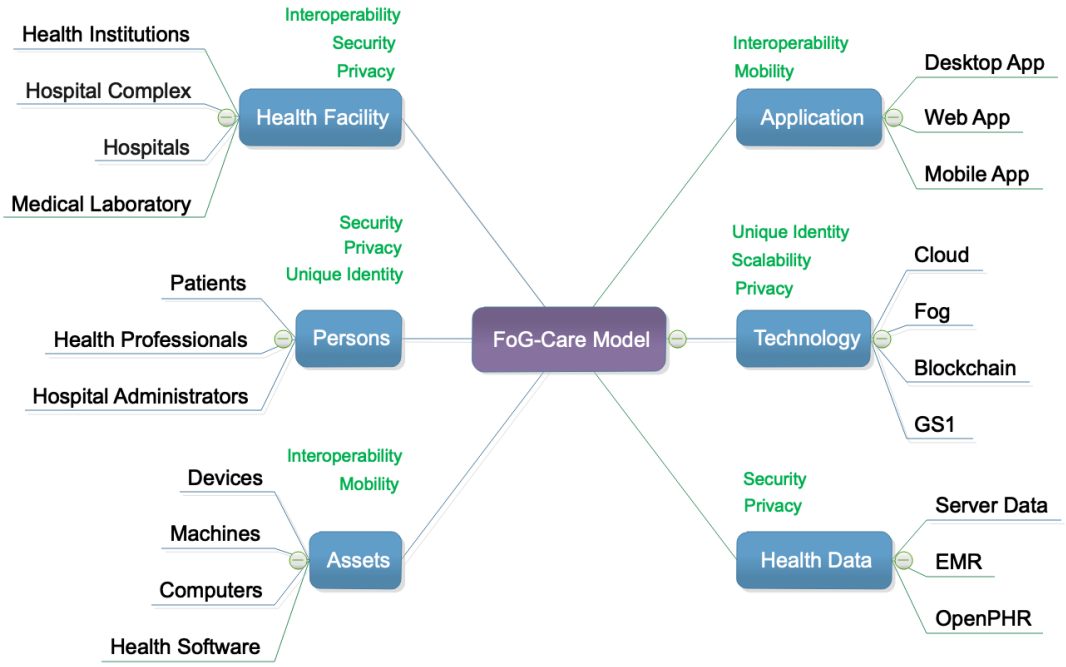

Figure 9 – Fog-Care contexts and detailed challenges.

treating, and preventing disease. Generally, laboratories work together with hospitals or clinics because of their specialized tests. In this model, each health unit can collaborate, share health data, and be geographically distributed close to or distant from each other.

- **Persons** This component represents, in this architecture, a single individual who received medical care in a hospital, clinic, or other locations. A global identification number globally identifies each patient. Patients are a central part of the model because health care aims to prevent disease, help people live longer, and improve their quality of life. A patient may have a device, such as a cellphone or a tablet, which can be used to consult and annotate relevant data about himself.

- **Assets** can contain devices (medical devices, smartphones, tablets, wearables), machines (Medical equipment), computers (desktops, laptops, servers), and health software. Due to hardware and software diversity and healthcare requirements, these artifacts are hard to manage. Assets are limited resources, and the possibility of globally searching and locating them quickly can help professionals and health facilities to be more efficient.

- **Application** can be considered a mobile app for the use of the patient or the medical professionals or web applications running on the cloud or Fog, for example. This kind of application is essential for use with distributed systems software. The desktop application must be considered in terms of interoperability and legacy information systems.

- **Technology** is crucial for this type of architecture. Cloud, Fog, Blockchain, and GS1 are core technologies proposed to develop the model and architecture for healthcare. The cloud can be considered for scale-distributed location data and services. The Fog is a component to help reduce latency and provide real-time applications. Blockchain is useful for privacy and GS1 for the unique and global identification of any kind of asset.

- **Health data** is the historical data that was found in a patient's medical records, such as an Electronic Health Record. The patient can usually access health data through a mobile app. Typically, this data is stored by the hospital and accessed by the doctor using some software. Global data comprises all data found outside of local and essential data. These data comprise the records of other hospitals, clinics, etc., and the patient must authorize access. The data can be stored on a blockchain distributed with each partner healthcare facility.

4.2 Fog-Care Model Overview

Figure 10 shows a general view of the Fog-Care model. For a better understanding, the high-level parts of the model are presented as follows. They are composed of the hospital complex, hospitals, patients, tokens, GS1 Standards, Fog, health data, and Blockchain. The main differential of this model is that it was built based on the challenges and gaps in privacy, unique identity, and scalability, found in the systematic literature review of this work, developed in chapter 3. The main components of the model are described as follows.

- **Hospitals / Clinics / Medical Laboratories**: They are any determined build or place for the hospitalization and treatment of a sick or injured person. Hospitals can belong to a determined Hospital Complex, 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 always smaller than a hospital, and the patients are generally more healthy and do not stay overnight. Medical laboratories are a place where clinical pathology tests are carried out on clinical specimens to obtain information about a patient's health to aid in the diagnosis, treatment, and prevention of disease. Generally, laboratories work together with hospitals or clinics because of their specialized tests. In this model, each health facility can collaborate, share health data, and be geographically distributed close or far from each other.

- **Patient**: This component represents, in this model, a unique individual who had received medical care at a hospital, clinic, or another place. A GTIN number globally identifies each patient. Patients are a central part of the model because healthcare aims to prevent diseases, help people live longer, and improve their quality of life. A patient may have

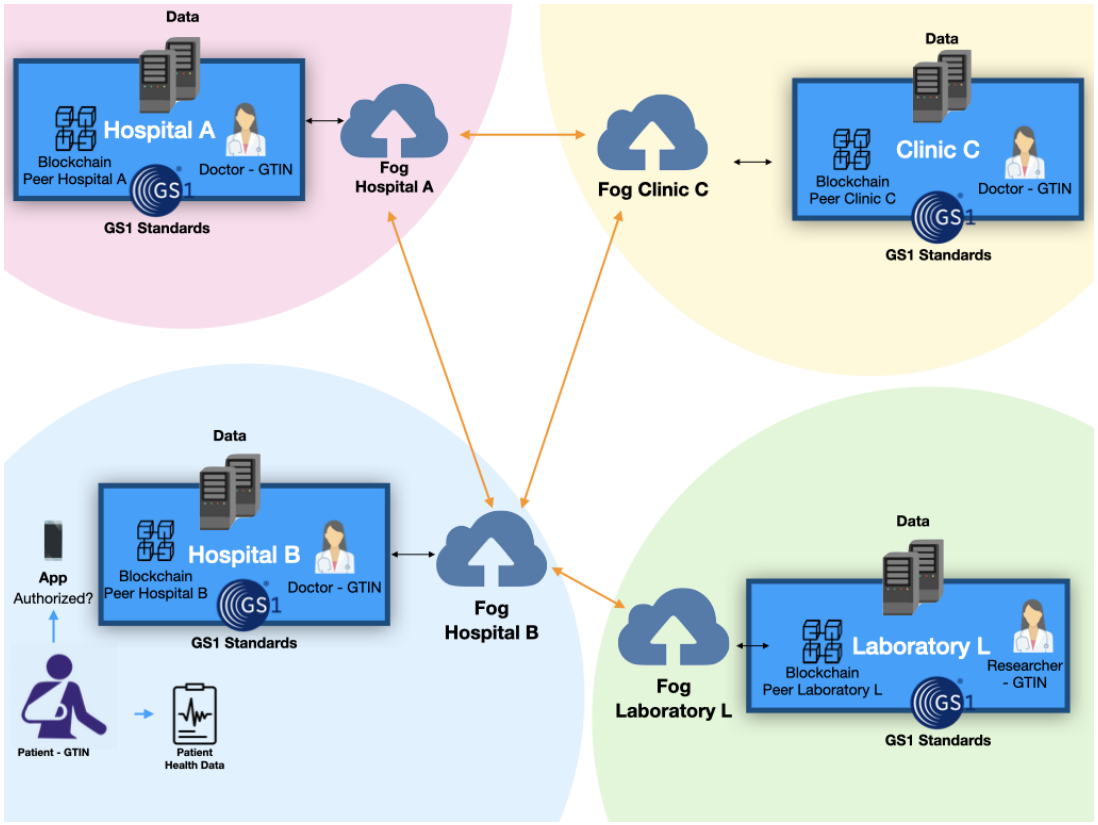

Figure 10 – FoG-Care Architecture overview.

a device, such as a cellphone or a tablet, which can be used to consult and write down relevant data from himself.

- **Fog-Care Token Card**: This token is a unique number associated with a single patient and represented by a card. The GTIN number globally identifies the token card. This token can be held virtually in a mobile app, with a bar of code, for ease of use. The patient can hold the card and show it to the attendant to read the care code. The patient can authorize the use of their health data through a mobile application, for example. The patient's location may be relevant so that the authentication and authorization process for using their health data can be automatically secure in this case.

- **Fog nodes**: The fog nodes are responsible for sending and receiving health data between hospitals and internal departments. Each Fog runs a REST service with an API defined to query, edit or share data. In this model, a Hospital can contain several internal fogs and a Fog to communicate with other institutions such as clinics, hospitals, laboratories, and others. Each time health data is requested fog checks if the information exists locally on an internal server or if it must be requested outside the health unit. The main idea of Fog is to reduce latency and locally process all possible health data, avoiding overloading the clouds.

- **Health data**: Health data can be divided into three parts: Mini EHR, local data, and

global data. Mini EHR data is the essential data like basic patient identification e.g., id, name, date of birth, gender, blood type, allergies, intolerance, etc. It can be queried by the token with the GTIN number and can be accessed by the patient through a mobile application. Local data are historical data found in patients' medical records, such as the Electronic Health Records. Typically, this data is stored by the hospital and accessed by the doctor using some software. Global data is made up of all data found outside of local and essential data. These data comprise the records of other hospitals, clinics, etc., and the patient must authorize access. The data can be stored on a blockchain distributed with each partner healthcare facility. ‘

- **Blockchain**: In general, essential health data can be shared with other hospitals for the purpose of obtaining a more detailed health history of patients. This data structure can be stored in the form of medical records on the Blockchain. The advantages of this approach are the guarantee of data privacy and the integrity and traceability of the entire processing of these records. In this model, the Blockchain stores its data, such as patients and exams, with standard GS1 codes like GTIN with the idea of global identification for use with each current or future partner healthcare facility.
- **GS1 Standards**: The technology helps develop, promote and implement global industry standards for solutions to prevent medical errors, combat counterfeit products and improve supply chain efficiency across the healthcare industry. This model aims to provide globally unique identification for healthcare assets, patients, exams, and medical equipment. Each asset receives a barcode and can be viewed via a mobile or web app.

4.2.1 Stakeholders Perspectives / Prototype

The Fog-Care model supports global data exchange between hospitals and institutions with privacy, scalability, and unique identification. We present three perspectives of the FoG-Care model application examples in a mobile application prototype. The first perspective is from the Patient and the second is under the health professional, and the third one is about the administrative staff. The data is stored in the smartphone, Blockchain, or a server or Fog of a health facility. The mobile application prototype called Fog-Care is divided into two versions. The first version (blue screen) is the Fog-Care Patient, responsible for the interaction of the patients and the second one (orange screen) is the Fog-Care Health Facility, which health professionals and administrative staff use to query and update the healthcare data. We can view the login screenshot of both versions in Figure 11.

- **Perspective of Patient:** The patients are the central part of this work. Each patient is identified by a global identifier number (GTIN) assigned the first time he goes to the hospital. With this number, patients can use the mobile Fog-Care application to manage their health information. In this application, the patient can save essential health information

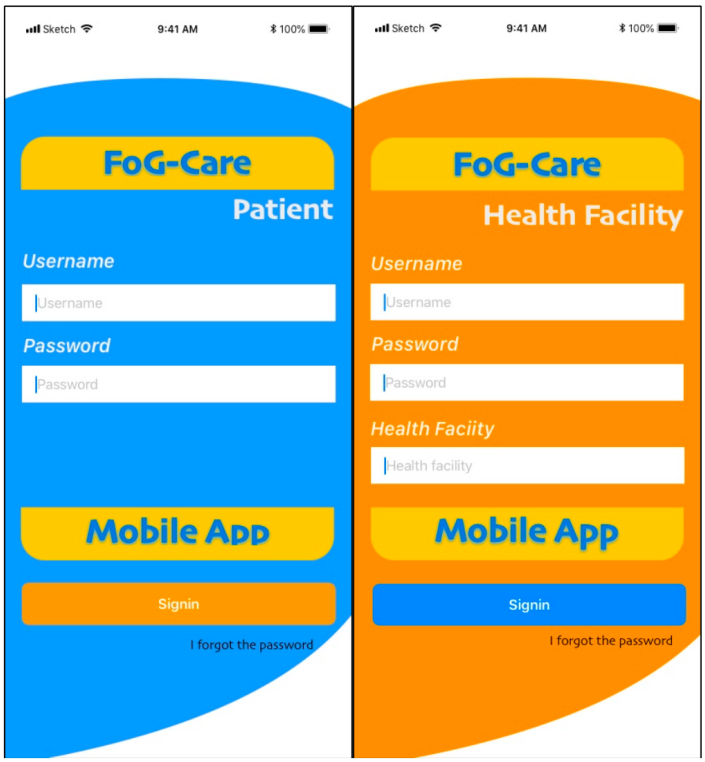

Figure 11 – Patient and Health Facility Login Screens.

about themselves (Mini EHR menu option), search for global information about their health data (Global EHR menu option), and authorize the use of their health information by health facilities (Authorization menu option). An image of the main menu of the prototype application is shown in Figure 12. The Mini EHR contains patient data such as blood type, age, food tolerance, and allergies. More detailed information regarding these items is presented in the next section, called Architecture. The Global EHR contains the health data of patients from multiple facilities, globally distributed, able to access and view the information. This data comes from the past use by the patient in these hospitals or clinics. The Authorization option permits the patient authorizes a health facility to view his health data. It can be from an automatic way, where the patient is near a hospital (detected by the smartphone's GPS) or specific permission assigned by the patient to determined hospitals or clinics. The code bar in the app and the token card can help to quickly get the patient to be attended to because all the information can be requested through the GTIN number of the patient.

- **Perspective of the Health Professional:** The health professional can be a doctor, a nurse, or a physiotherapist who works for a health facility, for example. He or she uses a mobile app version exclusive to them. He can search and update the EHR Global data of patients (Patient EHR Global option) if authorized, search assets such as medical machines and equipment (Search Global Assets), and enroll patients in the Fog-Care information system (Enroll Patient option). The prototype screen is shown in Figure 13.

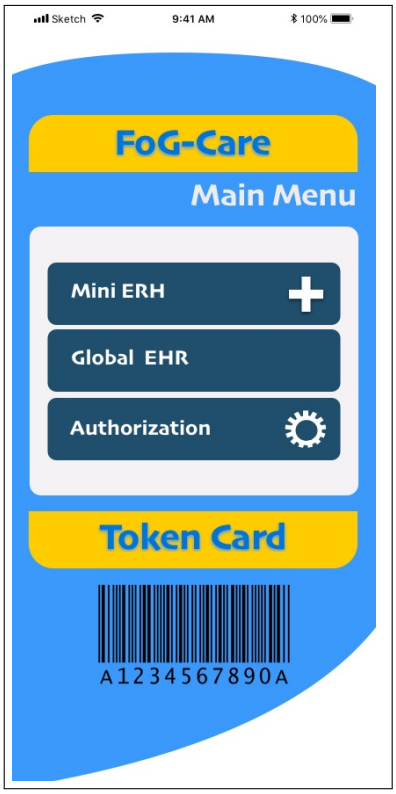

Figure 12 – Patient Main Menu Screen.

- **Perspective of Administrative Staff:** The administrative staff is attendants, managers, and directors of the health facility. They can enroll patients, enroll medical professionals and manage assets such as medical devices and equipment. They use the same application as health professionals, but the main menu is different, as shown in the picture 14.

4.3 Fog-Care Architecture

This architecture is detailed in Figure 15, using the Fundamental Modeling Control - FMC. This notation enables the communication of concepts and structures of complex informational systems efficiently among the different stakeholders. It is composed of a universal notation originating from existing standards, is easy to learn and apply, and is defined to visualize the structures and communicate coherently. In contrast to most of today's visualization and modeling standards, it focuses on human comprehension of complex systems on all levels of abstraction by clearly separating conceptual structures from implementation structures (FUNDAMENTAL MODELING CONCEPS, 2012).

The FoG-Care Architecture consists of a Patient Service Layer, an Installation Service (organization), and health data (GS1 Resource). A detailed description of the layers is shown below:

Health Data (GS1 Resource) is represented by Patient Data and hospital resources. Patient Data represents health data stored at a local hospital and the Token contains essential patient

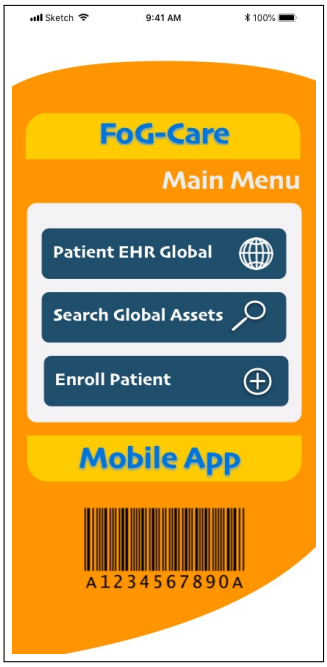

Figure 13 – Health Facility Main Menu Screen.

information. Hospital resources contain the EHR/PHR, Data warehouse, Blockchain, and Data Lake. The first is a standard in the healthcare industry data format, widely used by hospitals to store patient data internally. The last two resources are almost always used as auxiliary data in the hospital, usually for research subjects. Each service is responsible for managing its resource.

The Patient Care Layer has three services: Privacy Service, Security Service, and Interoperability Service. It is the layer responsible for patient-related security, privacy, and interoperability services. Patient data is considered all data that can be shared between healthcare facilities such as hospitals, laboratories, and clinics and is required for patient authorization. Patients and their resources have a unique number for global identification. The security service encapsulates basic security infrastructures such as authentication, Integrity, and access control. The privacy service addresses the issue of who is allowed to see what data. The Interoperability Service ensures that all data communication can be done correctly, adapting to each context, e.g. mobile desktop or web user interfaces.

Privacy Service is responsible for data privacy guarantees. It also ensures that patients, physicians, administrative users, and staff have adequate access and control. This includes using a blockchain network to control and audit the Integrity of healthcare data and services related to patient privacy.

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 patient data. Some data can be incomplete or invalid, so supporting these systems can improve security. Another important feature of this service is protecting which data can be shared externally with other health facilities such as hospitals,

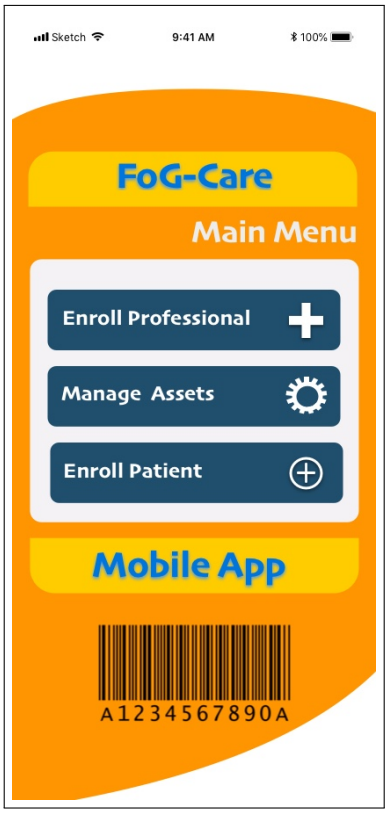

Figure 14 – Staff Main Menu Screen.

clinics, or laboratories partners.

The Interoperability Service can help streamline healthcare industry operations because often data comes from multiple information sources such as laboratories, clinics, pharmacies, and hospitals and has multiple 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 three services: Global Access Service, Fog Service, and Blockchain Service. A facility is any place where healthcare is provided, for example, a hospital, clinic, laboratory, etc. This layer contains the Global Access Service, Blockchain Service, and Fog Service.

The Global Access Service manages all health data access strategies for the unit. For example, it can directly delegate to a Fog or Blockchain if necessary, according to the facility's policies and rules. It implements the unique identification of patients' requirements.

