Date of publication xxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

ID-Care: a Model for Sharing Wide Healthcare Data

HUMBERTO JORGE DE MOURA COSTA[1,2], (Member, IEEE), CRISTIANO ANDRÉ DA COSTA[1], (Senior Member, IEEE), RODOLFO STOFFEL ANTUNES[1], (Member, IEEE), RODRIGO DA ROSA RIGHI[1], (Senior Member, IEEE), PAUL CROCKER[3], and VALDERI REIS QUIETINHO LEITHARDT[4, 5] (Senior Member, IEEE).

[1]SOFTWARELAB - Software Innovation Laboratory, Applied Computing Graduate Program - PPGCA, Universidade do Vale do Rio dos Sinos - UNISINOS, São Leopoldo, Brazil (e-mail: hjcosta@edu.unisinos.br, {cac, rrighi, rsantunes)@unisinos.br}

[2]IFRS Veranópolis - Instituto Federal de Ciência, Educação e Tecnologia, IFRS, Veranópolis, Brazil (e-mail: humberto.costa@veranopolis.ifrs.edu.br)

[3]Instituto de Telecomunicações and Department of Informatics, University of Beira Interior, Portugal (e-mail: paul.crocker@lx.it.pt)

[4]COPELABS, University Lusófona—ULHT, 1749-024 Lisbon, Portugal

[5]VALORIZA - Research Centre for Endogenous Resource Valorization, Polytechnic Institute of Portalegre, Portalegre, Portugal (e-mail: valderi@ipportalegre.pt)

Corresponding author: Cristiano André da Costa (e-mail: cac@unisinos.br).

This work is funded by FCT/MCTES through national funds and when applicable co-funded EU funds under the project UIDB/EEA/50008/2020.

ABSTRACT All over the world, there is a lot of patient health data in different locations such as hospitals, clinics, insurance companies, and other organizations. In this sense, global identification of the patient has emerged as an everyday healthcare challenge. Governments and institutions have to prioritize satisfactory, quick, and integrated decision-making in a wide, dispersed, and global environment because of unexpected challenges like pandemics or threats. In the current scientific literature, some of the existing challenges include support for a standard global unique identification that considers privacy issues, the combination of multiple technological biometry implementations, and personal documents. Thus, we propose a decentralized software model based on blockchain and smart contracts that includes privacy, global unique person identification supporting multiple combinations of documents, and biometric data using the Global Standards 1 - GS1 healthcare industry standard. Furthermore, we defined a methodology to evaluate a hypothetical use case of this model where an integrated and standard global health data sharing personal identification is crucial. For this, we implemented the proposed model in a global-wide continent location through cloud machines, fog computing, and blockchain considering the unique patient data identification and evaluate a use case scenario based on the top 5 most globally visited tourist destinations (France, Spain, the United States of America, China, and Italy), with an approach based on this model. The results show that using 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.

INDEX TERMS Blockchain, cloud computing, global identification, gs1, healthcare.

I. INTRODUCTION

Many organizations create their service system to differentiate distinct entities in a healthcare system [1]. 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 [2]. A patient on vacation can visit several countries in the same journey, but in each location, will probably have multiple health data and different identification codes [3].

One possible approach for developing healthcare software solutions is the use of standards, such as those from GS1, an international, non-profit global organization that develops and implements standards to improve supply chain management in several industries, including healthcare, and transportation [1]. However, there is currently no implemented official solution for the unique global identification of patients.

One of the main computational technologies used to address the decentralization of data is the Blockchain. Blockchain is a distributed model forming a peer-to-peer network, where cryptographically signed transactions of digital assets take place. The main feature of Blockchain is a distributed ledger technology that helps to address problems of digital transparency, non-repudiation, and trustworthy contracts [4], [5]. The Blockchain network consists of a peer-to-peer distributed ledger database for transactions without the necessity of a central authority or a third-party verification. Some of the benefits provided in a blockchain applied to healthcare are decentralized management, immutable audit trail, data provenance [6], improved security, and availability [7]. The blockchain can also improve medical record management, increase processes, accelerate clinical/biomedical research, and advance biomedical/healthcare data sharing [8].