The Fog Service represents one or more fog nodes depending on the strategy configuration. Fog, supported by fog nodes, helps to get the data with reduced latency compared to the cloud. Fog nodes are responsible for sending and receiving healthcare data between different hospitals or other psychic structures. Each Fog runs a REST service with an API defined to query, edit or share data. Each time health data is requested fog checks whether the information exists locally on an internal server or must be requested outside the health facility. The main idea of Fog is to reduce latency and locally process all possible health data without overloading the clouds. Your

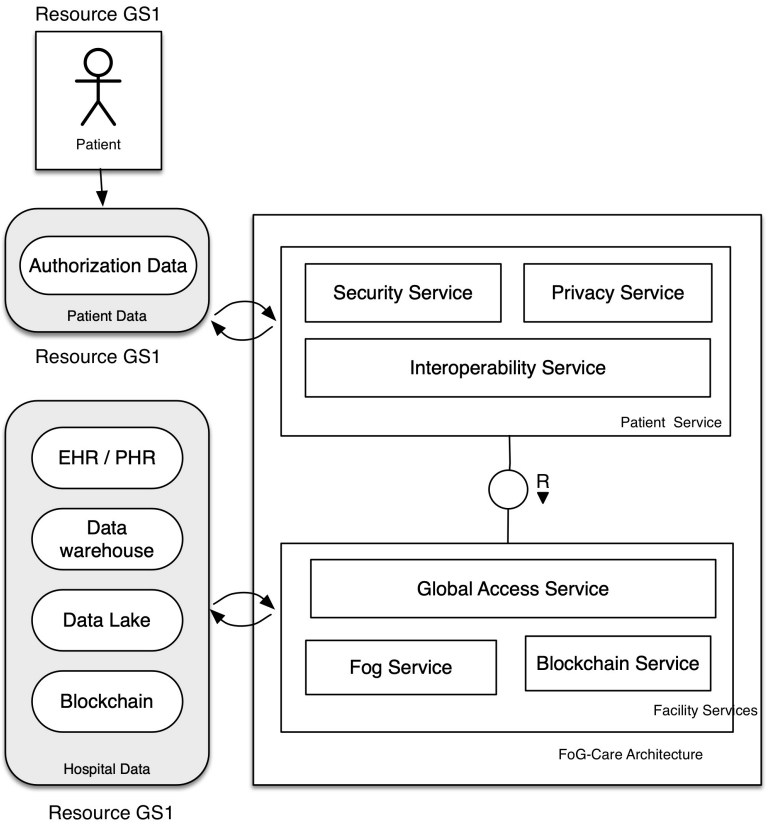

Figure 15 – FoG-Care Architecture.

services can access the Blockchain and all installation data as long as the user has permission. It implements the scalability requirement.

The Blockchain Service allows access to read or write health data in the same way as a database, with the difference that all data is tracked and the book cannot be deleted. It implements the privacy requirement. Blockchain implementation is included to share essential health data with other hospitals to get patients' more detailed health histories. This data structure can be stored in the form of medical records on the Blockchain. The advantages of this approach are the guarantee of data privacy and the Integrity and traceability of all 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 current or future partner organization. This service is formed by a set of layers described in Figure 16.

Privacy concerns exist when personally identifiable or other confidential information is collected, stored, used, and ultimately destroyed or deleted in digital or other format or otherwise (MITTAL, 2009). Blockchain guarantees data privacy. It also ensures that patients, physicians, administrative users, and staff have appropriate access and control. This includes using a blockchain network to control and audit the Integrity of healthcare data and services related to patient privacy. 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:

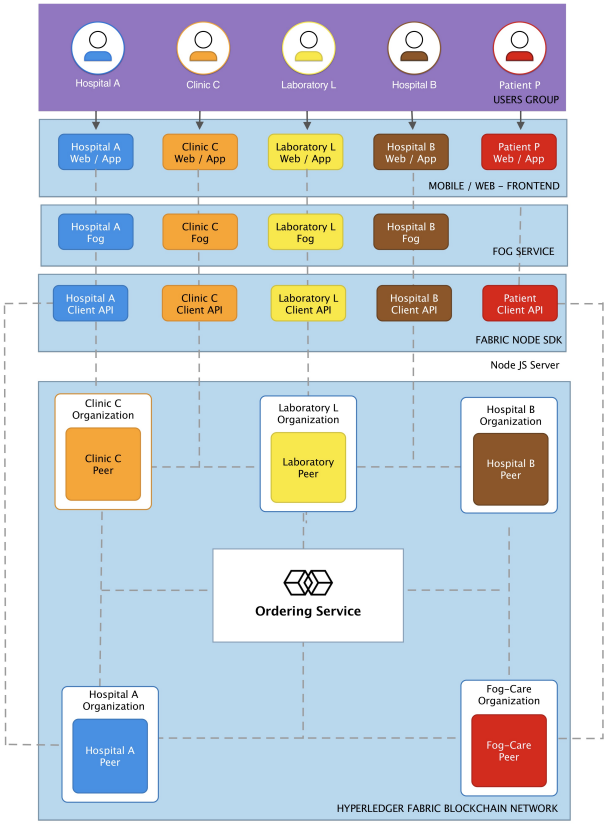

Figure 16 – Blockchain Service of Fog-Care Architecture.

- **The User Group** represents the authorized users of the Blockchain. They are grouped by affiliations or companies called Organizations. Various organizations may exist such as Hospital A, Hospital B, Clinic C, Laboratory L, and Patient P as examples demonstrated in this component. There are doctors, daycare centers, and attendants of these organizations, such as Hospital A, Hospital B, and all healthcare facilities participating in the blockchain network. Each user group belongs to a health unit (organization) where these individuals and groups do not know each other and may be geographically distributed. Therefore, they can trust to share health data due to the blockchain consensus providing the privacy and Integrity of all operations performed. Each organization controls its users, access, and permissions independently.

- **Mobile/Web - Front-end Layer** represents the user interface. This software can be a mobile application, web application, or both. Each healthcare facility hosts this software in their organization, except the patient group, which belongs to the FogCare group, a special organization created to manage the global identity of all blockchain patients. Authentication in this application is based on the organization's users defined in the previous layer, all participants in the Blockchain. The main features were presented in the previous model section. For example, a physician can search for exams for a particular patient, or a patient can authorize their health data to be viewed by all healthcare institutions.

- **The Fog Service Layer** consists of a set of Web Services to service and fulfill requests from the Front-end layer. Each organization has at least one Fog Service, including Fog nodes. Fog nodes can be routers, switches, or any server responsible for the communication of devices in your geographic area, being able to provide them with (DEBE et al., 2020) services. Fog nodes are positioned close to IoT devices and handle data heterogeneity from different devices. This Fog receives the internal requests and checks if the data can be brought in from the local network or if the request needs to be passed to an external organization. The purpose of this layer is to reduce network latency and provide a scalable near real-time healthcare application. The structure of the Fog Service is described and explained in the following subsection Healthcare Communication Service.

- **The Fabric Node SDK Layer** contains the server code that receives requests from the Fog Service to call essential client APIs for interacting with the blockchain network. Every organization, such as a healthcare facility, must have this code implemented and run on its network. The exception is the Patient Client API because the user uses the front-end or mobile app for patients that interact directly with this layer instead of Fog Service Layers, and it is not implemented in a healthcare facility. Some basic operations can be: creating channels, asking peer nodes to join the channel, installing chaincodes on peers, instantiating chaincodes on a channel, invoking transactions by calling the chaincode, and querying the ledger for transactions or blocks.

  As a client, all code in this layer interfaces with the ordering and peering services of the next layer, the Hyperledger Fabric Blockchain Network.

- **The Hyperledger Fabric Blockchain Network** is the core layer of the proposed blockchain architecture. It is formed by Peers, Ledger, Fog Service, and Ordering Service.

  - **The Peers** hosts instances of the ledger and instances of smart contracts (chaincode) containing the health code and health data of the health facility (GUPTA et al., 2020). This provides deliberate redundancy to avoid single points of failure. Each blockchain network is mainly composed of a set of peer nodes. In this layer, each health unit has its different pair. In addition, there is a unique Fog-Care partner to manage patients globally and address your unique global identification of them. In conjunction with the requester, Peers ensures that the ledger is kept up to date on all peers. The main purpose of a peer is to maintain the state of the network and a copy of the ledger. Therefore, there are two different types of peers, endorsing and committing peers. Endorsers' peers can simulate and endorse transactions, and committers' peers can verify endorsements and validate transaction results before committing transactions to the Blockchain. Thus, the ordering service accepts endorsed transactions, orders them into a block, and delivers the blocks to the acknowledgment peers.

– **The Ledger blockchain** is used to store the patient's health data, such as exams, location, medications, comorbidities, blood type, diseases, tolerance, and allergies. In this proposed healthcare blockchain architecture, the ledger can store patients' EHR securely and privately. GS1 standards are used on resources to ensure these essential resources' identification, location, and traceability. In Figure17, the Ledger attributes are shown. This approach aims to provide essential information for quicker health care and better response time (KUMAR et al., 2020). In the blockchain ledger, the Token Card and Mini EHR are stored. It can include exams, location, medications, comorbidities, blood type, diseases, tolerance, and allergies. In this proposed healthcare blockchain architecture, the ledger stores the patients' Mini EHR securely and privately.

– **The Fog Service** consists of a set of Web Services to service and fulfill requests from the Front-end layer. There is at least one Fog Service in each organization. This Fog receives the internal requests and checks if the data can be brought in from the local network or if the request needs to be passed to an external organization. The purpose of this layer is to reduce network latency and provide a scalable near real-time healthcare application. A set of web services implements it through a URI. All resource URIs of this API will have the following syntax described in Table 5:

Table 5 – Fog-Care Global Blockchain Asset data structure.

Statement	Sintaxe	Description
GET	GET fogRoot/fogName/fogVersion/	Gets a resource from the determined fog
PUT	PUT fogRoot/fogName/fogVersion/	Save a resource to the determined fog
DELETE	DELETE fogRoot/fogName/fogVersion/	Drop a resource from the determined fog

The fogRoot and fogName parameters are discovered using the naming service. The fog version is an integer and increases each time a new Fog version is released. The API includes support for HTTP or HTTPS schema host and an optional port. It will also support ETF RFC 2818 (HTTP over TLS). The content response will accept JSON format and must be identified by the application/JSON parameter.

This API uses the OAuth 2.0 client (IETF RFC 6749), and supports the GET statement, which is used to get a resource from a given fog. Otherwise, PUT saves a resource, and DELETE deletes a resource.

There are many web services on Fog. The main ones are Patient, User, Equipment, and EHR. They implement GET and PUT methods to query and add an item to the Fabric NODE SDK layer service or collect data from local healthcare facilities stored in a local EHR/PHR file, a Data Lake, or Data Warehouse, for example. Each health unit defines which data will be supported and implemented in the architecture.

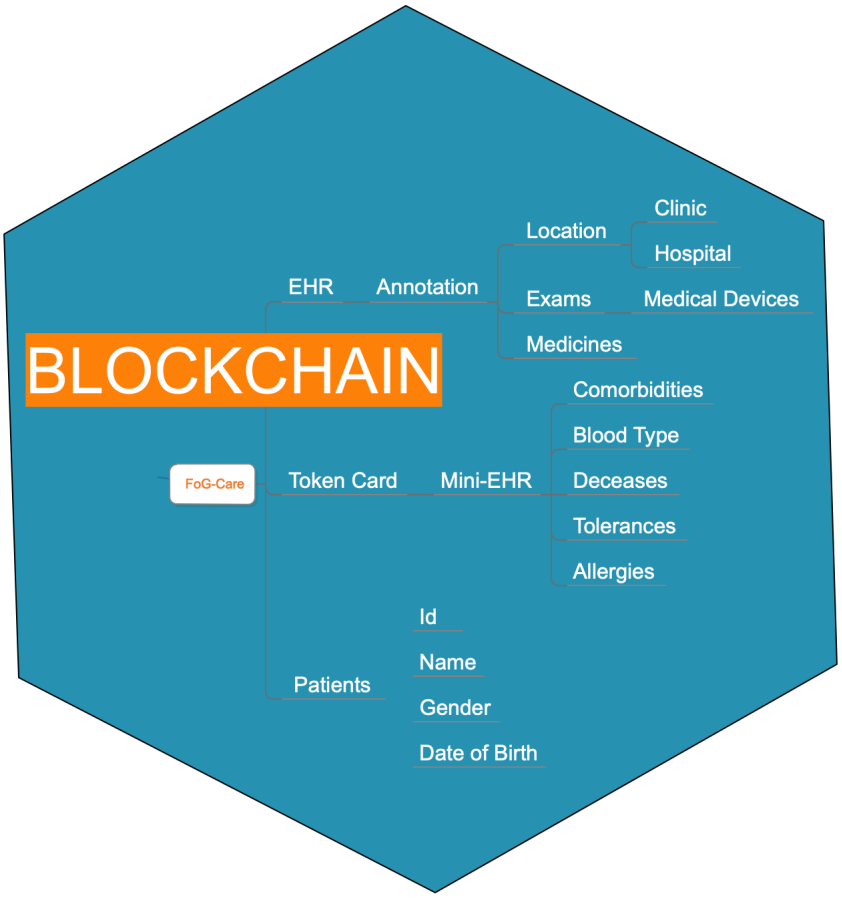

Figure 17 – Blockchain and GS1 point of view of the Model.

The patient is the main component of the health data and their Token Card. The Fog-Care Peer manages it. As we need to uniquely and globally identify it, it is essential to store a minimal identifiable data structure. The patient's name and birth data can resolve this concern. The 6 table demonstrates the patient data structure and patient data relationships of the Blockchain, as shown in Figures 18 and 19.

Table 6 – Fog-Care Global Blockchain Patient data structure.

Item	Type	Description
ID	String	GTIN of the patient
Name	String	Name of the patient
Gender	String	Gender of the patient
Date of Birth	Date	date of birth of the patient

Each patient has their own Mini EHR, stored exclusively in the Fog-Care pair. This health data contains relevant and essential information about the patient's health. So anyone who can scan the Token (the patient's GTIN number) can access the patient's blood type, possible food tolerance, allergies, and other data. Table 7 demonstrates the Mini EHR.

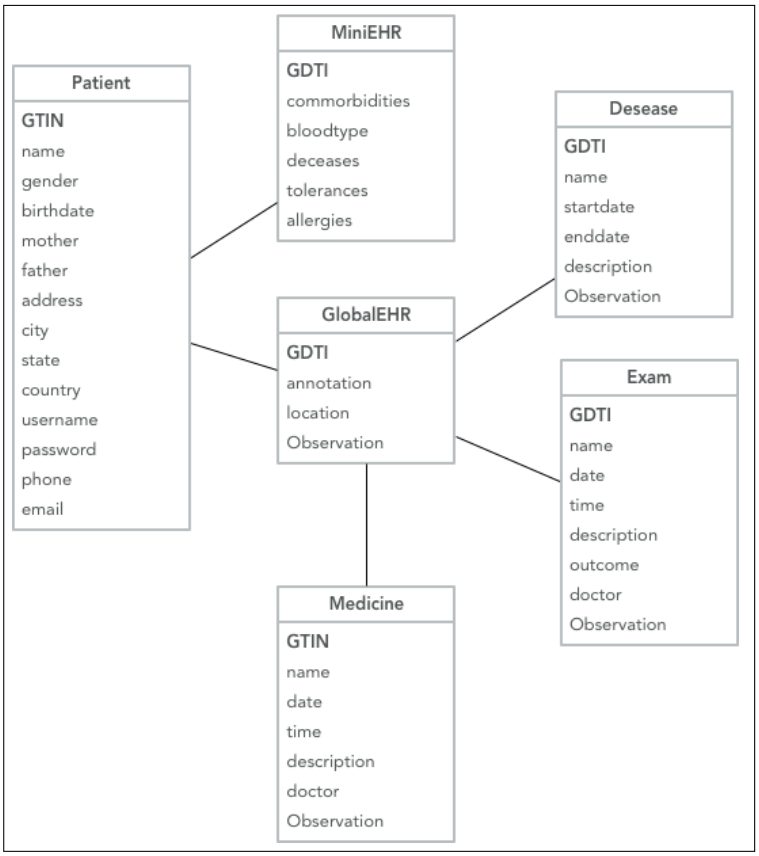

Figure 18 – Patient Data.

Table 7 – Fog-Care Global Blockchain Mini HR data structure.

Item	Type	Description
ID	String	GTIN of the patient
Comorbidity	String	Name of the patient
Blood type	String	Gender of the patient
Decease	String	GTIN of decease
Tolerance	String	GTIN of Tolerance
Allergy	String	GTIN of Allergy
Date	Date	Date of enroll

Exams are a fundamental part of health data. Each health unit can perform several tests. These exams have a GDTI number that uniquely identifies the id and is assigned to a particular patient. All exams can be entered by healthcare facilities on the Blockchain and available to other organizations if the patient has been authorized. The table 8 shows the data structure of the exams.

Assets are essential equipment for a healthcare facility. The lack of artificial respirators in ICU beds, for example, during pandemics such as COVID-19, defined the health system's ability to respond to the pandemic. With information on the quick location of these assets, the allocation of these scarce resources can be better distributed. The 9 table shows the assets of

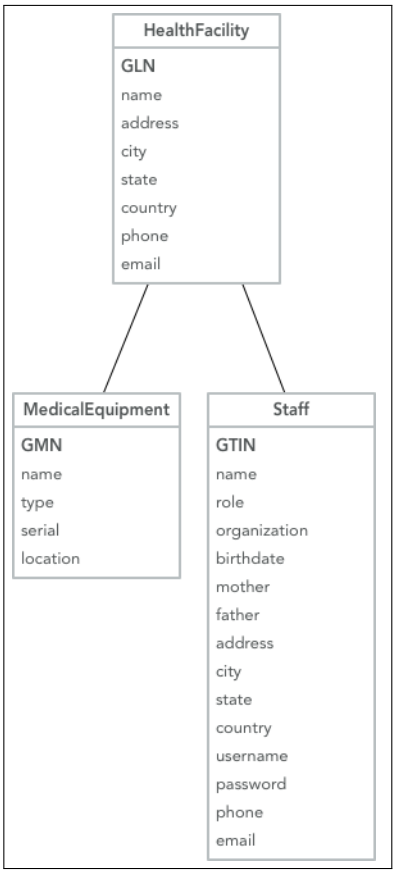

Figure 19 – Health Facility Data.

Table 8 – Fog-Care Global Blockchain Exam data structure.

Item	Type	Description
ID	String	GDTI of the Exam
Date of Exam	Date	Date of Exam
Location	String	GLN of Location of the exam
Medicine	String	GS of the medicine
Date	Date	Date of enroll

the FoG-Care Blockchain model.

Table 9 – Fog-Care Global Blockchain Asset data structure.

Item	Type	Description
ID	String	GLN of the health facility
Name	String	GIAI of the asset
model	String	GMN Model of the asset
Date	Date	date of enrollment of the asset

The model proposed in this article, called Fog-Care, aims to contribute to facing the problems and challenges in distributed computing software applied to the health domain. The most

relevant challenges are scalability, unique identity, and privacy. In addition, there are real gaps to be addressed, such as using these technologies in a more integrated way, considering asset uniqueness issues such as patient identity, and concerns of scaling from an integrated point of view and supporting distributed sharing. health data are considered.

Therefore, the GS1 standards approach was chosen due to the possibility of solving the global nomenclature problem with a scalable global solution. GS1 Global is an organization formed by a global community of voluntary users as stakeholders in the healthcare supply chain, including manufacturers, distributors, hospitals, solution providers, and regulatory and industrial bodies that have developed standards to enable healthcare providers to uniquely identify products, patients, clinics, assets and locations for transparent processes across the entire medical value chain with a single, unambiguous global identification system for sharing data (GS1, 2020). The advantages of these standards can be: ease of use and usefulness, product identification, accurate and reliable tracking, information accuracy, and information availability (KRITCHANCHAI; HOEUR; ENGELSETH, 2018).

The (BARIK et al., 2017) scalability support is implemented through Fog Computing (IORGA et al., 2018). Healthcare apps often need real-time interactions rather than batch processing for quick and urgent response (FARAHANI et al., 2018). Low latency is implemented with fog nodes placed close to smart end devices, so analysis and response are faster than from a centralized cloud service or data center. The importance of geographic distribution is because healthcare applications may require widely distributed, but geographically identifiable deployments, with geographically positioned hotspots along a wide (NASTIC et al., 2017) scope area.

A privacy issue (YUE et al., 2016) is a significant challenge for healthcare data systems to become more intelligent in collecting, storing, and analyzing personal healthcare data without generating privacy breaches. For these systems, privacy concerns created barriers to adopting health data systems (YUE et al., 2016), and the definitions described in (PEREIRA; CROCKER; LEITHARDT, 2022). The proposed approach to solving the privacy problem is Blockchain. Blockchains are tamper-proof digital ledgers implemented in a distributed fashion, without a central repository, often without a central authority such as a company or government. They can allow a community of users to record transactions in a shared ledger where no transactions can be changed once they are published (YAGA et al., 2019). Deploying healthcare data on a blockchain can provide several benefits, such as: complete, consistent, timely, accurate, and easily distributed data and agreements without the involvement of a trusted mediator. They were avoiding performance bottlenecks or a potential single point of failure. Patients can have control over their data. Changes to the health data of the Blockchain are visible to all members of the blockchain network, and all data entries are immutable. Furthermore, any unauthorized changes can be easily detected (ESPOSITO et al., 2018).

4.4 Global Identification

For global identification, several standards are required. For example, the GTIN is used to identify the patient, the Mini EHR, and all the information necessary to globally identify patient health data such as exams, comorbidities, deceased or dietary restrictions. Each patient can use a mobile app with their respective assigned patient token. For the geographic location of healthcare facilities such as hospitals, clinics, and laboratories, the Global Location Number - GLN is used by default. The location of the healthcare facility can be considered with the patient's proximity, and the patient can view their healthcare data per permission and privacy control. In addition, equipment such as medical machines can be located using a Global Model Number (GMN). In Table 10, we can visualize the Fog-Care Global Identification items.

Table 10 – Fog-Care Global Identification items.

Asset	Used for globally identify	GS1 Standard
Patient	global patient identifier	GTIN
Mini health records	global patient essential information	GTIN
Token	FoG-Care card	GTIN
Health facilities	Hospitals, clinics, laboratories	GLN
Medical Machines	mechanical respirators, Magnetic resonance imaging machine	GMN
Exams	X-ray, electrocardiography - ECG	GDTI
Decease	Cancer, HIV/AIDS	GTIN
Comorbidities	Diabetics, lactose tolerance, gluten tolerance	GTIN

Health data is represented by Patient Data and hospital resources. Patient Data represents healthcare data stored at a local hospital, and the Token contains essential information about the patient. Hospital resources contain the EHR/PHR, Data warehouse, Blockchain, and Data Lake. The first is a standard in the healthcare industry data format, widely used by hospitals to store patient data internally. The last two resources are almost always used as auxiliary data in the hospital, usually for research subjects. Each service is responsible for managing its resource.

4.4.1 ID-Care Component

The ID-Care component included in the Fog-Care model aims to address the issues and challenges related to globally unique identification, compliance with standards, privacy/security, and longevity of records previously studied in the literature review.

The Id-care has five parts: Legal Document, Biometry, ID Services, and Visualization (Figure 20).

- **Legal Document:** This layer is responsible for the legal traceability of a person. According to the country of origin, various documents can be accepted. For example, national identity, health identity, and passports are widely used by countries to identify citizens.

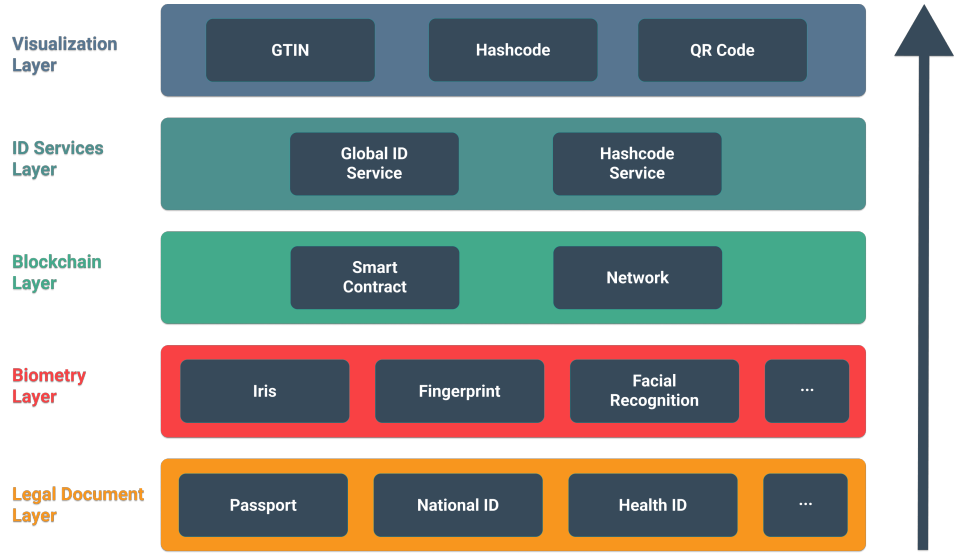

Figure 20 – Global ID Model.

Registering a patient on ID-Care must exist legally and be traceable, no matter where they were born. One of the ways to ensure this is by using documents from the country of origin or current residence. This layer is the basis for the other layers because a person must legally exist and be mapped to only a single record in the world.

- **Biometry:** Different countries use different biometrics methods to identify a person. The ID-Care model must support a variety of data, including those that will appear in the future. For this, there is a separate field in the blockchain records to store this data. The most well-known biometric data are fingerprint, iris, and facial recognition. For example, there are many forms of facial recognition, but they all result in a number or string that can be used as part of a font for a unique identifier. In general, a set of numbers representing a fingerprint can be included in an algorithm mixed with a patient's document ID to create the global ID. The biometric layer is used in the model according to each country, as some of them still do not implement biometric authentication. In this case, the fields are padded with zeros.

- **Blockchain:** The blockchain layer is responsible for the most important privacy and security implementations, such as smart contracts and a decentralized network model. There are smart contracts that identify people and assets to create subsidies for use in the identification services layer. These smart contracts can be upgraded and create additional future services for the population based on demand and need. Thus, the Network service supports new hospitals and healthcare facilities, helping to integrate them into a global-scale environment.

- **ID Services Layer:** In this layer, all services supported by global health identification are provided. The primary services are the global id services, which are responsible

for generating and validating the global ID, and the Hashcode service, which exposes an API for generating and validating associated hashcodes. Implementing identification services in the API format can enable future integration with government health service applications from all interested countries or academic research carried out by universities or international health organizations.

- **View Layer:** In the view layer, GTIN, hashcode, and QRCode views are provided. These services get the data from the ID Services layer. The GTIN, which is created according to the GS1 specification, can be used by compatible healthcare applications simply by implementing QRCode reading support.

Typically, a user workflow consists of a process from authentication to decision-making (Figure 21). It includes creating a global id for the patient and digitally linking it to their healthcare data, sharing it on a global blockchain network available and distributed in various associated countries. This approach allows for the rapid identification of patients and the visualization of their health data by health facilities and authorities, contributing to informed health-related decision-making. The main items are:

- **global unique identification:** The importance of geographic distribution is because healthcare applications may require widely distributed, but geographically identifiable deployments, with geographically positioned hotspots along a wide (NASTIC et al., 2017) scope area.

- **standards compatibility:** The proposed model implements the GS1 standards approach due to the support of a scalable global solution. GS1 Global is an organization that has developed standards to enable healthcare institutions to uniquely identify products, patients, clinics, assets, and locations with a global and unambiguous identification infrastructure to share data (GS1, 2020). The main advantages are ease of use and usefulness for product identification, accurate tracking, and reliable availability of information (KRITCHANCHAI; HOEUR; ENGELSETH, 2018).

- **privacy/security:** Privacy concerns are crucial for healthcare data applications. Blockchain can be used to collect, store and analyze health data more intelligently and prevent privacy breaches (YUE et al., 2016). In this proposed model, all data is stored in blockchain smart contracts to maintain the Integrity and privacy of distributed health data sharing. Patients can have privacy control of their data. Using a blockchain to store healthcare data offers several benefits, such as supporting complete, consistent, timely, accurate, and easily distributed data and agreements without a single trusted intermediary.

- **longevity of records:** Blockchains are tamper-proof and tamper-proof digital ledgers. This ensures that changes to the integrity data of the Blockchain are transparent to all

members of the blockchain network and that all data entered is immutable. Also, any unauthorized changes can be detected easily due to implementation without a central repository or authority such as a company or government (ESPOSITO et al., 2018). Blockchain applications can allow a community of users to record transactions on a shared ledger where no transaction can be changed once published (YAGA et al., 2019) and has the benefits of avoiding performance bottlenecks in contrast to the potential single point of failure of other models.

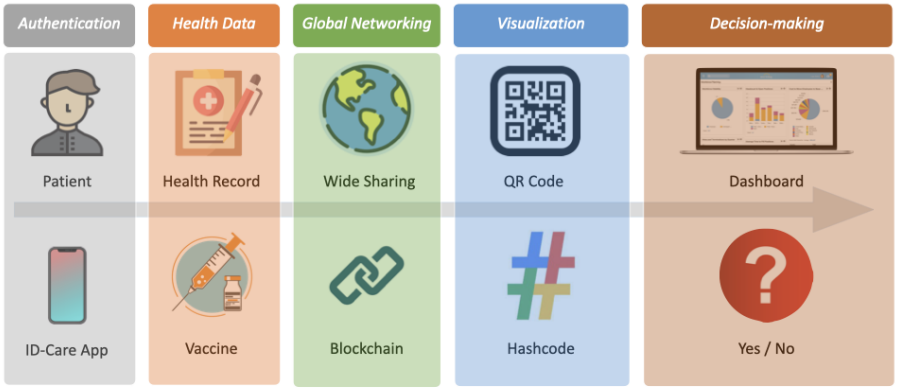

Figure 21 – Global ID Process Flow.

The ID-Care process flow is composed of seven components: Healthcare Professionals, Hospitals, ID-Care Desktop, and Mobile Application, Blockchain Network, ID-Care QR Code, and Patient, as described below:

- **Healthcare Professionals:** Professionals such as doctors, nurses, physiotherapists, psychiatrists, and assistants. These professionals work in hospitals or other healthcare facilities. They often see patients and operate the mobile software's ID-Care Desktop.

- **Hospitals:** organizations that may be geographically distributed across countries and continents, such as hospitals, clinics, and laboratories. Each organization can enroll new patients in the ID-Care software through an app or desktop application. Each hospital has its professionals and health team. ID-Care software verifies that the patient is registered, according to documents and biometric data, when a hospital employee registers an appointment.

- **ID-Care Desktop:** Software run in hospitals that allows the enrollment or consultation of an ID-Care patient. The software can be used by patients and healthcare professionals authorized by their healthcare facilities. The software can generate a QR Code to identify the patient and uses a blockchain network.

- **ID-Care Application:** Mobile application that the patient can use to identify himself as a unique global patient through a QR Code generated by the ID-Care Software. This app is available globally to all people around the world.
- **Blockchain Network:** A decentralized network that supports blockchain smart contracts such as Hyperledger or Ethereal.
- **ID-Care QR Code:** QR-Code generated by ID-Care software based on a unique global hashcode of patient documents and biometric data.
- **Patient:** A person who goes to a health facility because they need health services. This person will be enrolled in the ID-Care software if they have not already done so. Identity care is the same in all countries for the same person.

5 MATERIALS AND METHODS

This chapter presents the methodology and evaluation for this work. It is divided into the Implementation section, where is presented the implementation of the evaluation proposed, section Scalability Evaluation, presenting the metrics proposed in a vaccination scenario; and the section Unique Identity and Privacy Evaluation, where another evaluation is proposed, considering the uniqueness of identity and privacy in a global healthcare data sharing scenario.

We propose evaluating the Fog-Care model considering the features of scalability, privacy, and unique identification (Table 26), which were described as crucial for the success of healthcare applications in the systematic literature review. This evaluation is divided into two parts: a use case of a global vaccination campaign evaluating the scalability and a global tourism strategy for evaluating unique identity and privacy issues. To summarize, the evaluation might answer these questions:

- **Scalability** The proposed architecture has to support many computers from geographically distributed locations. As more computers are added to the architecture, latency issues can occur. Does the model need to support real-time operation even with dozens of computers connected? Considering five health establishments, the model can be scaled from five to fifty organizations. What is the measured performance between the two scenarios?

- **Privacy** Security and privacy are critical issues in this work's systematic literature review. Healthcare has several restrictions and limitations regarding functions and access to electronic health records and health assets. Did the architecture increase patient privacy and meet all the requirements of care limitations identified in the literature review?

- **Unique identity** Could the patient be uniquely and globally identified without concerns and restrictions in a healthcare setting? The authorization process considered the automatic location of the patient and her authorization. The health data stored on the blockchain proved healthy and up-to-date in the application landscape.

The first section, Implementation, describes the details of these scenarios and the model implementation and its infrastructure. The second section, Scalability Evaluation, demonstrates the metrics proposed to evaluate the scalability in the vaccination scenario. The third section, Unique Identity, and Privacy Evaluation propose an evaluation of these features in the scenario of a global tourism strategy.

5.1 Implementation

For the evaluation of the Fog-Care model, several virtual machines from Amazon Web Service - AWS were installed and configured (Figure 22). Each VM was instantiated on its own,

serving as a Fog node. The configuration used for the tests was a standard AWS t2.micro machine with one vCPUs and 1 RAM (GiB) (AMAZON EC2 T2 INSTANCES, 2012). A Hyperledger Caliper version 0.43 evaluation suite was used for metrics evaluations of the blockchain network.

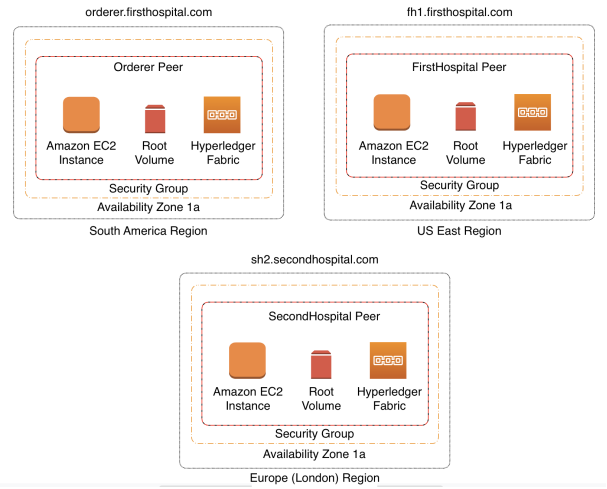

Figure 22 – Fog-Care implementation on Amazon Web Services - AWS.

To support the privacy of vaccination data, a Hyperledger Blockchain implementation is developed that includes the definition of 5 main assets: Person, Vaccine, Vaccination, Questions, and Answers (Figure 23).

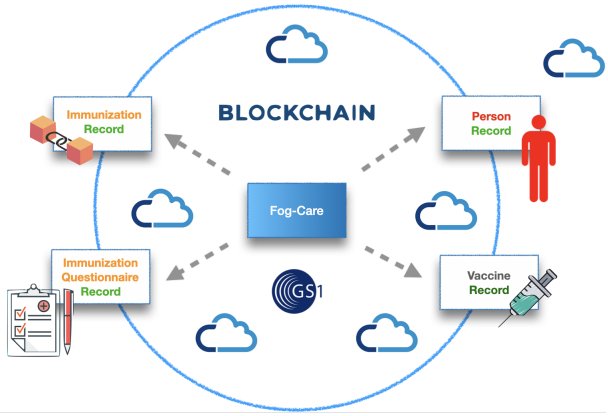

Figure 23 – Fog-Care implementation in a vaccination use case.

The **Vaccine Record** consists of a representation of a Vaccine and is implemented in a Smart Contract with the ReadVaccine and WriteVaccine methods. The fields include some characteristics like name, minimum temperature, maximum temperature, a unique identification id, and others shown in Table 11.

Table 11 – 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		

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

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

5.1.1 Legal Document Implementation

Documents are one of the most important and traditional assets to prove who a person is. Several countries have a national identification number, such as the Social Security Number (SSN) in the US or the Cadastro de Pessoas Físicas (CPF) in Brazil. In general, IDs have requirements for validation. For example, in the US the SSN has these requirements:

- Contains 9 digits.
- Can be split into 3 blocks separated by a hyphen.

- The first block must be 3 digits long and cannot be 000, 666 or between 900 and 999.

- The second block must be 2 digits long and between 01 and 99.

- The third block must be 4 digits long and is between 0001 and 9999.

A regular expression would be a viable solution, but it would not be viable on a global scale, considering that each document format has different validation. Although this solution addresses US identification, each country has its ID, including a different validation method. In France, Spain, and Italy, national identity cards are issued by the governments of all member states of the European Economic Area (EEA) except Iceland, Denmark, and Ireland. In China, the Resident Identity Card is an official identity document for personal identification in the People's Republic of China. The ID card contains basic information such as full name, gender, ethnicity, date of birth, domicile, and personal photo. Since 1999, there has been a citizen identification number consisting of an 18-digit code. This number is made up of the first five numbers of the address code, the next eight numbers, the date of birth, and the next three digits, a code used to disambiguate people with the same date of birth and address code, and the last one a code check.

Also, in some countries, there are other documents like health identification numbers, driver's licenses, etc. Therefore, in the implementation of this work, the ID-Care definition supports a validation method for each document and country.

5.1.2 Biometry Implementation

There are a large number of biometrics technology found in various countries. The main technologies are fingerprint scanning, iris recognition, and facial recognition. Even the same technology, like facial recognition, can be solved by a few different algorithm implementations. In Brazil, the election is carried out through electronic voting machines. The person who will vote must be registered in a fingerprint-based authentication software as a requirement. This fingerprint and facial recognition system can currently be used to identify a citizen in other government software applications.

The European Union uses mandatory fingerprints and facial images on EU citizens' identity cards and non-EU family members' residence cards for regulatory proposals in three areas: EU citizens' ID cards, registration certificates, and residence cards issued to Union family members who are not nationals of a Member State.

Each country has its biometrics system, but the biometrics result is usually a string or number representing the image. The ID-Care software must have a comparison method to test if this result is the same or different from the stored data of a patient.

5.1.3 Blockchain Implementation

Blockchain implementation is divided into two parts: network and smart contracts. The network consists of a private hyperledger blockchain model defined by Costa et al. (COSTA et al., 2022). The main feature of this module is to include a peer, remove a peer and authenticate peers and users, according to the organization of health facilities. The smart contract module is coded for the Go language, making it possible to register and enter new information about patients and vaccination processes. There are several smart contracts dealing with the solution. The smart contracts created are included in the Listing 2

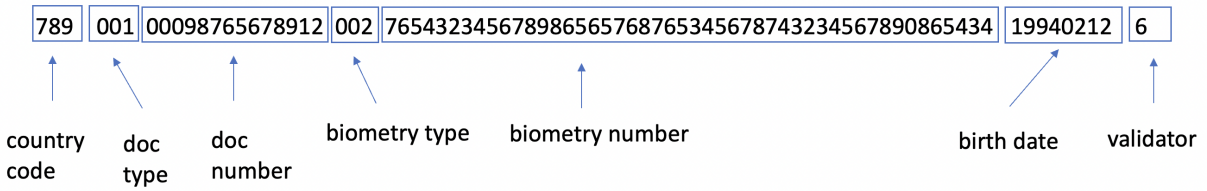

Figure 24 – Hashcode Implementation.

5.1.4 ID Services Implementation

ID Services has two modules: the Hashcode Service and the Global ID Service. First, the Hashcode Service generates the global id hashcode based on the EPC Global GS1 Standard. The format is shown in Figure 24. There are seven parts to this hash code: country code, document type, document number, biometrics data, biometrics number, date of birth, and validator. A summary of the fields can be viewed in Table 12.

- **Country Code:** The country code is the standardized GS1 code in which the patient was born. In our hypothetical vaccination scenario, including the US, Brazil, United Kingdom, USA, Spain, and Portugal the codes are respectively: 789, 100, 960, 840, and 560.

- **Document Type:** A document type is a code that represents documents available for use. For example, 001 id, 002 driver's license, 003 passport, and so on. For our hypothetical scenario, the chosen values are 001, 001, 003, 001, and 002.

- **Document Number:** The document number is exactly the digits of the selected document. For example, in Brazil, the id consists of 11 digits. Since the field consists of 14 numbers (Table 12), we need to add 000 to the left of the number of patients in this country. The hypothetical values are 00098765678912, 00000463786537, 00008356789871, 00599287656839, and 0000000654356839.

Table 12 – Summary of Main Fields.

Field	Digits	Description	Examples
Country Code	3	GS1 country code which the patient was born	789 Brazil, 001 USA
Document Type	3	National document type of patient	001 national id, 002 driver's license
Document Number	14	Patient identification id number	00098765678912
Biometry Data	3	Biometry data used for patient identification	001 Fingerprint, 002 Face detection
Biometry Number	48	Last 48 digits of biometry number	7654323456789865657687 653456787432345678908 65434
Birth Date	8	Birth date of patient (yyyymmdd)	Documents and Biometry
Validator	1	GS1 code validator	6
Global ID (id-care)	522	SHA512 from Hashcode	idcare://1b0517faa833231f9 2a23104800e92f5eeeb296f3 346da9e1e68b7a2...

- **Biometrics Data:** The biometric type is a 3-digit code representing current and future biometric technologies, such as 001 fingerprint, 002 face detection, 003 iris recognition, or 000 none. The main idea is to allow all countries to choose the technology according to their possibilities. For our scenario, the values are 002, 001, 002, 001, and 001, respectively.

- **Biometric number:** The biometric number represents the result of the chosen biometric image (i.e., the last 48 of the fingerprint, iris, or face image) if it is greater than this number (For example, Table 13.

- **Date of birth:** The date of birth represents a patient's date of birth in "year month day"format. The values in the scenario are 19940212, 19850430, 19720915, 19980502, and 19660322.

- **Validator:** The validator is a single digit from 0 to 9 that validates the entire hashcode. This validator is based on the GS1 validation number (CHECK DIGIT CALCULATOR. HOW TO CALCULATE A DIGIT CHECK MANUALLY, 2022). To generate the validator, follow these steps:

  - **Step one:** Build a table with 80 columns, and put the number to be verified, but the last digit reserved for the validator
  - **Step two:** Add the numbers in odd positions.
  - **Step three:** Multiply the result of Step Two by three.

- **Step four:** Add the numbers in even positions.
- **Step Five:** Add the results of Step Three and Step Four.
- **Step six:** Check that the digit is the smallest value needed to round the result of Step Five to the nearest multiple of 10. Figure 24 shows the first hashcode generated in our scenario. Listing 1 is the complete code for validation.

After obtaining the hashcode, it is important to use the Global ID service to generate the Global ID (ID-Care). These services use a SHA512 encryption algorithm to generate the final number.

5.1.5 View Implementation

For Visualization Services, it is possible to visualize the data in 3 hashcode formats, GTIN and QRCode.

- **hashcode:** The visualization in hashcode format is shown in Figure 24. This format allows the investigation of the fields that form the patient data. It is stored on a privacy-controlled blockchain.
- **GTIN:** The GTIN format is the hashcode with a SHA512 encryption algorithm forming the Global ID, including an ”id-care://”prefix. The purpose is to point the address for an application or software to use to manipulate that address.
- **QR Code:** The QR Code format is generated by the application from the Global ID Data.

Table 13 – Fields of Patients' Scenario.

Patient	Country	Doc Type	Doc Number	Bio Type	Bio Number	Birth date	Validator
1	789	001	00098765678912	002	765432345678986565768765345678743234567890865434	19940212	6
2	100	001	00000463786537	001	546787654234567898654356789456723456983256798125	19850430	8
3	960	003	00008356789871	002	954325873257947031768024794368490236487498465894	19720915	4
4	840	001	00599287656839	001	176543879863087653789052678904376578958904532671	19980502	3
5	560	002	00000006543287	001	078765318798754789056783480451497905784276804589	19660322	2

Table 14 – Global ID from hashcodes.