This article aims to combine blockchain and global unique identification to support distributed healthcare data in a global scenario. The major contribution of this work is to fill the following gaps found in the state-of-the-art of healthcare technology:

- The development of a decentralized software model based on blockchain and smart contracts including privacy, considering global unique person identification, supporting multiple documents, and biometric data whilst respecting a healthcare industry standard [9].
- Propose a methodology for an evaluation of a hypothetical vaccination scenario where an integrated and standard global health data sharing personal identification.

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

II. RELATED WORK

Some of the most important issues and challenges of unique identification for healthcare data are the uniqueness of records [10], compatibility with standards, privacy/security [11], and longevity of records. There are several related works available in the current literature. We selected the most relevant and recent papers related to this field of study through a search using the most well-known scientific databases including IEEE Xplore [12], Science Direct [13] and Google Scholar [14].

Anne et al. [15] propose a prototype of an iris biometric identification system that was created for Unique patient identification. Through pattern analysis, a 12-digit ID number is generated based on a template from those patterns. In the next visits, the patients' irises are re-scanned, and the pattern is matched to saved templates to retrieve this ID number. The Iris recognition biometric identification system tested the feasibility and acceptability of integrating into routine HIV care services at 4 sites in Kenya.

Ambadiy et al. [16] propose a method for creating a unique id based on the core point of the fingerprint of an individual. The minutia features of the fingerprint are extracted with the core point as the reference. The numerical value thus generated is used to create the unique ID in the form of a QR code and this is printed in the security documents.

Mishra et al. [17] propose a zero watermark scheme that solves the problem of biometric data security without moderating the biometric data. The biometric iris pattern is used to develop a digital binary code for iris images. This binary pattern is mixed with a watermark which is the identity of an associated person to create a unique, completely uninformative ID that does not reveal the person's biometric information and identity.

Ren et al. [18] propose an improved information fusion method based on D-S evidence theory to combine fingerprint information and personal identification. Experimental results show that the performance of the proposed algorithm can solve the evidence conflict problem and may effectively improve the precision and performance of fingerprint identification.

Hung et al. [19] introduce a globally unique identifier used for personal health information protection, developed by the National Institutes of Health of the United States, that was used in data collection for a health management study in a Taiwanese aboriginal tribe. This global identifier permits researchers to associate and share data specific to a study participant without the use of personally identifiable information. This global identifier is made up of random alphanumeric characters and is not directly generated from protected health information.

Nguyen et al. [20] propose data sharing for healthcare using edge computing and blockchain. The authors developed an efficient data transfer scheme for privacy-conscious data processing. There is some data integration to allow data exchange between healthcare users through a blockchain network and a control mechanism for sharing EHR data in smart contracts. The results demonstrate superior QoS, enhanced data privacy and security, and low smart contract costs.

Majumder et al. [21] propose an integration of permissioned blockchain and smart contracts using deep learning techniques to design a secure and efficient data-sharing framework called PBDL. This framework includes a blockchain scheme to register, verify, and validate the communicating entities using the smart contract-based consensus mechanism. The architecture is multilayer and is composed of several components representing various entities related to the healthcare environment. Some examples of entities are Patients, doctors, clinics or hospitals, and medical records.

The work of Afaq et al. [22] integrates mobile devices to develop a blockchain-based patient-centric sharing of Electronic Medical Records - EMR supporting data security, data integrity, and patient privacy. Selective sharing of data between different institutions via real-time blockchain is allowed with the permission of patients. Patients have the control to disclose which data can be shared. Furthermore. Patients can easily use mobile devices to scan the doctor-provided QR code and include public key infrastructure for better data security.