Global ID (ID-Care)
idcare://48240ee9281f84aab6992b7f80d82b400eafd8a3a75d53d75168134be6cd8158f1ebbbc9a0ee77b61a7e851a88de40ba0163a556516676d6147bde35a5d97960
idcare://6265d58f6b727c02bbca0a5241e608df43f5e115d1eb419385b9007057edc6e1aed593d5e9f9b46d2c7b57f4a1759577adac6383185b7de1ac0df0b14199bbec
idcare://22884ad68269f637bfe23f50db2c63ec103c16d644431cdb1d18aceae678b28e9515ef33f32f8507f7c80ee112700bf54fb783309ea82aefb8018661ae675415
idcare://fc078ac074d4f130c8bd3a73f2849b20962098fe1a7d98ff1c7e5ac4936acfec84070f505217ab4c97b6a8b90f226a961d4c813c8b645c8bfe1fbccc03c9ba87
idcare://d68f6fe7f738427c17e90c3756f2f6f7bf79b1c00734cf0990f6d8d5ce1fcedb8e172119cffc608bffe80a6ae95ae678a126ff8ee34f6a53edb93a67b7613444

Figure 25 – ID-Care QR Code of Patients.

5.1.6 Prototype Implementation

The main focus is to support the unique global identification of the patient. After a mutual meeting, the countries decided to implement a solution based on the ID-Care model, and the aim is to support a global vaccination plan which can be good for all countries. Figure 33 shows the prototype screens for patient use. The following actions (Figure 33 b)) can be done by patients: login, schedule vaccination, take the vaccine, show their global ID, and view their profile.

- **Login:** the login process (Figure 33 a)) is done through username and password or cell phone biometrics. These logins are recorded by hospital staff during the patient's first use.

- **Schedule vaccination:** This option allows the patient to schedule a vaccine by typing the type of vaccine, date, time, and location (hospital, clinic, etc.) of the application (Figure 33 c)).

- **Get the vaccine:** It is used in the vaccination process. If everything is right, the Pass is shown! message (Figure 33 g)) including vaccination data, otherwise the message Failed (Figure 33 f)) and the reason for the failure.

- **Global ID:** This option displays the patient's Global ID QR code and hashcode (Figure 33 d)) to optimize care.

- **Profile:** This selection shows all the data of the patient's profile (Figure 33 e)), and serves for the patient to know his data and verify that they are correct.

5.2 Scalability Evaluation

Scenario evaluation has been used for several works related to fog computing, and health (RAHMANI et al., 2018). The evaluation is made by measuring the results of scalability and privacy of the proposed architecture, including analysis of scenarios with the use of architecture.

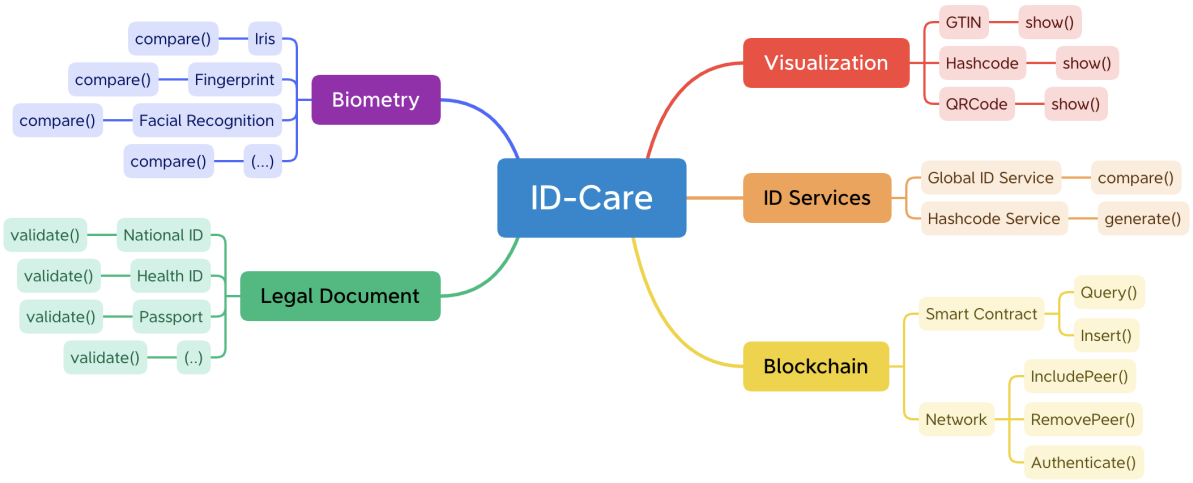

Figure 26 – Taxonomy of ID-Care Model Services.

For the evaluation of this work, a vaccination use case is proposed where health data from patients around the world distributed in a continental geographic space are included. This scenario simulates an integrated global COVID-19 vaccination campaign, being emphasized by a peak in the vaccination process. It aims to verify if the architecture meets the requirements and addresses the challenges of the studied care architecture.

5.2.1 Vaccination scenario

This scenario comprises some assumptions. It is the year 2021, and the COVID-19 pandemic must be brought under control quickly. Due to the risk of the arrival of new variants of SARS-CoV-2, a consortium of countries decided to invest in the Fog-Care solution to enable faster decision-making through data from the vaccination process around the world. This decision could be, for example, to donate vaccines to certain countries, invest in booster doses, propose strategies to block or restrict access, or even provide faster access to global health data for scientists worldwide.

Thus, the consortium of countries initially prepared a vaccination plan covering three geographically dispersed countries: Brazil, the USA, and England. In that case, each country will try to prevent more deaths by vaccinating as many people as possible. The requirements for this process are to support globally unique patient identification, data privacy, and scalability. After a mutual meeting, the countries decided to implement a solution based on the Fog-Care architecture, and the aim is to support vaccination worldwide, supporting the values of the countries with the highest peaks (10 million/day) in COVID-19 Pandemic vaccination, as can be seen in Figure 27, Our World in Data (RITCHIE et al., 2020) data source. India has peaked at 10 million vaccinations, while the United States and Brazil have nearly 4 million.

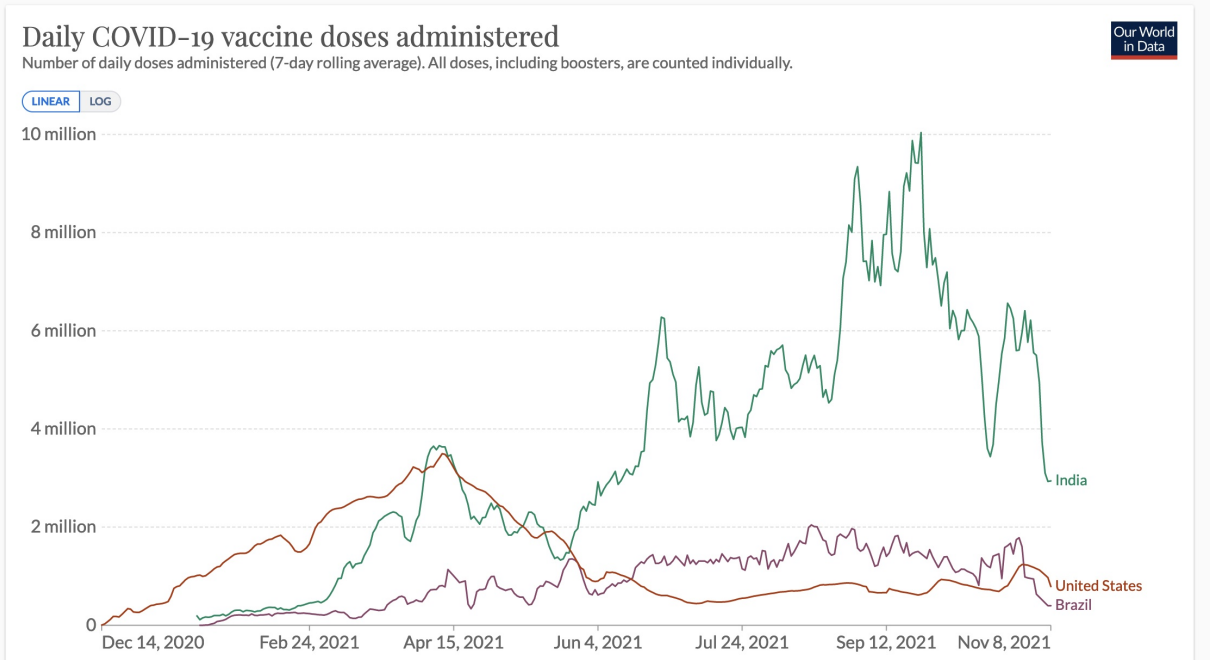

Figure 27 – Moving Average of 7 days vaccination in US, India, and Brazil. Source: (RITCHIE et al., 2020).

5.2.2 Metrics

The assessment is based on a performance benchmark testing software called Hyperledger Caliper[1], which is a performance tool maintained by the Hyperledger Foundation that supports case testing of custom use to test various blockchain networks such as Hyperledger Fabric and Ethereal. The calibrator can generate reports including various performance metrics such as latency, throughput, and send rate. Caliper components include a benchmark and network settings, and a report. The choice of Caliper is due to the fact that it is currently an established reference set for a large number of existing blockchain technologies such as Ethereum, Hyperledger Fabric, Besu, Burrow, Iroha, Sawtooth, and FISCO BCOS.

The following Caliper configuration parameters were used (HYPERLEDGER BLOCKCHAIN PERFORMANCE METRICS, 2021):

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

The worker number represents the number of worker processes to use to run the workload, rounds txNumber is the number of transactions the Caliper should send during the round, and

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

rounds off the rateControl type, which represents the desired rate of sending transactions. When we use a fixed rate, it means that Caliper will send incoming transactions at a fixed interval which is specified as transactions per second. In this case 10 to 100 at a time.

The following metrics were measured (HYPERLEDGER BLOCKCHAIN PERFORMANCE METRICS, 2021):

- 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 smart contract function 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, latency is the difference, in seconds, between a transaction submitted and finished considering the network.

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 ability to send transactions to the blockchain. Total time is measured in seconds. The metric only considers the rate at which requests were sent to the blockchain without considering the time taken to get a response.

Throughput is described as follows:

$$Throughput = TotalCommittedTransactions/TotalTime$$

The Throughput measure differs from the Shipping Rate when considering the actual execution capacity. While the send rate measures the ability to send code to run on the blockchain, the throughput measures the ability to execute it. In other words, this metric also measures the rate at which the blockchain can respond to requests. For example, the blockchain can send 50 transactions per second (Send Rate), but only process 25 transactions per second (Throughput).

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

The main configuration of Caliper consists of describing the network in a file called network-config.yaml and defining the general configuration. The network configuration file contains the configuration of Organizations (FirstHospital and SecondHospital), channels (fogcarechannel),

and peers involved, and the general configuration file stores all the settings related to the workload. In this case, parameters were chosen for a fixed load of 10 to 100 transactions per second per execution, limiting a total of 500 total transactions.

To better understand the results, the average latency, minimum latency, maximum latency, sending rate, and throughput metrics are divided into write operations and read operations. Write operations save data on the blockchain and read operations read data. In the previous definition of the Fog-Care smart contract implementation, the best representative functions were selected, which are ReadVaccination() and ReadPerson() to measure the read operations and the CreatePerson() and CreateVaccitation() functions to measure the writing on the blockchain.

The interquartile range (IQR) is also considered to treat outliers. It is a measure of variability based on dividing a dataset into quartiles. The values dividing each part are called the first, second, and third quartiles, denoted by Q1, Q2, and Q3, respectively.

- Q1 is the "middle" value in the first half of the dataset sorted by rank.
- Q2 is the median value in the set.
- Q3 is the "middle" value in the second half of the sorted dataset.

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 order peer and two anchor peers. These computers were simulated in a virtual environment using Amazon Web Service - AWS. Orderer was hosted in Brazil (São Paulo), and the pairs named FirstHospital and SecondHospital were hosted in the US (Northern Virginia) and UK (London). The machines used were of type T2.Micro (22) to standardize to a cheap and widely known standard specification. It is also considered the highest vaccination rate, 7-day moving average in India, consisting of 10 million vaccinations per day (Figure 27).

The goal of the scalability evaluation of the Fog-Care model is to verify if the model supports a large number of computers from geographically distributed locations, respecting the latency issues that can occur supporting real-time operations even with several computers connected in the analyzed scenarios.

5.3 Unique Identity and Privacy Evaluation

We proposed a use case of a global vaccination campaign against the COVID-19 virus, which simulates a scenario in which anyone in the world can be vaccinated in any country that participates in the ID-Care initiative. The World Health Organization recognizes and suggests policy considerations for implementing a risk-based approach to international travel in the context of COVID-19 (TECHNICAL CONSIDERATIONS FOR IMPLEMENTING A RISK-BASED APPROACH TO INTERNATIONAL TRAVEL IN THE CONTEXT OF COVID-19, 2021). Health data on patients around the world are distributed across a continental geographic space. This simulation of a global vaccination scenario aims to verify that the proposed model meets the requirements to address the challenges of health data integration using a unique global health identification strategy. For this, we describe this scenario in detail, the implementation of each layer (ID Services, Legal Document, Biometrics, Blockchain, ID Services, Visualization), and the development of the mobile application prototype for people to use.

5.3.1 Global Data Sharing Scenario

To evaluate the model, a use case is proposed: a global vaccination campaign against the COVID-19 virus. This simulates the scenario where the citizen of any country can be vaccinated in any country that participates in the ID-Care initiative. For this, we have defined some important steps necessary to achieve this goal:

- Select the countries participating in the proposed scenario
- Collect your relevant tourism and population data
- Collect COVID-19 Vaccination Data
- Define possible tourist mobility use cases
- Analyze the proposed scenario suggesting possible protective sanitary measures

To illustrate a use case, suppose a foreign patient arrives at the hospital to be vaccinated. Healthcare professionals ask the patient if he/she has the ID-Care application. The patient shows the QR Code on his cell phone. From there, the ID-Care app already detects all the vaccines taken in your country of origin and the possible incompatibilities and recommended deadlines for your age and health condition. The process can be similar to registering or verifying a patient. When entering patient information in the ID-Care registration application, it is verified that the patient does not yet have a global identification. Then, the application generates a new ID associated with that patient and authorization for the first access by the application. Data validation occurs through documents and/or biometric data that are entered according to the information provided by the patient.

The main idea is to evaluate if a patient could be uniquely and globally identified without issues and restrictions in a healthcare application. The authorization process considered the context of the country and the profile of the patient vaccination data stored in the blockchain. Furthermore, privacy in healthcare has several restrictions and limitations regarding functions and access to electronic health records and health assets. The evaluation objectives verify whether the Fog-Care model increase patient privacy and meets the requirements and healthcare limitations identified in the literature.

6 RESULTS AND DISCUSSION

This chapter presents the results and discussion of the Fog-Care proposed model. It is divided into the section Fog-Care Results, where the results are presented; section Fog-Care Discussion, where the analysis and discussion of the model are presented; and the section Future Directions, where some trends based on results are presented.

6.1 Fog-Care Results

6.1.1 Scalability Evaluation Results

All proposed metrics results were considered an average of 5 runs of the same smart contract code. After this procedure, the outliers were removed using the IQR method. The results were finally grouped into read operations and write operations to better understand the processes.

In Figure 28, 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 is expected due to network traffic of a wide geographically dispersed network.

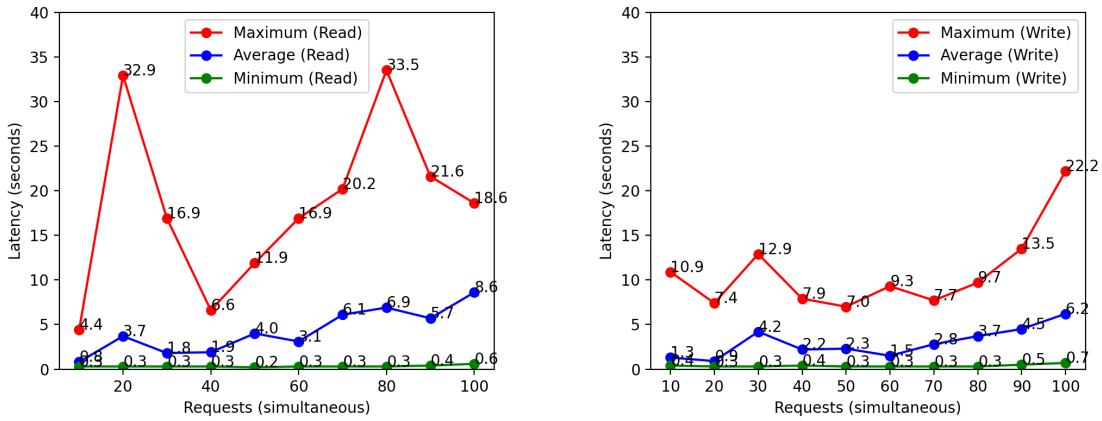

Figure 28 – Minimum, Maximum, and Average Latency - Read and Write Operations.

The latency, maximum, average, and minimum latency for blockchain write operations relative to transactions per second are shown. Minimum values are low (above 1 second), and average latency grows consistently with maximum latency.

In Figure 29, the sending rate for blockchain is shown. It grows rapidly as an exponential function on both read and write operations. In Figure 30, the throughput for reading operations consistently grows up to 80 requests, where it reverses motion, causing some randomness. Likewise, the throughput for write operations increases up to 70 requests, where it reverses the movement in behavior similar to that of the read operation.

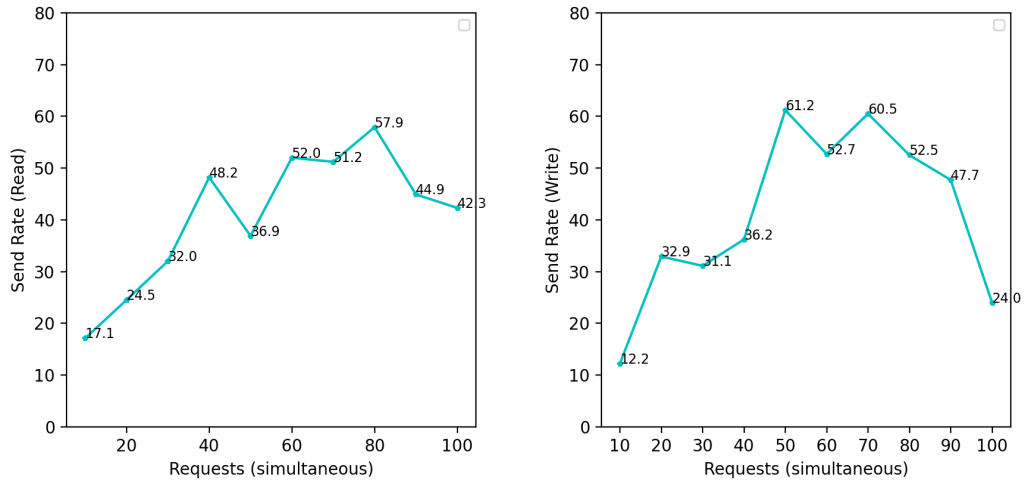

Figure 29 – Send Rate - Read and Write Operations.

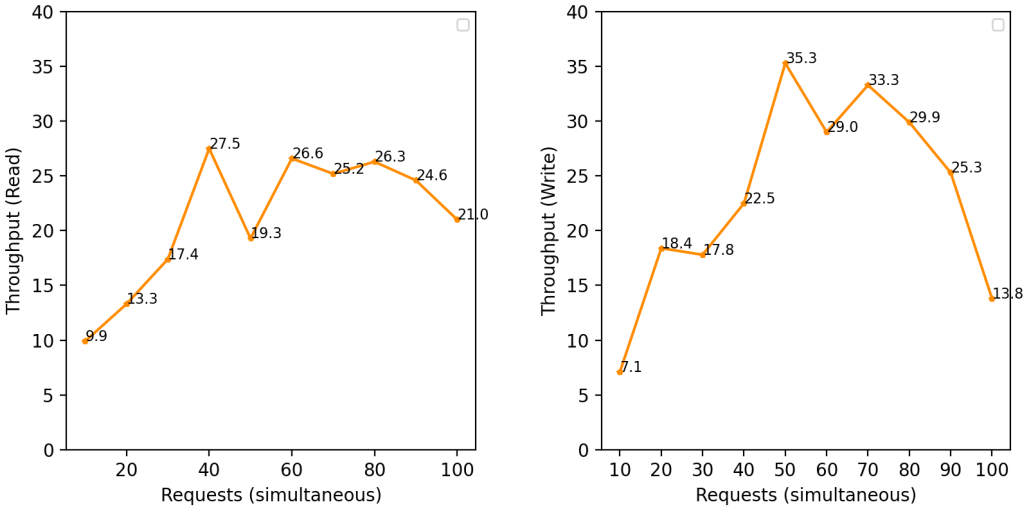

Figure 30 – Throughput - Read and Write Operations.

In the results, an effective sending peak of 61.2 transactions per second was reached, or 5,287,680 per day, considering 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 pairs. The maximum peak of vaccination was in India, with 10 million vaccinations per day, a moving average of 7 days. Even considering only three pairs of low-cost hardware it was possible to obtain good performance results considering that using Fog-Care architecture in a heavily populated country would be multiple fog nodes such as 1 per state and better hardware too. Considering the linear scalability in the latency, send rate, and throughput results, a blockchain with a peer per state will undoubtedly handle a higher workload and more than 10 million transactions per day.

6.1.2 Unique Identity and Privacy Results

The results of implementing the proposed scenario are presented as follows. A case study was done considering pre-pandemic tourism numbers and current vaccination rates to show the effectiveness of the app. For this case study, some scenarios were defined.

For the vaccination scenario, we defined five steps: select the participating countries of the proposed scenario, collect relevant tourism and population data, collect COVID-19 vaccination data, define possible tourism mobility use cases and analyze the proposed scenario suggesting possible protective sanitary measures. These steps are described below:

1. **Select the countries participating in the proposed scenario:** We selected the five most visited countries in 2019, the year before the start of the COVID-19 pandemic. The selected countries are France, Spain, the United States of America, China, and Italy (Table 15). The objective of selecting these countries is justified by the need to choose a group of countries due to their tourist attractiveness, which would need to make an integrated global vaccination plan to deal with the number of geographically very dispersed visitors. For this, we created a map containing the main population of millions of people (Figure 31).

Table 15 – Top 5 foreign tourism in 2019.

Place	Country	Tourists	Population
1º	France	89.4 million	67.0 million
2º	Spain	83.7 million	46.9 million
3º	USA	79.3 million	328,329.95 million
4º	China	65.7 million	1,433,783,686 billion
5º	Italy	64.5 million	60.4 million

2. **Collect your relevant tourism and population data:** The next step is to collect official inbound tourism data from different countries. We carefully chose the number of tourists in 2019, before the pandemic, to represent the regular tourist demand in these countries

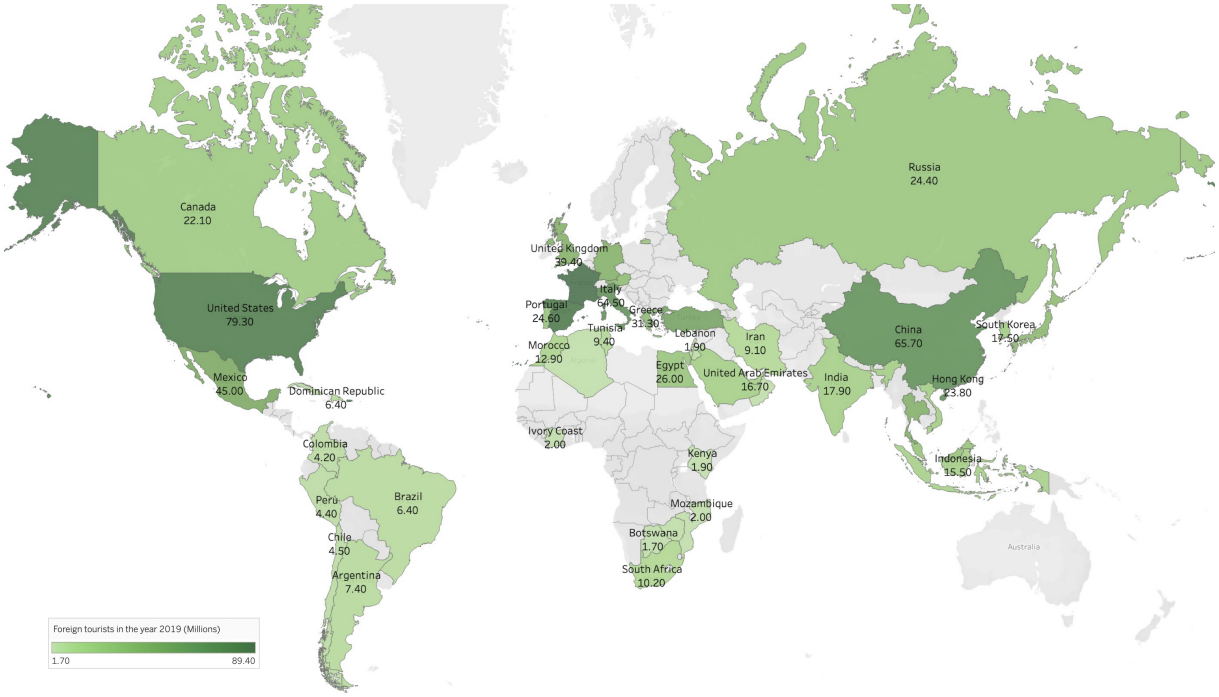

Figure 31 – Number of foreign tourists by country in 2019 (Millions).

Table 16 – International Tourism Revenue in 2019 / 2020.

Country	Income 2019	Income 2020	Difference.
France	70.78 billion	35.96 billion	34.82 billion
Spain	31.59 billion	20.46 billion	11.13 billion
USA	239.45 billion	84.2 billion	155.25 billion
China	27.7 billion*	13.3 billion*	14.4 billion
Italy	51.91 billion	25.4 billion	26.51 billion
Total	**421.43 billion**	**179.32 billion**	**242.11 billion**

(ORGANIZATION, 2020). Regardless of these countries, we can see the huge demand for a global health identification ID by analyzing the number of tourists around the world in millions of foreign visitors (Figure 31) and the international income of these countries in 2019 (before the pandemic) and 2020 (after the pandemic) seen in Table 16. The numbers inside the asterisk are estimates. For tourism and population data, we use Eurostat (EU POPULATION UP TO OVER 513 MILLION ON 1 JANUARY 2019, 2019) (POPULATION CHANGE - DEMOGRAPHIC BALANCE AND CRUDE RATES AT NATIONAL LEVEL, 2022) for Europe, World Data (CHINA POPULATION 2019, 2019) (CHINA POPULATION 2022, 2022) for China and Statista (RESIDENT POPULATION OF THE UNITED STATES FROM 1980 TO 2021, 2019), and (U.S. POPULATION ESTIMATED AT 332,403,650 ON JAN. 1, 2022, 2022) for the US. Revenue data comes from the World Bank (INTERNATIONAL TOURISM, RECEIPTS , CURRENT US$). These sources are based on official figures from the respective governments, excluding

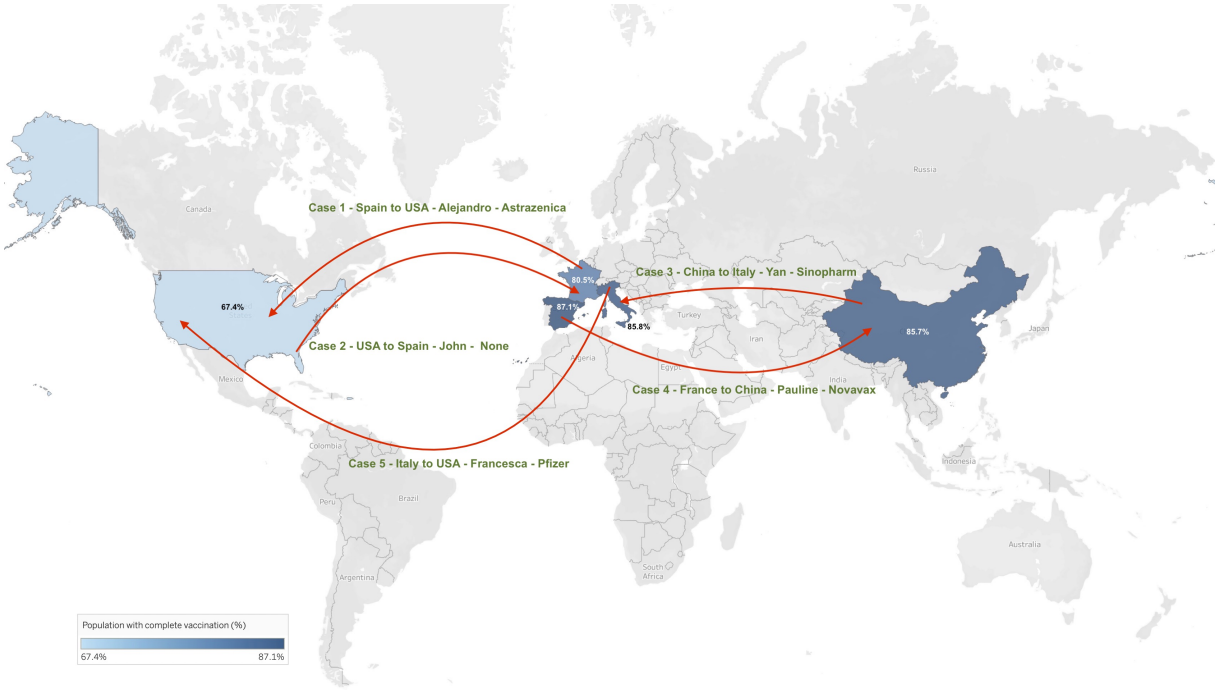

Figure 32 – Vaccination use cases.

China.

3. **Gathering COVID-19 Vaccination Data:** For the collection of vaccination data, the Oxford University website Our World of Data (NUMBER OF PEOPLE VACCINATED AGAINST COVID-19 AUGUST 31, 2022, 2022) is a world reference as it contains a huge compilation of data from vaccination in various formats, from text, maps and graphics, and is known for its up-to-date COVID-19 vaccination data (MATHIEU et al., 2021). We have included vaccination data through August 31, 2022, as seen in the 17 and 17 Tables. We also consider that each country has chosen a different brand of vaccines. In addition, there are some differences in the time and number of doses administered (Table 19).

Table 17 – Percentage of vaccination by country until August 2022.

Country	Population	Completed	Only 1º Dose	% Completed
France	67.6 million	54.5 million	1.5 million	80.5%
Spain	47.3 million	41.2 million	0.6 million	87.1%
USA	332.4 million	224.1 million	38.7 million	67.4%
China	1.4 billion	1.2 billion	33.1 million	85.7%
Italy	59.2 million	50.8 million	2.8 million	85.8%

4. **Define possible tourism mobility use cases:** To exemplify the benefits of the proposed work, we selected five common tourism routes and visitor profiles grouped as use cases 1 to 5. These are graphically shown in Figure 32, and are described as follows:

Table 18 – Percentile of delivered vaccines by country.

Vaccine	France	Spain	United States	China	Italy
AstraZenica	4.98%	15.94%	0%	0%	13.08%
Janssen	1.79%	9.97%	3.86%	0%	1.59%
Moderna	26.41%	20.42%	37.28%	0%	17.51%
Novavax	1.28%	0%	0%	0%	0.72%
Pfizer	65.54%	53.67%	58.77%	0%	67.09%
Sinopharm	0%	0%	0%	0.13%	0%
Unknown	0%	0%	0.08%	99.87%	0%

Table 19 – Delivered vaccines by type.

Vaccine	France	Spain	United States	China	Italy
AstraZenica	10.3 million	26.4 million	0	0	18,62 million
Janssen	3,7 million	16.5 million	31,1 million	0	2.2 million
Moderna	54.9 million	33.9 million	300,8 million	0	24.9 million
Novavax	2,6 million	0	0	0	1.0 million
Pfizer	136.3 million	89.1 million	474,1 million	0	95.5 million
Sinopharm	0	0	0	5,0 million	0
Unknown	0	0	0,6 million	3,7 billion	0

- **Case 1:** Alejandro is a 32-years-old Spaniard who is traveling from Spain to the USA. He was vaccinated with AstraZeneca 30 days ago.
- **Case 2:** John is a 22-years-old American traveling from the USA to Spain. He was not vaccinated.
- **Case 3:** Yan is a 62-years-old Chinese man traveling from China to Italy. He was vaccinated with Sinopharm 18 days ago.
- **Case 4:** Paulina is a 35-year-old French woman traveling from France to China. She was vaccinated with Novavax 35 days ago.
- **Case 5:** Francesca is an Italian woman who is traveling from Italy to the USA. She was vaccinated with Pfizer 20 days ago.

5. **Analyze the proposed scenario and automatically suggest possible protective sanitary measures according to each case:** In this proposed scenario, a border control measure can be applied by the sanitary authority. For example, upon arrival of a tourist, there may be 3 standard recommendations after reviewing the global tourist identification information provided by the Global ID Vaccination software: 1 - accept traveler entry without restrictions, 2 - deny traveler entry, or 3 - apply a requirement such as giving a booster dose of the COVID-19 vaccine or another preventive health measure, to accept the traveler's entry into the country. Looking at case 1, Alejandro is trying to enter the US and is vaccinated with AstraZeneca. As there is no AstraZeneca vaccine in the US (Table 19), the Global ID software suggests that the US health authority give a booster

dose of Pfizer and then accept the traveler. Case 2, John, a young American, is arriving in Spain. Global ID software recognizes John as unvaccinated against COVID-19. Thus, the software suggests denying entry into the country. Case 3 is about Yan, an old Chinese man arriving in Italy. The Global ID software detects his old age and recognizes that he is vaccinated with Sinopharm. The software suggests a booster shot of Pfizer or Moderna, vaccines available in Italy. Case 4 is related to Paulina, a French woman going to China. She was vaccinated with Novavax. The Global ID software suggests that the Chinese health authority give a booster dose of Sinopharm and accept the traveler due to Novavax still being given to a low percentage of people worldwide. Case 5 is about Francesca, an Italian vaccinated with Pfizer and traveling to the US. The Global ID software recommends accepting the traveler without restrictions, as he is vaccinated with Pfizer, a vaccine recognized in the USA. Considering the scenario in which the Id-Care model is used, and the vaccine was ready for use, approximately 80% of all arriving tourists managed to enter the analyzed countries.

Furthermore, unlike related works, we demonstrate that this proposed model is viable for implementation and can benefit healthcare services due to its standardization and usefulness in a healthcare environment with a large number of foreign visitors from several countries and supports privacy, scalability, and unique identification. Another differential is that this model supports any technology used for identification in the country of origin, from national identification numbers to patient biometric data.

6.2 Fog-Care Discussion

This section discusses the performance result of scalability tests and the privacy and unique identification scenarios on the Fog-Care model.

6.2.1 Scalability Discussion

In the scalability evaluation, all results were considered from an average of 5 executions of the same smart contract code. Read and Write Methods. After this procedure, outliers were removed using the Interquartile Range - IQR method described in the Materials and Methods section. They have also been grouped into Read Operations and Write Operations.

Transaction throughput and latency metrics are the two most relevant blockchain performance metrics and are not always satisfactory in recent popular blockchain applications (ZHENG et al., 2018)

The result of the latency performance evaluation is considered satisfactory for this project's scope. The minimum read and write latency is less than 1 second, indicating that under ideal conditions, scalability is possible. From about 60 transaction requests, the transaction per second starts to grow rapidly.

One of the most important metrics is latency. The result shows an increasing result with a suitable support delay of up to 100 transactions per second. It can be noted that due to the network traffic of a wide geographically dispersed network, a few small seconds are expected. Considering these results, it can be inferred by an exponential distribution that the Fog-Care Architecture can support vaccination of about 22 shots per second, or more than 2,000,000 shots per day, in this use case.

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

As the size of the blockchain increases, the processing power, storage, and throughput also need to increase, or all nodes will not be able to process blocks at some point (ROMASHKOVA; KOMAROV; OMETOV, 2021). The limitation of results considers three peers on the blockchain, with 1 being the requester on a standard T2.Micro AWS machine. This type of virtual machine is very basic and focuses on low cost with reasonable computer performance. Scalability support can be done by adding at least 2 more peers and allocating better CPU final memory virtual machines, but the value of 1 peer/fog node per state is optimal. Some limitations of blockchain testing should be considered because the testing environment can drastically affect the results. Some examples are the geographic distribution of the nodes, if the nodes and peers are dispersed or not in a local environment, the type of hardware of the 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 in that it used a broad geographic approach (Brazil, the United States, and the United Kingdom), considering testing the blockchain not in a local environment but in a simulated use case of global vaccination. In this case, latency, throughput, and send rate are strongly affected by the distance between the peers and the requestor. Each transaction operation must be accepted and replicated by computers on different continents, compared to related jobs that usually run tests on a single machine or a small local network. Despite the use of several fog nodes to improve scalability, the results obtained with these tests can be compared with related future work, as the use of a standard parameter such as the number of rounds, rate control, and total transactions, among others provided by the Caliper tool, allows you to emulate the environment and test alternative configurations. Several approaches can be used to improve scalability, such as increasing the block size, reducing the transaction size, or reducing the number of transactions processed by (XIE et al., 2019) nodes. The alternative of increasing the block size includes more transactions per block to increase throughput, but this approach requires more nodes to process the data and causes more delay due to the propagation process. Reducing transaction size by increasing the number of transactions per block is also an alternative, reducing the digital signature required per block. The

last option may be to reduce the transactions processed by the nodes, which can be achieved by using off-chain transactions, increasing throughput.

6.2.2 Unique Identity and Privacy Discussion

The proposed model supports several functionalities to implement the unique global identification of patients focusing on healthcare. In the case of vaccination scenario results, the use of the Global ID software can combine historical traveler profile data with global vaccination data and help the health authority of participating countries to establish a dynamic decision-making strategy based on knowledge of global information on vaccines and people to decide on public health policies.

These differential Global ID results come from the model's unique features, such as support for smart contracts and a decentralized network. While some related works have implemented controllable privacy and security, they do not support decentralized data sharing and traceability. This lack of recourse affects record longevity gaps and privacy/security concerns in the current literature.

Another important challenge in the literature is the support of unique health records. All related works studied do not implement any form of the uniqueness of identification considering a global scope of patients. The global id suggested by this proposed work can provide quick, accurate, and secure identification of a person associated with their health data. In the scenario studied, tourists were quickly identified by their global IDs and with the knowledge of related health data, the speed of service was instantaneous, which proposes the reduction of several costs and the possibility of adopting necessary measures of sanitary protection.

With the implementation of a global ID, some issues need to be resolved. Person identification documents vary in type, format, and size of numbers. Related works do not provide any strategy for dealing with different documents coming from different places. Some countries use a national identity and individual taxpayer numbers, among others. The biometrics technology involved with this identification, such as fingerprint or facial recognition, must be considered as it provides an important level of security and unique identification. Most related works support some kind of biometric identification, but unlike this proposal, it only supports a single biometric, usually fingerprint or iris recognition. The proposed model implements the support of several biometric technologies simultaneously and together with identification document numbers, forming a unique hashcode and the support of QR Codes. An important issue found in the literature is the lack of standardization or compatibility with norms. None of the related works support a global standard. The proposed model was developed to support the EPC Global Standard GS1, which is widely known. We implement all code numbers according to GS1 guidelines, including the proposed hashcode validation code. The hashcodes generated in the scenario are examples of this pattern applied.

A relevant piece of information considered was the number of tourists in 2019 among the top

5 who arrived in the countries. This number ranges from 64.5 million (Italy, fifth) to 89.4 million (France, first). It implies an enormous potential need for vaccination for foreign tourists. In the proposed scenario, we can see that different brands of vaccines are applied to people according to each country. Pfizer leads in France, Spain, the United States, and Italy. Janssen was the only single-shot vaccine and could benefit, but only Italy and Spain were applied.

The prototype results guarantee the feasibility of the applications. Some data, such as the Country, Doc Type, Doc Number, Biological Data, Bio Number, Date of Birth, and Validator fields, successfully allowed patients' enrollment from different countries.

These fields only contain immutable data such as date of birth and country of origin. The field validator ensures that all other fields are with integrity. Using blockchain smart contracts helps with data reliability, privacy, and security. Support for GS1 standards is another differentiator from related work.

Using a blockchain network and an open-source SHA512 algorithm to encrypt the original hashcode hides sensitive information from an unauthorized person while creating a unique, privacy-supported generated number.

The model implemented a QR code generated from the GTIN number for general use and visualization. This allows for a better user interface for patients and healthcare professionals, who just need a smartphone with a camera and an internet connection to use features quickly. The set of unique features, such as document traceability and the support of model biometric technologies, differs from the standard approaches in related works.

Considering the proposed scenario of vaccination of incoming tourists from the 5 main tourist countries in the world, by proximity, in Europe, the average of the three most visited countries (France, Spain, and Italy) is 79.2 million tourists, compared to the USA, the figure of 79.3 million visitors is similar, and China with 65.7 million visitors, this proposed work has the potential to contribute to the implementation of health data sharing strategies on a global scale. A large number of visitors and the implementation of this Global ID model on a global scale has the potential to reduce costs, time, and efforts to help control and mitigate the effects of threats such as possible pandemics or even any disease that depends on vaccination or any other scenario. global sharing of health data.

To summarize, considering the results, using Fog-Care architecture can benefit the healthcare services supporting the standards for the global identification of assets and sharing of geographically distributed information considering scalability, latency, and privacy issues. Using a standard global identification strategy for patients is a differential in the literature, addressing the issues of dealing with quick identification in an integrated world-class healthcare strategy. The use of blockchain technology considered privacy issues, including integrity, transparency, and traceability of all procedures and processes. Sharing healthcare data around the world using the Fog-Care model can benefit the healthcare sector because of the ability to integrate all the stakeholders in a trusted and decentralized environment. The scalability results demonstrate the potential of blockchain networks associated with fog computing. We published two arti-

cles regarding this work: Fog computing in health: A systematic literature review (Springer Health and Technology) and A Fog and Blockchain Software Architecture for a Global Scale Vaccination Strategy (IEEE Access). A third article, ID-Care: A Global Scale Identification Model for Sharing Healthcare Data was submitted to IEEE Access, and it is under review. For future work, we intend to implement Artificial Intelligence features like Machine Learning in the Fog-Care Model, such as pandemic risk analyses, profile context detection, and integration with other future healthcare data.

6.3 Future Directions

Fog computing is a trend in a cloud computing environment. Increasingly, applications are cloud intensive. While hardware has dramatically increased its capacity, healthcare applications need the information to be obtained as quickly as possible. Fog computing can substantially help solve this problem. Soon, artificial intelligence services such as filtering, data mining, and data prediction will be part of the daily routine of hospitals. In addition, services will be available to patients' homes outdoors through increased mobility of the devices and the improvement of their communication technologies, allowing the healthcare professional or medical center to be anywhere in the world at any time.

7 CONCLUSION

Technology is considered a great tool allied to health. In the current scientific environment, many good related works and available computing technologies such as cloud computing, fog, and blockchain can potentially be applied to healthcare. However, many of these works discuss challenges and performance issues considering small local settings, such as a single hospital or a group in a centralized, local area. With the arrival of the COVID-19 pandemic, many scientists and organizations are focusing on global 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. A software prototype was implemented successfully, evaluating a hypothetical scenario where an integrated global vaccination campaign is adopted, simulating a solution approach based on integrated blockchain and fog computing technologies. From the results, it can be concluded the following contributions: (1) in terms of scalability, it is crucial to add more fog nodes, such as one per state, to support the increased transaction demand on a blockchain with dispersed wide nodes. (2) the average transaction latency is just a few seconds; even 100 concurrent 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 addressed globally with blockchain by writing smart contracts representing these features. (5) The lack of mutation and integrity of the ledger in a global healthcare environment can increase and help to protect patient privacy. (6) unique and global identification of people and resources is required and can be done with GS1 Standards accordingly. (7) It is possible to implement better policy decision-making and a more globally coordinated health strategy with faster and earlier results available. For future work, we intend to evaluate the architecture with the inclusion of several changes. First, an increasing number of pairs, such as 3, 5, 7, and 9. To compare the results, a different network with more Fog nodes, different smart contract benchmark parameters, and other virtual machine configurations. We also implemented a globally unique id for patients in a global vaccination strategy scenario. The results showed that it is possible to integrate biometrics technology with feasibility in a global environment. For future work, we will implement more features, such as a web application to support global information for governments and health universities to support research, and machine learning prediction considering the study of privacy and security issues involved. Another contribution was publishing two articles based on this work: Fog computing in health: A systematic literature review (Springer Health and Technology), and A Fog and Blockchain Software Architecture for a Global Scale Vaccination Strategy (IEEE Access). A third article, ID-Care: A Global Scale Identification Model for Sharing Healthcare Data was submitted to IEEE Access Journal and is currently under review.

REFERENCES

ABIDEEN, Z. U.; SHAH, M. A. An iot based robust healthcare model for continuous health monitoring. In: AUTOMATION AND COMPUTING (ICAC), 2017 23RD INTERNATIONAL CONFERENCE ON, 2017. **Anais...** [S.l.: s.n.], 2017. p. 1–6.

AGBO, C. C.; MAHMOUD, Q. H.; EKLUND, J. M. Blockchain technology in healthcare: a systematic review. In: HEALTHCARE, 2019. **Anais...** [S.l.: s.n.], 2019. v. 7, n. 2, p. 56.

AHMAD, M. et al. Health fog: a novel framework for health and wellness applications. **The Journal of Supercomputing**, [S.l.], v. 72, n. 10, p. 3677–3695, 2016.

AHMADI, Z. et al. Fog-based healthcare systems: a systematic review. **Multimedia Tools and Applications**, [S.l.], p. 1–40, 2021.

AKRIVOPOULOS, O. et al. On the deployment of healthcare applications over fog computing infrastructure. In: COMPUTER SOFTWARE AND APPLICATIONS CONFERENCE (COMPSAC), 2017 IEEE 41ST ANNUAL, 2017. **Anais...** [S.l.: s.n.], 2017. v. 2, p. 288–293.

AL HAMID, H. A. et al. A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. **IEEE Access**, [S.l.], v. 5, p. 22313–22328, 2017.

ALAM, M. G. R. et al. Edge-of-things computing framework for cost-effective provisioning of healthcare data. **Journal of Parallel and Distributed Computing**, [S.l.], v. 123, p. 54–60, 2019.

ALHADHRAMI, Z. et al. Introducing blockchains for healthcare. In: ICECTA), 2017., 2017. **Anais...** [S.l.: s.n.], 2017. p. 1–4.

ALI, S.; GHAZAL, M. Real-time heart attack mobile detection service (rhamds): an iot use case for software defined networks. In: ELECTRICAL AND COMPUTER ENGINEERING (CCECE), 2017 IEEE 30TH CANADIAN CONFERENCE ON, 2017. **Anais...** [S.l.: s.n.], 2017. p. 1–6.

ALSHIKY, A. M.; BUHARI, S. M.; BARNAWI, A. Ehr attribute-based access control (abac) for fog computing environment. **Computer Science & Information Technology**, [S.l.], p. 87, 2017.

AMAZON ec2 t2 instances. Accessed: 2019-08-15, https://aws.amazon.com/ec2/instance-types/t2/.

ANDRIOPOULOU, F.; DAGIUKLAS, T.; ORPHANOUDAKIS, T. Integrating iot and fog computing for healthcare service delivery. In: **Components and services for iot platforms**: paving the way for iot standards. Cham: Springer International Publishing, 2017. p. 213–32.

AWOTUNDE, J. B.; BHOI, A. K.; BARSOCCHI, P. Hybrid cloud/fog environment for healthcare: an exploratory study, opportunities, challenges, and future prospects. **Hybrid Artificial Intelligence and IoT in Healthcare**, [S.l.], p. 1–20, 2021.

AZIMI, I. et al. Medical warning system based on internet of things using fog computing. In: BIG DATA AND INFORMATION SECURITY (IWBIS), INTERNATIONAL WORKSHOP ON, 2016. **Anais...** [S.l.: s.n.], 2016. p. 19–24.

AZIMI, I. et al. Hich: hierarchical fog-assisted computing architecture for healthcare iot. **ACM Transactions on Embedded Computing Systems (TECS)**, [S.l.], v. 16, n. 5s, p. 174, 2017.

BARIK, R. et al. Fog2fog: augmenting scalability in fog computing for health gis systems. In: IEEE/ACM INTERNATIONAL CONFERENCE ON CONNECTED HEALTH: APPLICATIONS, SYSTEMS AND ENGINEERING TECHNOLOGIES (CHASE), 2017., 2017. **Anais...** [S.l.: s.n.], 2017. p. 241–242.

BARIK, R. K. et al. Geofog4health: a fog-based sdi framework for geospatial health big data analysis. **Journal of Ambient Intelligence and Humanized Computing**, [S.l.], p. 1–17, 2018.

BARIK, R. K. et al. Mist data: leveraging mist computing for secure and scalable architecture for smart and connected health. **Procedia Computer Science**, [S.l.], v. 125, p. 647–653, 2018.

BHATIA, M.; SOOD, S. K. Exploring temporal analytics in fog-cloud architecture for smart office healthcare. **Mobile Networks and Applications**, [S.l.], p. 1–19, 2018.

BIOLCHINI, J. et al. Systematic review in software engineering. **System Engineering and Computer Science Department COPPE/UFRJ, Technical Report ES**, [S.l.], v. 679, n. 05, p. 45, 2005.

BLAIR, G. S. et al. Interoperability in complex distributed systems. In: INTERNATIONAL SCHOOL ON FORMAL METHODS FOR THE DESIGN OF COMPUTER, COMMUNICATION AND SOFTWARE SYSTEMS, 2011. **Anais...** [S.l.: s.n.], 2011. p. 1–26.

BONDI, A. B. Characteristics of scalability and their impact on performance. In: SOFTWARE AND PERFORMANCE, 2., 2000. **Proceedings...** [S.l.: s.n.], 2000. p. 195–203.

BONOMI et al. Fog computing and its role in the internet of things. In: MCC WORKSHOP MOBILE CLOUD COMPUT., 2012. **Anais...** New York, 2012. p. 13–16.

BONOMI, F. et al. Fog computing: a platform for internet of things and analytics. In: _____. **Big data and internet of things**: a roadmap for smart environments. Switzerland: Springer International Publishing, 2014. p. 169–186.

BUDGEN, D.; BRERETON, P. Performing systematic literature reviews in software engineering. In: SOFTWARE ENGINEERING, 28., 2006. **Proceedings...** [S.l.: s.n.], 2006. p. 1051–1052.

BUYYA, R. et al. Cloud computing and emerging it platforms: vision, hype, and reality for delivering computing as the 5th utility. **Future Generation computer systems**, [S.l.], v. 25, n. 6, p. 599–616, 2009.

CAO, Y. et al. Distributed analytics and edge intelligence: pervasive health monitoring at the era of fog computing. In: WORKSHOP ON MOBILE BIG DATA, 2015., 2015. **Proceedings...** [S.l.: s.n.], 2015. p. 43–48.

CERINA, L. et al. A fog-computing architecture for preventive healthcare and assisted living in smart ambients. In: RESEARCH AND TECHNOLOGIES FOR SOCIETY AND INDUSTRY (RTSI), 2017 IEEE 3RD INTERNATIONAL FORUM ON, 2017. **Anais...** [S.l.: s.n.], 2017. p. 1–6.

CHECK digit calculator. how to calculate a digit check manually. Accessed: 2022-07-13, https://www.gs1us.org/DesktopModules/Bring2mind/DMX/Download.aspx?EntryId=729.

CHINA population 2019. Accessed: 2022-09-06, https://www.worldometers.info/world-population/china-population/.

CHINA population 2022. Accessed: 2022-09-06, https://www.worldometers.info/world-population/china-population/.

CONOSCENTI, M.; VETRO, A.; DE MARTIN, J. C. Blockchain for the internet of things: a systematic literature review. In: IEEE/ACS 13TH INTERNATIONAL CONFERENCE OF COMPUTER SYSTEMS AND APPLICATIONS (AICCSA), 2016., 2016. **Anais...** [S.l.: s.n.], 2016. p. 1–6.

COSTA, H. J. D. M. et al. A fog and blockchain software architecture for a global scale vaccination strategy. **IEEE Access**, [S.l.], v. 10, p. 44290–44304, 2022.

DARWISH, A. et al. The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. **Journal of Ambient Intelligence and Humanized Computing**, [S.l.], v. 10, n. 10, p. 4151–4166, 2019.

DASTJERDI, A. V. et al. Fog computing: principles, architectures, and applications. In: **Internet of things**. [S.l.]: Elsevier, 2016. p. 61–75.

DEBE, M. et al. Monetization of services provided by public fog nodes using blockchain and smart contracts. **IEEE Access**, [S.l.], v. 8, p. 20118–20128, 2020.

DUBEY, H. et al. Fog data: enhancing telehealth big data through fog computing. In: ASE BIGDATA & SOCIALINFORMATICS 2015, 2015. **Proceedings...** [S.l.: s.n.], 2015. p. 14.

DWIVEDI, A. D. et al. A decentralized privacy-preserving healthcare blockchain for iot. **Sensors**, [S.l.], v. 19, n. 2, p. 326, 2019.

ELMISERY, A. M.; RHO, S.; ABORIZKA, M. A new computing environment for collective privacy protection from constrained healthcare devices to iot cloud services. **Cluster Computing**, [S.l.], p. 1–28, 2017.

ESPOSITO, C. et al. Blockchain: a panacea for healthcare cloud-based data security and privacy? **IEEE Cloud Computing**, [S.l.], v. 5, n. 1, p. 31–37, 2018.

EU population up to over 513 million on 1 january 2019. Accessed: 2022-09-06, https://ec.europa.eu/eurostat/documents/2995521/9967985/3-10072019-BP-EN.pdf/e152399b-cb9e-4a42-a155-c5de6dfe25d1.

FARAHANI, B. et al. Towards fog-driven iot ehealth: promises and challenges of iot in medicine and healthcare. **Future Generation Computer Systems**, [S.l.], v. 78, p. 659–676, 2018.

FRATU, O. et al. Fog computing system for monitoring mild dementia and copd patients-romanian case study. In: TELECOMMUNICATION IN MODERN SATELLITE, CABLE AND BROADCASTING SERVICES (TELSIKS), 2015 12TH INTERNATIONAL CONFERENCE ON, 2015. **Anais...** [S.l.: s.n.], 2015. p. 123–128.

FUNDAMENTAL modeling conceps. Accessed: 2019-08-15, http://www.fmc-modeling.org/quick-intro.

GIA, T. N. et al. Fog computing in healthcare internet of things: a case study on ecg feature extraction. In: COMPUTER AND INFORMATION TECHNOLOGY; UBIQUITOUS COMPUTING AND COMMUNICATIONS; DEPENDABLE, AUTONOMIC AND SECURE COMPUTING; PERVASIVE INTELLIGENCE AND COMPUTING (CIT/IUCC/DASC/PICOM), 2015 IEEE INTERNATIONAL CONFERENCE ON, 2015. **Anais...** [S.l.: s.n.], 2015. p. 356–363.

GIA, T. N. et al. Low-cost fog-assisted health-care iot system with energy-efficient sensor nodes. In: WIRELESS COMMUNICATIONS AND MOBILE COMPUTING CONFERENCE (IWCMC), 2017 13TH INTERNATIONAL, 2017. **Anais...** [S.l.: s.n.], 2017. p. 1765–1770.

GIA, T. N. et al. Fog computing approach for mobility support in internet-of-things systems. **IEEE Access**, [S.l.], v. 6, p. 36064–36082, 2018.

GS1. **About gs1**. 2020.

GS1 healthcare. Accessed: 2022-10-29, https://www.gs1.org/industries/healthcare/implementation.

GUPTA, R. et al. Smart contract privacy protection using ai in cyber-physical systems: tools, techniques and challenges. **IEEE Access**, [S.l.], v. 8, p. 24746–24772, 2020.

HASHEM, I. A. T. et al. The rise of "big data" on cloud computing: review and open research issues. **Information systems**, [S.l.], v. 47, p. 98–115, 2015.

HE, S. et al. Proactive personalized services through fog-cloud computing in large-scale iot-based healthcare application. **China Communications**, [S.l.], v. 14, n. 11, p. 1–16, 2017.

HRIPCSAK, G.; ALBERS, D. J. Next-generation phenotyping of electronic health records. **Journal of the American Medical Informatics Association**, [S.l.], v. 20, n. 1, p. 117–121, 2013.

HYPERLEDGER blockchain performance metrics. Accessed: 2021-12-20, https://www.hyperledger.org/learn/publications/blockchain-performance-metrics.

INTERNATIONAL tourism, receipts (current us$) - united states, france, spain, china, italy. Accessed: 2022-09-19, https://data.worldbank.org/indicator/ST.INT.RCPT.CD?end=2020&locations=US-FR-ES-CN-IT&start=1999.

IORGA, M. et al. **Fog computing conceptual model**. [S.l.]: NIST, 2018.

ISO. **Health informatics —- guidance on health information privacy education in healthcare organizations.** 2017.

JAYARAMAN, R. et al. Data standards in healthcare supply chain operations. In: IIE ANNUAL CONFERENCE. PROCEEDINGS, 2011. **Anais...** [S.l.: s.n.], 2011. p. 1.

JAYARAMAN, R. et al. An exploratory pilot study on supply chain data standards in a hospital pharmacy. **Engineering Management Journal**, [S.l.], v. 27, n. 3, p. 141–151, 2015.

KHALID, A.; SHAHBAZ, M.; FAYYAZ, H. Using body sensor networks to show that fog computing is more efficient than traditional cloud computing. **International Journal of Computer Science and Information Security**, [S.l.], v. 14, n. 12, p. 190, 2016.

KHAREL, J.; REDA, H. T.; SHIN, S. Y. An architecture for smart health monitoring system based. **Journal of Communications**, [S.l.], v. 12, n. 4, 2017.

KHAREL, J.; REDA, H. T.; SHIN, S. Y. Fog computing-based smart health monitoring system deploying lora wireless communication. **IETE Technical Review**, [S.l.], p. 1–14, 2017.

KITCHENHAM, B. Procedure for undertaking systematic reviews. **Computer Science Department, Keele University (TRISE-0401) and National ICT Australia Ltd, Joint Technical Report**, [S.l.], 2004.

KITCHENHAM, B. **Guidelines for performing systematic literature reviews in software engineering.** 2007.

KLONOFF, D. C. Fog computing and edge computing architectures for processing data from diabetes devices connected to the medical internet of things. **Journal of Diabetes Science and Technology**, [S.l.], v. 11, n. 4, p. 647–652, 2017.

KRAEMER, A. et al. Fog computing in healthcare — a review and discussion. **IEEE Access**, [S.l.], v. 5, p. 9206–9222, 2017.

KRITCHANCHAI, D.; HOEUR, S.; ENGELSETH, P. Develop a strategy for improving healthcare logistics performance. In: SUPPLY CHAIN FORUM: AN INTERNATIONAL JOURNAL, 2018. **Anais...** [S.l.: s.n.], 2018. v. 19, n. 1, p. 55–69.

KUMAR, A. et al. A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. **IEEE Access**, [S.l.], v. 8, p. 118433–118471, 2020.

LEITHARDT, V. et al. A solution for dynamic management of user profiles in iot environments. **IEEE Latin America Transactions**, [S.l.], v. 18, n. 07, p. 1193–1199, 2020.

LEWIS, G. A. Role of standards in cloud-computing interoperability. In: HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 2013., 2013. **Anais...** [S.l.: s.n.], 2013. p. 1652–1661.

LIU, X. et al. Hybrid privacy-preserving clinical decision support system in fog–cloud computing. **Future Generation Computer Systems**, [S.l.], v. 78, p. 825–837, 2018.

LV, Z.; CHIRIVELLA, J.; GAGLIARDO, P. Bigdata oriented multimedia mobile health applications. **Journal of medical systems**, [S.l.], v. 40, n. 5, p. 120, 2016.

MAKSIMOVIć, M. Hybrid privacy-preserving clinical decision support system in fog–cloud computing. **ITA-JOURNAL OF INFORMATION TECHNOLOGY AND APLICATIONS**, [S.l.], v. 14, n. 2, 2018.

MANOGARAN, G. et al. A new architecture of internet of things and big data ecosystem for secured smart healthcare monitoring and alerting system. **Future Generation Computer Systems**, [S.l.], v. 82, p. 375–387, 2018.

MARKAKIS, E. K. et al. Emynos: next generation emergency communication. **IEEE Communications Magazine**, [S.l.], v. 55, n. 1, p. 139–145, 2017.

MASOUROS, D. et al. From edge to cloud: design and implementation of a healthcare internet of things infrastructure. In: POWER AND TIMING MODELING, OPTIMIZATION AND SIMULATION (PATMOS), 2017 27TH INTERNATIONAL SYMPOSIUM ON, 2017. **Anais...** [S.l.: s.n.], 2017. p. 1–6.

MASSIMO CANONICO STEFANIA MONTANI, M. S. A telemedicine support for improving medical emergency management. **EAI Endorsed Transactions on Ambient Systems**, [S.l.], v. 4, n. 16, p. 1–6, 2017.

MATHIEU, E. et al. A global database of covid-19 vaccinations. **Nature human behaviour**, [S.l.], v. 5, n. 7, p. 947–953, 2021.

MEHMOOD, I.; SAJJAD, M.; BAIK, S. W. Mobile-cloud assisted video summarization framework for efficient management of remote sensing data generated by wireless capsule sensors. **Sensors**, [S.l.], v. 14, n. 9, p. 17112–17145, 2014.

MELL, P.; GRANCE, T. et al. The nist definition of cloud computing. **Communications of the ACM**, [S.l.], v. 53, n. 6, p. 50, 2011.

MITTAL, P. **Programme management**: managing multiple projects successfully. [S.l.]: Global India Publications, 2009.

MOKHTARI, G.; ANVARI-MOGHADDAM, A.; ZHANG, Q. A new layered architecture for future big data-driven smart homes. **IEEE Access**, [S.l.], 2019.

MOORE, P.; VAN PHAM, H. Fog computing and low latency context-aware health monitoring in smart interconnected environments. In: INTERNATIONAL CONFERENCE ON EMERGING INTERNETWORKING, DATA & WEB TECHNOLOGIES, 2018. **Anais...** [S.l.: s.n.], 2018. p. 29–40.

MORAIS BARROCA FILHO, I. de; AQUINO JUNIOR, G. S. de. Iot-based healthcare applications: a review. In: INTERNATIONAL CONFERENCE ON COMPUTATIONAL SCIENCE AND ITS APPLICATIONS, 2017. **Anais...** [S.l.: s.n.], 2017. p. 47–62.

MOURA COSTA, H. J. de et al. Fog computing in health: a systematic literature review. **Health and Technology**, [S.l.], v. 10, p. 1025–1044, 2020.

MOURA COSTA, H. J. de et al. Fog computing in health: a systematic literature review. **Health and Technology**, [S.l.], v. 10, p. 1025–1044, 2020.

MOURADIAN, C. et al. A comprehensive survey on fog computing: state-of-the-art and research challenges. **IEEE Communications Surveys & Tutorials**, [S.l.], v. 3, p. 854–864, 2017.

NAKAMOTO, S. **Bitcoin**: a peer-to-peer electronic cash system. [S.l.]: Manubot, 2008.

NASTIC, S. et al. A serverless real-time data analytics platform for edge computing. **IEEE Internet Computing**, [S.l.], v. 21, n. 4, p. 64–71, 2017.

NUMBER of people vaccinated against covid-19 august 31, 2022. Accessed: 2022-09-06, https://ourworldindata.org/covid-vaccinations.

NúñEZ-GóMEZ, C.; CAMINERO, B.; CARRIóN, C. Hidra: a distributed blockchain-based architecture for fog/edge computing environments. **IEEE Access**, [S.l.], v. 9, p. 75231–75251, 2021.

OLIVEIRA, R. N. et al. Notification oriented paradigm applied to ambient assisted living tool. **IEEE Latin America Transactions**, [S.l.], v. 16, n. 2, p. 647–653, 2018.

ORGANIZATION, W. T. World tourism barometer. **World Tourism Organization**, [S.l.], v. 18, 2020.

PEREIRA, F.; CROCKER, P.; LEITHARDT, V. R. Padres: tool for privacy, data regulation and security. **SoftwareX**, [S.l.], v. 17, p. 100895, 2022.

PETTICREW M, R. H. **Systematic reviews in the social sciences**. [S.l.]: Blackwell Pub;, 2006.

POPULATION change - demographic balance and crude rates at national level. Accessed: 2022-09-06, https://ec.europa.eu/eurostat/databrowser/view/tps00001/default/table.

PRIETO GONZÁLEZ, L. et al. Fog computing architectures for healthcare: wireless performance and semantic opportunities. **Journal of Information, Communication and Ethics in Society**, [S.l.], v. 14, n. 4, p. 334–349, 2016.

QUAINI, T. et al. A model for blockchain-based distributed electronic health records. **IADIS International Journal on WWW/Internet**, [S.l.], v. 16, n. 2, 2018.

RAHMANI, A. M. et al. Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach. **Future Generation Computer Systems**, [S.l.], v. 78, p. 641–658, 2018.

RAMALHO, F. et al. Enhancing ehealth smart applications: a fog-enabled approach. In: E-HEALTH NETWORKING, APPLICATION & SERVICES (HEALTHCOM), 2015 17TH INTERNATIONAL CONFERENCE ON, 2015. **Anais...** [S.l.: s.n.], 2015. p. 323–328.

REJEB, A.; BELL, L. Potentials of blockchain for healthcare: case of tunisia. **Available at SSRN 3475246**, [S.l.], 2019.

RESIDENT population of the united states from 1980 to 2021. Accessed: 2022-09-06, https://www.statista.com/statistics/183457/united-states–resident-population/.

RITCHIE, H. et al. Coronavirus pandemic (covid-19). **Our world in data**, [S.l.], 2020.

ROEHRS, A. et al. Analyzing the performance of a blockchain-based personal health record implementation. **Journal of biomedical informatics**, [S.l.], v. 92, p. 103140, 2019.

ROMASHKOVA, I.; KOMAROV, M.; OMETOV, A. Demystifying blockchain technology for resource-constrained iot devices: parameters, challenges and future perspective. **IEEE Access**, [S.l.], v. 9, p. 129264–129277, 2021.

SAHOO, P. K.; MOHAPATRA, S. K.; WU, S.-L. Analyzing healthcare big data with prediction for future health condition. **IEEE Access**, [S.l.], v. 4, p. 9786–9799, 2016.

SAHOO, P. K.; MOHAPATRA, S. K.; WU, S.-L. Sla based healthcare big data analysis and computing in cloud network. **Journal of Parallel and Distributed Computing**, [S.l.], v. 119, p. 121–135, 2018.

SAKR, S. et al. A survey of large scale data management approaches in cloud environments. **IEEE Communications Surveys & Tutorials**, [S.l.], v. 13, n. 3, p. 311–336, 2011.

SANAEI, Z. et al. Heterogeneity in mobile cloud computing: taxonomy and open challenges. **IEEE Communications Surveys & Tutorials**, [S.l.], v. 16, n. 1, p. 369–392, 2013.

SAREEN, S.; GUPTA, S. K.; SOOD, S. K. An intelligent and secure system for predicting and preventing zika virus outbreak using fog computing. **Enterprise Information Systems**, [S.l.], v. 11, n. 9, p. 1436–1456, 2017.

SMITH, B. K.; NACHTMANN, H.; POHL, E. A. Improving healthcare supply chain processes via data standardization. **Engineering Management Journal**, [S.l.], v. 24, n. 1, p. 3–10, 2012.

SOOD, S. K.; MAHAJAN, I. Wearable iot sensor based healthcare system for identifying and controlling chikungunya virus. **Computers in Industry**, [S.l.], v. 91, p. 33–44, 2017.

SOOD, S. K.; MAHAJAN, I. A fog-based healthcare framework for chikungunya. **IEEE Internet of Things Journal**, [S.l.], v. 5, n. 2, p. 794–801, 2018.

SOOD, S. K.; MAHAJAN, I. Fog-cloud based cyber-physical system for distinguishing, detecting and preventing mosquito borne diseases. **Future Generation Computer Systems**, [S.l.], 2018.

STANDARDS, G. **Gs1 general specifications**. 2022.

STANTCHEV, V. et al. Smart items, fog and cloud computing as enablers of servitization in healthcare. **Sensors & Transducers**, [S.l.], v. 185, n. 2, p. 121, 2015.

SWAN, M. **Blockchain** : blueprint for a new economy. [S.l.]: O'Reilly Media, 2015.

TASATANATTAKOOL, P.; TECHAPANUPREEDA, C. Blockchain: challenges and applications. In: INTERNATIONAL CONFERENCE ON INFORMATION NETWORKING (ICOIN), 2018., 2018. **Anais...** [S.l.: s.n.], 2018. p. 473–475.

TECHNICAL considerations for implementing a risk-based approach to international travel in the context of covid-19. Accessed: 2022-09-06, https://www.who.int/publications/i/item/WHO-2019-nCoV-Policy-Brief-Risk-based-international-travel-2021.1.

TEMPLETON, D. Be an early riser. there's still time to prepare hospitals for global location number sunrise. **Modern healthcare**, [S.l.], v. 40, n. 10, p. 23, March 2010.

THE health industry business communications council. Accessed: 2022-07-18, https://www.hibcc.org.

UNGUREAN, I.; BREZULIANU, A. An internet of things framework for remote monitoring of the healthcare parameters. **Advances in Electrical and Computer Engineering**, [S.l.], v. 17, n. 2, p. 11–16, 2017.

U.S. population estimated at 332,403,650 on jan. 1, 2022. Accessed: 2022-09-06, https://www.census.gov/library/stories/2021/12/happy-new-year-2022.html.

VAQUERO, L. M.; RODERO-MERINO, L. Finding your way in the fog: towards a comprehensive definition of fog computing. **SIGCOMM Computer Communication Review**, New York, NY, USA, v. 44, n. 5, p. 27–32, Oct. 2014.

VERMA, P. et al. Fetch: a deep learning-based fog computing and iot integrated environment for healthcare monitoring and diagnosis. **IEEE Access**, [S.l.], v. 10, p. 12548–12563, 2022.

VERMA, P.; SOOD, S. K. Cloud-centric iot based disease diagnosis healthcare framework. **Journal of Parallel and Distributed Computing**, [S.l.], v. 116, p. 27–38, 2018.

VERMA, P.; SOOD, S. K. Fog assisted-iot enabled patient health monitoring in smart homes. **IEEE Internet of Things Journal**, [S.l.], 2018.

VOHRA, N.; JAIN, N. Synchronization of health informatics with "aadhaar"(uid: unique identification). In: INTERNATIONAL JOINT CONFERENCE ON ADVANCES IN SIGNAL PROCESSING AND INFORMATION TECHNOLOGY, 2011. **Anais...** [S.l.: s.n.], 2011. p. 201–204.

XIE, J. et al. A survey on the scalability of blockchain systems. **IEEE Network**, [S.l.], v. 33, n. 5, p. 166–173, 2019.

YAGA, D. et al. Blockchain technology overview. **arXiv preprint arXiv:1906.11078**, [S.l.], 2019.

YUE, X. et al. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. **Journal of medical systems**, [S.l.], v. 40, n. 10, p. 218, 2016.

ZAMFIR, M. et al. Towards a platform for prototyping iot health monitoring services. In: INTERNATIONAL CONFERENCE ON EXPLORING SERVICES SCIENCE, 2016. **Anais...** [S.l.: s.n.], 2016. p. 522–533.

ZHANG, Q.; CHENG, L.; BOUTABA, R. Cloud computing: state-of-the-art and research challenges. **Journal of internet services and applications**, [S.l.], v. 1, n. 1, p. 7–18, 2010.

ZHENG, P. et al. A detailed and real-time performance monitoring framework for blockchain systems. in 2018 ieee/acm 40th international conference on software engineering: software engineering in practice track (icse-seip). **IEEE, New York, NY, USA**, [S.l.], p. 134–143, 2018.

Appendices

APPENDIX A – FINAL LIST OF SELECTED ARTICLES

Table 20 – Final list of selected articles

Article	Ref.	Year.	Publisher	Type
Farahani et al.	(FARAHANI et al., 2018)	2018	Elsevier	Journal
Sood et al.	(SOOD; MAHAJAN, 2018a)	2018	IEEE	Journal
Manogaran et al.	(MANOGARAN et al., 2018)	2018	Elsevier	Journal
Verma et al.	(VERMA; SOOD, 2018a)	2018	Elsevier	Journal
Rahmani et al.	(RAHMANI et al., 2018)	2018	Elsevier	Journal
Bhatia et al.	(BHATIA; SOOD, 2018)	2018	Springer	Journal
Verma et al.	(VERMA; SOOD, 2018b)	2018	Elsevier	Journal
Klonoff et al.	(KLONOFF, 2017)	2018	SAGE Publications	Journal
Moore et al.	(MOORE; VAN PHAM, 2018)	2018	Springer	Conference
Sood et. al	(SOOD; MAHAJAN, 2018b)	2018	Elsevier	Journal
Liu et al.	(LIU et al., 2018)	2018	Elsevier	Journal
Barik et al.	(BARIK et al., 2018a)	2018	Springer	Journal
Maksimovic et al.	(MAKSIMOVIć, 2018)	2018	Elsevier	Journal
Barik et al.	(BARIK et al., 2018b)	2018	Elsevier	Journal
Massouros et al.	(MASOUROS et al., 2017)	2017	IEEE	Conference
Cerina et al.	(CERINA et al., 2017)	2017	IEEE	Conference
Elmisery et al.	(ELMISERY; RHO; ABORIZKA, 2017)	2017	Springer	Journal
Al et al.	(AL HAMID et al., 2017)	2017	IEEE	Journal
Nastic et al.	(NASTIC et al., 2017)	2017	IEEE	Journal
kharel et al.	(KHAREL; REDA; SHIN, 2017a)	2017	Oxford Univ. Press	Journal
Sareen et al.	(SAREEN; GUPTA; SOOD, 2017)	2017	Taylor & Francis	Journal
Ungurean et al.	(UNGUREAN; BREZULIANU, 2017)	2017	University of Suceava	Journal
Abideen et al.	(ABIDEEN; SHAH, 2017)	2017	IEEE	Conference
Alshikyehr et al.	(ALSHIKY; BUHARI; BARNAWI, 2017)	2017	EAI	Journal
Arkakis et al.	(MARKAKIS et al., 2017)	2017	IEEE	Journal
kharel et al.	(KHAREL; REDA; SHIN, 2017b)	2017	Taylor & Francis	Journal
Azimi	(AZIMI et al., 2017)	2017	ACM	Journal
Gia et al.	(GIA et al., 2017)	2017	IEEE	Conference
Akrivopoulos et al.	(AKRIVOPOULOS et al., 2017)	2017	IEEE	Conference
He et al.	(HE et al., 2017)	2017	IEEE	Journal
Ali et al.	(ALI; GHAZAL, 2017)	2017	IEEE	Conference
Sood et al.	(SOOD; MAHAJAN, 2017)	2017	Elsevier	Journal
Canonico et al	(MASSIMO CANONICO STEFANIA MONTANI, 2017)	2017	Elsevier	Journal
Zamfir et al.	(ZAMFIR et al., 2016)	2016	Springer	Conference
Khalid et al.	(KHALID; SHAHBAZ; FAYYAZ, 2016)	2016	LJS Publishing	Journal
Prieto et al.	(PRIETO GONZÁLEZ et al., 2016)	2016	Elsevier	Journal
Ahmad et al.	(AHMAD et al., 2016)	2016	Springer	Journal
Azimi et al.	(AZIMI et al., 2016)	2016	IEEE	Conference
Ramalho et al.	(RAMALHO et al., 2015)	2015	IEEE	Conference
Cao et al.	(CAO et al., 2015)	2015	ACM	Conference
Gia et al.	(GIA et al., 2015)	2015	IEEE	Conference
Fratu et al.	(FRATU et al., 2015)	2015	IEEE	Conference
Dubey et al.	(DUBEY et al., 2015)	2015	ACM	Conference
Stantchev et al.	(STANTCHEV et al., 2015)	2015	IFSA Publishing	Journal

APPENDIX B – CHALLENGES AND RELATED ARTICLES

Table 21 – Challenges and related articles.

Challenge	Reference Articles
Data Management	(FARAHANI et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (NASTIC et al., 2017), (VERMA; SOOD, 2018a), (ALSHIKY; BUHARI; BARNAWI, 2017), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (AZIMI et al., 2017), (AZIMI et al., 2016), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016)
Scalability	(FARAHANI et al., 2018), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (SAREEN; GUPTA; SOOD, 2017), (ABIDEEN; SHAH, 2017), (ALSHIKY; BUHARI; BARNAWI, 2017), (RAHMANI et al., 2018), (GIA et al., 2015), (KHAREL; REDA; SHIN, 2017b), (SOOD; MAHAJAN, 2018b), (BARIK et al., 2018a), (MAKSIMOVIć, 2018), (BARIK et al., 2018b), (AKRIVOPOULOS et al., 2017), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016)
Interoperability	(FARAHANI et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a). (RAHMANI et al., 2018), (PRIETO GONZÁLEZ et al., 2016), (GIA et al., 2015), (KHAREL; REDA; SHIN, 2017b), (BARIK et al., 2018a), (MAKSIMOVIć, 2018), (BARIK et al., 2018b), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016)
Security Aspects	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (SAREEN; GUPTA; SOOD, 2017), (UNGUREAN; BREZULIANU, 2017), (ABIDEEN; SHAH, 2017), (VERMA; SOOD, 2018a), (MASSIMO CANONICO STEFANIA MONTANI, 2017), (ALSHIKY; BUHARI; BARNAWI, 2017), (MARKAKIS et al., 2017), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (KLONOFF, 2017), (MOORE; VAN PHAM, 2018), (PRIETO GONZÁLEZ et al., 2016), (GIA et al., 2015), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (GIA et al., 2017), (BARIK et al., 2018b), (AKRIVOPOULOS et al., 2017), (HE et al., 2017), (ALI; GHAZAL, 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
Privacy	(FARAHANI et al., 2018), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (SAREEN; GUPTA; SOOD, 2017), (UNGUREAN; BREZULIANU, 2017), (ABIDEEN; SHAH, 2017), (MASSIMO CANONICO STEFANIA MONTANI, 2017), (ALSHIKY; BUHARI; BARNAWI, 2017), (RAHMANI et al., 2018), (VERMA; SOOD, 2018b), (KLONOFF, 2017), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (BARIK et al., 2018b), (AKRIVOPOULOS et al., 2017), (STANTCHEV et al., 2015), (KHALID; SHAHBAZ; FAYYAZ, 2016)

APPENDIX C - LIST OF APPLICATIONS AND RELATED ARTICLES

Table 22 – List of Applications and related articles.

Application / Service	Articles
mHealth	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (NASTIC et al., 2017), (UNGUREAN; BREZULIANU, 2017), (VERMA; SOOD, 2018a), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (AHMAD et al., 2016), (ZAMFIR et al., 2016), (SOOD; MAHAJAN, 2017)
Medication	(FARAHANI et al., 2018), (CERINA et al., 2017), (PRIETO GONZÁLEZ et al., 2016), (FRATU et al., 2015), (SOOD; MAHAJAN, 2018b), (HE et al., 2017), (SOOD; MAHAJAN, 2017)
Recommender Service	(ELMISERY; RHO; ABORIZKA, 2017)
Real-time health analytics	(ELMISERY; RHO; ABORIZKA, 2017), (KHAREL; REDA; SHIN, 2017a), (VERMA; SOOD, 2018a), (VERMA; SOOD, 2018b), (MOORE; VAN PHAM, 2018), (GIA et al., 2015), (KHAREL; REDA; SHIN, 2017b), (LIU et al., 2018), (GIA et al., 2017), (HE et al., 2017)
Continuous monitoring of health	(MANOGARAN et al., 2018), (ABIDEEN; SHAH, 2017), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (AHMAD et al., 2016), (AZIMI et al., 2017), (ALI; GHAZAL, 2017)
Prognostics & health management	(FARAHANI et al., 2018), (UNGUREAN; BREZULIANU, 2017)
Ambient Assisted Living (AAL)	(FARAHANI et al., 2018), (UNGUREAN; BREZULIANU, 2017), (MARKAKIS et al., 2017), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (FRATU et al., 2015), (AZIMI et al., 2017), (ZAMFIR et al., 2016)

APPENDIX D - DEVICE LAYER ARTICLES

Table 23 – Device Layer articles.

Name	Description	Detail	Articles
Interface	Wearable / Anywhere		(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (SAREEN; GUPTA; SOOD, 2017), (UNGUREAN; BREZULIANU, 2017), (ABIDEEN; SHAH, 2017), (VERMA; SOOD, 2018a), (CAO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (KLONOFF, 2017), (PRIETO GONZÁLEZ et al., 2016), (GIA et al., 2015), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (GIA et al., 2017), (AZIMI et al., 2016), (BARIK et al., 2018b), (AKRIVOPOULOS et al., 2017), (HE et al., 2017), (ALI; GHAZAL, 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
	Smart home		(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a). (UNGUREAN; BREZULIANU, 2017), (VERMA; SOOD, 2018a), (RAHMANI et al., 2018), (VERMA; SOOD, 2018b), (MOORE; VAN PHAM, 2018), (SOOD; MAHAJAN, 2018b), (BARIK et al., 2018a), (AHMAD et al., 2016), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (SOOD; MAHAJAN, 2017)
	Smart city		(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (MOORE; VAN PHAM, 2018), (KHAREL; REDA; SHIN, 2017b), (BARIK et al., 2018a), (AZIMI et al., 2017), (AKRIVOPOULOS et al., 2017), (ALI; GHAZAL, 2017)
Protocol	Data Format	Text	(FARAHANI et al., 2018), (MASSIMO CANONICO STEFANIA MONTANI, 2017), (RAHMANI et al., 2018), (MASOUROS et al., 2017), (GIA et al., 2017)
		Binary	(FARAHANI et al., 2018), (BARIK et al., 2018a), (AZIMI et al., 2017)
	Application Layer	MQTT	(FARAHANI et al., 2018), (UNGUREAN; BREZULIANU, 2017), (AKRIVOPOULOS et al., 2017), (ZAMFIR et al., 2016)
		AMQP	(FARAHANI et al., 2018)
		CoAP	(FARAHANI et al., 2018), (MANOGARAN et al., 2018)
		XMPP	(FARAHANI et al., 2018), (ABIDEEN; SHAH, 2017)
	Transport Layer	DTLS	(FARAHANI et al., 2018), (ABIDEEN; SHAH, 2017)
		TCP	(FARAHANI et al., 2018), (RAHMANI et al., 2018), (AZIMI et al., 2017), (GIA et al., 2017), (AZIMI et al., 2016)
		UDP	(FARAHANI et al., 2018)
	Network Layer	6LoWPAN	(FARAHANI et al., 2018), (AL HAMID et al., 2017), (UNGUREAN; BREZULIANU, 2017), (ABIDEEN; SHAH, 2017), (RAHMANI et al., 2018), (GIA et al., 2015), (KHAREL; REDA; SHIN, 2017b), (GIA et al., 2017)
		LoRaWAN	(KHAREL; REDA; SHIN, 2017a), (KHAREL; REDA; SHIN, 2017b)
	Link Layer	BLE	(FARAHANI et al., 2018), (RAHMANI et al., 2018), (GIA et al., 2015), (MASOUROS et al., 2017)
		LoRa	(KHAREL; REDA; SHIN, 2017a), (KHAREL; REDA; SHIN, 2017b)
		NFC	(FARAHANI et al., 2018), (UNGUREAN; BREZULIANU, 2017), (BHATIA; SOOD, 2018), (KHAREL; REDA; SHIN, 2017b)
		RFID	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (KHAREL; REDA; SHIN, 2017a), (UNGUREAN; BREZULIANU, 2017), (ABIDEEN; SHAH, 2017), (VERMA; SOOD, 2018a), (BHATIA; SOOD, 2018), (PRIETO GONZÁLEZ et al., 2016), (KHAREL; REDA; SHIN, 2017b), (SOOD; MAHAJAN, 2018b), (HE et al., 2017), (STANTCHEV et al., 2015), (SOOD; MAHAJAN, 2017)
		ZigBee	(FARAHANI et al., 2018), (KHAREL; REDA; SHIN, 2017a), (UNGUREAN; BREZULIANU, 2017), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (GIA et al., 2015), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (AHMAD et al., 2016), (GIA et al., 2017), (STANTCHEV et al., 2015), (KHALID; SHAHBAZ; FAYYAZ, 2016)
		ZWave	(FARAHANI et al., 2018)
Sensor	Physical		(FARAHANI et al., 2018), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (KHAREL; REDA; SHIN, 2017a), (SAREEN; GUPTA; SOOD, 2017), (UNGUREAN; BREZULIANU, 2017), (VERMA; SOOD, 2018a), (MASSIMO CANONICO STEFANIA MONTANI, 2017), (ALSHIKY; BUHARI; BARNAWI, 2017), (MARKAKIS et al., 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (MOORE; VAN PHAM, 2018), (PRIETO GONZÁLEZ et al., 2016), (GIA et al., 2015), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (AHMAD et al., 2016), (AZIMI et al., 2017), (GIA et al., 2017), (AKRIVOPOULOS et al., 2017), (ALI; GHAZAL, 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016)
	Virtual		(FARAHANI et al., 2018)

APPENDIX E - FOG LAYER ARTICLES

Table 24 – Fog layer articles.

Name	Description	Articles
Interoperability	Protocol translator	(RAHMANI et al., 2018)
	Network layer	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (SAREEN; GUPTA; SOOD, 2017), (ABIDEEN; SHAH, 2017), (VERMA; SOOD, 2018a), (MARKAKIS et al., 2017), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (KLONOFF, 2017), (MOORE; VAN PHAM, 2018), (PRIETO GONZÁLEZ et al., 2016), (GIA et al., 2015), (KHAREL; REDA; SHIN, 2017b), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (GIA et al., 2017), (AZIMI et al., 2016), (BARIK et al., 2018b), (AKRIVOPOULOS et al., 2017), (HE et al., 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
	Messenger layer	(FARAHANI et al., 2018)
	Data annotation layer	(FARAHANI et al., 2018)
Data Manipulation	Aggregation	(FARAHANI et al., 2018), (CERINA et al., 2017), (ELMISERY; RHO; ABORIZKA, 2017), (ALSHIKY; BUHARI; BARNAWI, 2017), (RAHMANI et al., 2018), (KLONOFF, 2017), (MOORE; VAN PHAM, 2018), (PRIETO GONZÁLEZ et al., 2016), (AZIMI et al., 2017), (AKRIVOPOULOS et al., 2017)
	Filtering	(FARAHANI et al., 2018), (UNGUREAN; BREZULIANU, 2017), (CAO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (PRIETO GONZÁLEZ et al., 2016), (DUBEY et al., 2015), (AZIMI et al., 2017)
	Formatting	(FARAHANI et al., 2018), (RAHMANI et al., 2018), (KLONOFF, 2017)
	Encoding	(FARAHANI et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (KHAREL; REDA; SHIN, 2017a), (KHAREL; REDA; SHIN, 2017b), (BARIK et al., 2018a), (AHMAD et al., 2016), (LIU et al., 2018), (GIA et al., 2017)
	Decoding	(FARAHANI et al., 2018), (AL HAMID et al., 2017), (PRIETO GONZÁLEZ et al., 2016)
Technologies	Context-aware	(FARAHANI et al., 2018), (CERINA et al., 2017), (SAREEN; GUPTA; SOOD, 2017), (VERMA; SOOD, 2018a), (MARKAKIS et al., 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (MOORE; VAN PHAM, 2018), (BARIK et al., 2018a), (AZIMI et al., 2017), (AZIMI et al., 2016), (ALI; GHAZAL, 2017), (ZAMFIR et al., 2016), (SOOD; MAHAJAN, 2017)
	Mobility	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (SAREEN; GUPTA; SOOD, 2017), (UNGUREAN; BREZULIANU, 2017), (ABIDEEN; SHAH, 2017), (CAO et al., 2015), (ALSHIKY; BUHARI; BARNAWI, 2017), (MARKAKIS et al., 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (VERMA; SOOD, 2018b), (MOORE; VAN PHAM, 2018), (GIA et al., 2015), (KHAREL; REDA; SHIN, 2017b), (MASOUROS et al., 2017), (AZIMI et al., 2017), (MAKSIMOVIć, 2018), (GIA et al., 2017), (ALI; GHAZAL, 2017), (STANTCHEV et al., 2015), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
	Big Data	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), A3, (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (SAREEN; GUPTA; SOOD, 2017), (VERMA; SOOD, 2018a), (CAO et al., 2015), (MASSIMO CANONICO STEFANIA MONTANI, 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (KLONOFF, 2017), (PRIETO GONZÁLEZ et al., 2016), (GIA et al., 2015), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (AZIMI et al., 2016), (HE et al., 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
	QoS	(NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (SAREEN; GUPTA; SOOD, 2017), (CAO et al., 2015),(MASSIMO CANONICO STEFANIA MONTANI, 2017), (MARKAKIS et al., 2017), (RAHMANI et al., 2018), (VERMA; SOOD, 2018b), (GIA et al., 2015), (KHAREL; REDA; SHIN, 2017b), (AZIMI et al., 2017), (HE et al., 2017), (ALI; GHAZAL, 2017), (STANTCHEV et al., 2015)
	Database	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (ABIDEEN; SHAH, 2017), (SAREEN; GUPTA; SOOD, 2017), (VERMA; SOOD, 2018a), (ALSHIKY; BUHARI; BARNAWI, 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (MOORE; VAN PHAM, 2018), (GIA et al., 2015), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (GIA et al., 2017), (AZIMI et al., 2016), (AKRIVOPOULOS et al., 2017), (HE et al., 2017), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
	Web Service	(MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (NASTIC et al., 2017), (SAREEN; GUPTA; SOOD, 2017), (VERMA; SOOD, 2018a), (CAO et al., 2015), (RAHMANI et al., 2018), (PRIETO GONZÁLEZ et al., 2016), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AZIMI et al., 2017), (HE et al., 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (SOOD; MAHAJAN, 2017)
	Real-time Analytics	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (NASTIC et al., 2017), (SAREEN; GUPTA; SOOD, 2017), (VERMA; SOOD, 2018a), (CAO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (KLONOFF, 2017), (MOORE; VAN PHAM, 2018), (PRIETO GONZÁLEZ et al., 2016), (GIA et al., 2015), (FRATU et al., 2015), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (AZIMI et al., 2016), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016)
Fog Nodes	Database	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (ABIDEEN; SHAH, 2017), (VERMA; SOOD, 2018a) (ALSHIKY; BUHARI; BARNAWI, 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (MOORE; VAN PHAM, 2018), (GIA et al., 2015), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (GIA et al., 2017), (AZIMI et al., 2016), (AKRIVOPOULOS et al., 2017), (HE et al., 2017), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
	Security	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (ABIDEEN; SHAH, 2017), (VERMA; SOOD, 2018a) (ALSHIKY; BUHARI; BARNAWI, 2017), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (KLONOFF, 2017), (MOORE; VAN PHAM, 2018), (GIA et al., 2015), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (GIA et al., 2017), (BARIK et al., 2018b), (AKRIVOPOULOS et al., 2017), (HE et al., 2017), (ALI; GHAZAL, 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
	Processing	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (ABIDEEN; SHAH, 2017), (VERMA; SOOD, 2018a) (ALSHIKY; BUHARI; BARNAWI, 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (KLONOFF, 2017), (MOORE; VAN PHAM, 2018), (GIA et al., 2015), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (GIA et al., 2017), (AZIMI et al., 2016), (BARIK et al., 2018b), (AKRIVOPOULOS et al., 2017), (HE et al., 2017), (ALI; GHAZAL, 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
	Analytics	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (VERMA; SOOD, 2018a) (ALSHIKY; BUHARI; BARNAWI, 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (KLONOFF, 2017), (MOORE; VAN PHAM, 2018), (GIA et al., 2015), (FRATU et al., 2015), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (AZIMI et al., 2016), (BARIK et al., 2018b), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016)
	Event	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (VERMA; SOOD, 2018a), (ALSHIKY; BUHARI; BARNAWI, 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AZIMI et al., 2017), (MAKSIMOVIć, 2018), (AKRIVOPOULOS et al., 2017), (HE et al., 2017), (ALI; GHAZAL, 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (SOOD; MAHAJAN, 2017)
	Format	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (VERMA; SOOD, 2018a) (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (KLONOFF, 2017), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AZIMI et al., 2017), (LIU et al., 2018), (AKRIVOPOULOS et al., 2017), (ZAMFIR et al., 2016), (SOOD; MAHAJAN, 2017)
Interface	Multi-standard	(FARAHANI et al., 2018)
	Standard	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (SAREEN; GUPTA; SOOD, 2017), (UNGUREAN; BREZULIANU, 2017), (ABIDEEN; SHAH, 2017), (VERMA; SOOD, 2018a), (ALSHIKY; BUHARI; BARNAWI, 2017), (MARKAKIS et al., 2017), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (KLONOFF, 2017), (PRIETO GONZÁLEZ et al., 2016), (GIA et al., 2015), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (GIA et al., 2017), (AZIMI et al., 2016), (BARIK et al., 2018b), (AKRIVOPOULOS et al., 2017), (HE et al., 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
Service	Communication	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (ABIDEEN; SHAH, 2017), (VERMA; SOOD, 2018a) (ALSHIKY; BUHARI; BARNAWI, 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (KLONOFF, 2017), (MOORE; VAN PHAM, 2018), (GIA et al., 2015), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (KHAREL; REDA; SHIN, 2017b), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (GIA et al., 2017), (AZIMI et al., 2016), (BARIK et al., 2018b), (AKRIVOPOULOS et al., 2017), (HE et al., 2017), (ALI; GHAZAL, 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
	CPU	(FARAHANI et al., 2018), (CERINA et al., 2017), (MANOGARAN et al., 2018), (AL HAMID et al., 2017), (RAMALHO et al., 2015), (VERMA; SOOD, 2018b), (KHAREL; REDA; SHIN, 2017b), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AZIMI et al., 2016), (HE et al., 2017), (SOOD; MAHAJAN, 2017)
	Storage	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (ABIDEEN; SHAH, 2017), (VERMA; SOOD, 2018a) (ALSHIKY; BUHARI; BARNAWI, 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (KLONOFF, 2017), (MOORE; VAN PHAM, 2018), (GIA et al., 2015), (KHAREL; REDA; SHIN, 2017b), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (GIA et al., 2017), (AZIMI et al., 2016), (BARIK et al., 2018b), (AKRIVOPOULOS et al., 2017), (HE et al., 2017), (ALI; GHAZAL, 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
Tasks	Assessments	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (SAREEN; GUPTA; SOOD, 2017), (VERMA; SOOD, 2018a), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (BARIK et al., 2018a), (AZIMI et al., 2017), (SOOD; MAHAJAN, 2017)
	Notification	(FARAHANI et al., 2018), (UNGUREAN; BREZULIANU, 2017), (ALSHIKY; BUHARI; BARNAWI, 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (KLONOFF, 2017), (PRIETO GONZÁLEZ et al., 2016), (FRATU et al., 2015), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (AZIMI et al., 2017), (AKRIVOPOULOS et al., 2017), (HE et al., 2017), (KHALID; SHAHBAZ; FAYYAZ, 2016)
	Decision Making	(CERINA et al., 2017), (MANOGARAN et al., 2018), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (SAREEN; GUPTA; SOOD, 2017), (ABIDEEN; SHAH, 2017), (VERMA; SOOD, 2018a), (CAO et al., 2015), (MARKAKIS et al., 2017), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (GIA et al., 2017), (AZIMI et al., 2016), (STANTCHEV et al., 2015), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
	Data Processing	(FARAHANI et al., 2018), (MANOGARAN et al., 2018), (AL HAMID et al., 2017), (NASTIC et al., 2017), (SAREEN; GUPTA; SOOD, 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (KLONOFF, 2017), (MOORE; VAN PHAM, 2018), (PRIETO GONZÁLEZ et al., 2016), (GIA et al., 2015), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (MAKSIMOVIć, 2018), (GIA et al., 2017), (AKRIVOPOULOS et al., 2017), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016)

APPENDIX F - CLOUD LAYER ARTICLES

Table 25 – Cloud layer articles.

Name	Description	Articles
Service Model	Software as a Service - SaaS	(FARAHANI et al., 2018), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (BARIK et al., 2018a), (BARIK et al., 2018b), (HE et al., 2017)
	Platform as a Service - PaaS	(FARAHANI et al., 2018), (MANOGARAN et al., 2018)
	Infrastructure as a Service - IaaS	(FARAHANI et al., 2018), (MANOGARAN et al., 2018), (UNGUREAN; BREZULIANU, 2017), (VERMA; SOOD, 2018a)
Deployment Model	Community cloud	(FARAHANI et al., 2018)
	Hybrid cloud	(FARAHANI et al., 2018), (MANOGARAN et al., 2018)
	Private cloud	(MANOGARAN et al., 2018), (AL HAMID et al., 2017), (PRIETO GONZÁLEZ et al., 2016)
	Public cloud	(FARAHANI et al., 2018), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (AHMAD et al., 2016)
Security	Privacy	(FARAHANI et al., 2018), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (SAREEN; GUPTA; SOOD, 2017), (UNGUREAN; BREZULIANU, 2017), (ABIDEEN; SHAH, 2017), (MASSIMO CANONICO STEFANIA MONTANI, 2017), (ALSHIKY; BUHARI; BARNAWI, 2017), (RAHMANI et al., 2018), (VERMA; SOOD, 2018b), (KLONOFF, 2017), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (AZIMI et al., 2016), (BARIK et al., 2018b), (AKRIVOPOULOS et al., 2017), (STANTCHEV et al., 2015), (KHALID; SHAHBAZ; FAYYAZ, 2016)
	Confidentiality	(FARAHANI et al., 2018), (MANOGARAN et al., 2018), (SAREEN; GUPTA; SOOD, 2017), (UNGUREAN; BREZULIANU, 2017), (ALSHIKY; BUHARI; BARNAWI, 2017), (RAHMANI et al., 2018), (PRIETO GONZÁLEZ et al., 2016), (AZIMI et al., 2017), (KHALID; SHAHBAZ; FAYYAZ, 2016)
	Integrity	(FARAHANI et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (SAREEN; GUPTA; SOOD, 2017), (UNGUREAN; BREZULIANU, 2017), (ABIDEEN; SHAH, 2017), (MASSIMO CANONICO STEFANIA MONTANI, 2017), (RAHMANI et al., 2018), (PRIETO GONZÁLEZ et al., 2016), (MAKSIMOVIć, 2018), (ALI; GHAZAL, 2017), (KHALID; SHAHBAZ; FAYYAZ, 2016)
	Availability	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (ELMISERY; RHO; ABORIZKA, 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (SAREEN; GUPTA; SOOD, 2017), (ABIDEEN; SHAH, 2017), (MASSIMO CANONICO STEFANIA MONTANI, 2017), (ALSHIKY; BUHARI; BARNAWI, 2017), (RAHMANI et al., 2018), (PRIETO GONZÁLEZ et al., 2016), (KHAREL; REDA; SHIN, 2017b), (AHMAD et al., 2016), (AZIMI et al., 2017), (MAKSIMOVIć, 2018), (GIA et al., 2017), (AKRIVOPOULOS et al., 2017), (ALI; GHAZAL, 2017), (STANTCHEV et al., 2015), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)
	Accountability	(MAKSIMOVIć, 2018), (KHALID; SHAHBAZ; FAYYAZ, 2016)
	Access Control	(FARAHANI et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (SAREEN; GUPTA; SOOD, 2017), (VERMA; SOOD, 2018a), (ALSHIKY; BUHARI; BARNAWI, 2017), (AHMAD et al., 2016), (MAKSIMOVIć, 2018), (STANTCHEV et al., 2015)
	Law / Compliance	(FARAHANI et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (BHATIA; SOOD, 2018), (KLONOFF, 2017), (MOORE; VAN PHAM, 2018), (PRIETO GONZÁLEZ et al., 2016), (BARIK et al., 2018a), (AKRIVOPOULOS et al., 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (SOOD; MAHAJAN, 2017)
	Data Protection	(FARAHANI et al., 2018), (MANOGARAN et al., 2018), (AL HAMID et al., 2017), (PRIETO GONZÁLEZ et al., 2016), (AHMAD et al., 2016)
Big Data	Data Analytics	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), A3, A4, (ELMISERY; RHO; ABORIZKA, 2017), (NASTIC et al., 2017), (VERMA; SOOD, 2018a), (CAO et al., 2015), (MARKAKIS et al., 2017), (RAMALHO et al., 2015), (RAHMANI et al., 2018), (MOORE; VAN PHAM, 2018), (DUBEY et al., 2015), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AZIMI et al., 2017), (MAKSIMOVIć, 2018), (AZIMI et al., 2016), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016)
	Machine Learning	(FARAHANI et al., 2018), A4, (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (KHAREL; REDA; SHIN, 2017a), (VERMA; SOOD, 2018a), (CAO et al., 2015), (RAHMANI et al., 2018), (PRIETO GONZÁLEZ et al., 2016), (KHAREL; REDA; SHIN, 2017b), (DUBEY et al., 2015), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (AZIMI et al., 2016), (ZAMFIR et al., 2016)

APPENDIX G - LIST OF MAIN CHALLENGES

Table 26 – List of main challenges.

Challenges	Problems / Gaps	References
Interoperability	Connect different networks, protocols and manage and exchange data.	(FARAHANI et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a). (RAHMANI et al., 2018), (PRIETO GONZÁLEZ et al., 2016), (GIA et al., 2015), (KHAREL; REDA; SHIN, 2017b), (BARIK et al., 2018a), (MAKSIMOVIć, 2018), (BARIK et al., 2018b), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016)
Privacy	Access control and data leak.	(FARAHANI et al., 2018), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (AL HAMID et al., 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (SAREEN; GUPTA; SOOD, 2017), (UNGUREAN; BREZULIANU, 2017), (ABIDEEN; SHAH, 2017), (MASSIMO CANONICO STEFANIA MONTANI, 2017), (ALSHIKY; BUHARI; BARNAWI, 2017), (RAHMANI et al., 2018), (VERMA; SOOD, 2018b), (KLONOFF, 2017), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (AZIMI et al., 2016), (BARIK et al., 2018b), (AKRIVOPOULOS et al., 2017), (STANTCHEV et al., 2015), (KHALID; SHAHBAZ; FAYYAZ, 2016)
Security	Integrity, accountability	(FARAHANI et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (SAREEN; GUPTA; SOOD, 2017), (UNGUREAN; BREZULIANU, 2017), (ABIDEEN; SHAH, 2017), (MASSIMO CANONICO STEFANIA MONTANI, 2017), (RAHMANI et al., 2018), (PRIETO GONZÁLEZ et al., 2016), (MAKSIMOVIć, 2018), (ALI; GHAZAL, 2017), (KHALID; SHAHBAZ; FAYYAZ, 2016), (MAKSIMOVIć, 2018), (KHALID; SHAHBAZ; FAYYAZ, 2016)
Unique Identity	integrated identification	(JAYARAMAN et al., 2011), (KRITCHANCHAI; HOEUR; ENGELSETH, 2018), (SMITH; NACHTMANN; POHL, 2012), (ISO, 2017)
Scalability	Latency, support real-time.	(ELMISERY; RHO; ABORIZKA, 2017), (KHAREL; REDA; SHIN, 2017a), (VERMA; SOOD, 2018a), (VERMA; SOOD, 2018b), (MOORE; VAN PHAM, 2018), (GIA et al., 2015), (KHAREL; REDA; SHIN, 2017b), (LIU et al., 2018), (GIA et al., 2017), (HE et al., 2017)
Mobility	Access anytime, anywhere, any device.	(FARAHANI et al., 2018), (SOOD; MAHAJAN, 2018a), (CERINA et al., 2017), (MANOGARAN et al., 2018), (ELMISERY; RHO; ABORIZKA, 2017), (NASTIC et al., 2017), (KHAREL; REDA; SHIN, 2017a), (SAREEN; GUPTA; SOOD, 2017), (UNGUREAN; BREZULIANU, 2017), (ABIDEEN; SHAH, 2017), (VERMA; SOOD, 2018a), (CAO et al., 2015), (RAHMANI et al., 2018), (BHATIA; SOOD, 2018), (VERMA; SOOD, 2018b), (KLONOFF, 2017), (PRIETO GONZÁLEZ et al., 2016), (GIA et al., 2015), (FRATU et al., 2015), (KHAREL; REDA; SHIN, 2017b), (DUBEY et al., 2015), (SOOD; MAHAJAN, 2018b), (MASOUROS et al., 2017), (BARIK et al., 2018a), (AHMAD et al., 2016), (AZIMI et al., 2017), (LIU et al., 2018), (MAKSIMOVIć, 2018), (GIA et al., 2017), (AZIMI et al., 2016), (BARIK et al., 2018b), (AKRIVOPOULOS et al., 2017), (HE et al., 2017), (ALI; GHAZAL, 2017), (STANTCHEV et al., 2015), (ZAMFIR et al., 2016), (KHALID; SHAHBAZ; FAYYAZ, 2016), (SOOD; MAHAJAN, 2017)

APPENDIX H - CODE LIST

```
public int calcValDigit(String gid) {
  int sum   = 0;
  int odds  = 0;
  int evens = 0;

  for (int i = 0; i < gid.length(); i++) {

    if ((i+1) % 2 == 1) { // if position odd
      odds = odds +  Integer.parseInt(
      String.valueOf(gid.charAt(i)));

    }else { // if position even
      evens = evens + Integer.parseInt(
      String.valueOf(gid.charAt(i)));
    }

  }
  sum = (odds * 3 + evens);

  int superior = sum;

  while(superior % 10 != 0) {
    superior++;
  }

    return superior - sum;

}
```

Listing 1: Validation Code.

```
type PersonSmartContract struct {
        contractapi.Contract
}

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

type Vaccine struct {
        IdVaccine    int    `json:"IdVaccine"`
        Gtin         int    `json:"gtin"`
        Name         string `json:"name"`
        Version      string `json:"version"`
        Country      string `json:"country"`
        MinTemp      int    `json:"minTemp"`
        MaxTemp      int    `json:"maxTemp"`
        ExpirityDays int    `json:"expirityDays"`
    (...)
}

type Vaccination struct {
        IdVaccination int `json:"IdVaccination"`
        GIDPerson     int    `json:"GIDPerson"`
        IdVaccine     int    `json:"idVaccine"`
        Dose          int    `json:"dose"`
        Lot           int    `json:"lot"`
        Local         string `json:"local"`
        (...)
}

type GIDPerson struct {
        hashcode       string  `json:"string"`
        coutrycode     string  `json:"string"`
        docnumber      string  `json:"string"`
        biometrydata   string  `json:"string"`
        biometrynumber string  `json:"string"`
        birthdate      string  `json:"string"`
        validator      string  `json:"string"`
}
```

Listing 2: Fragment of source code of Person, Vaccine, Vaccination, and GIDPerson Smart Contracts.

APPENDIX I - ADDITIONAL FIGURES

Figure 33 – ID-Care Prototype.