In the article by George et al. [23], the authors evaluate existing blockchain-based interoperable solutions and propose a permissioned blockchain solution called Quorum that addresses the security challenges of interoperability data communication in healthcare and proposes a patient-centric data-based approach, where the patient takes control of his/her healthcare data.

In the work of Do et al. [24], the solution named HoloCare is proposed to ensure data security and privacy through blockchain. This software architecture proposal has the objective to implement a single source of the patient's PHR for authentication, permission granting, and remote access to health information data from other Electronic Medical Record - EMR systems.

We organized the studied articles into the following categories: Technology, Unique ID, Cryptography, Hashcode, Privacy, Design, and Standard. The Technology category lists the type of technology used to compose a global id in each article. These technologies include iris scanning, fingerprinting, multiple fingerprinting, watermarks, or documents like national IDs or driver's licenses. The Unique ID category represents the purpose of applying the global id in each respective article. Some articles are generic, such as identifying people, and others may be specific to the identification of patients with a certain disease or to ensure the security of a document. The cryptography category classifies the algorithm as custom, proprietary, open source, or not identified (N. I.). The custom value means that the authors implemented the algorithm, compared to open-source and proprietary solutions. The hashcode category represents which components are included to compose itself. For example, documents like id and driver's license, biometric data such as fingerprint or iris recognition, personal data, or the generation of links to EHR data or QR Codes. The privacy category demonstrates whether or not a determined work allows privacy to be controlled by the person. The design category shows how the data is stored, it may be in a repository, centralized or permanent. The Standard category shows whether an article implements an industry standard or not. If yes, which standard is used. This comparison is shown in Table 1.

Comparing the related work (Summary shown in Table 1) with the proposed model, the uniqueness and longevity of records [10] are implemented in all related works. The implementation of hashcode includes a link to EHR (Anne et al [15]), conversion to QR Code (Ambadiyil et al. [16]), and the support of biometric data (Mishra et al. [17], and Ren et al. [18]). Most of the privacy concerns can be controlled by the applications developed in the related works (Anne et al [15], Ambadiyil et al. [16], and Hung et al. [19]), nevertheless the cryptography method includes proprietary and customized algorithms and not informed for some works.

To summarize, there are some gaps and challenges to overcome:

- Some works implement controllable privacy and security, however, these issues are not a primary concern because data traceability or decentralized data sharing (for example, blockchain) is not implemented.
- None of the related work has included a standard compliance support application.
- Most articles support biometric technologies such as iris scanning and fingerprinting. But, the combination of using data extracted from documents like a national identity card or driver's license, and several biometric traits are not implemented.

To fill these gaps, the ID-Care model proposes to implement privacy and security using a decentralized blockchain network including smart contracts, and supporting multiple combinations of documents, biometric data, and generation of unique global identification id compatible with the EPC Global GS1 Standard implementation [25].

III. MODEL

A. GLOBAL ID HEALTHCARE MODEL OVERVIEW

The model proposed in this article is called ID-Care and aims to contribute to addressing the issues and challenges related to globally unique identification, compliance with standards, privacy/security, and longevity of records previously studied in the literature review. Typically, a user workflow consists of a process from authentication to decision-making (Figure 1). It includes creating a global id for the patient and digitally linking it to their health 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.

- **global unique identification:** The importance of Geographical distribution is because healthcare applications can demand widely, but geographically identifiable, distributed deployments with access points geographically positioned along with a wide scope area [26].
- **compatibility with standards:** The proposed model implements the GS1 standards approach due to support a scalable global solution. The GS1 Global is an organization that has developed patterns to allow healthcare institutions to identify products, patients, clinics, assets, and locations uniquely with a common globally, and unambiguous identification infrastructure for sharing data [1]. The main advantages are the ease of use and usefulness for product identification, precise tracking, and Reliable information availability [27].
- **privacy/security:** Privacy concerns are crucial for health data applications. Blockchain can be used to collect, store and analyze health data smarter and avoid privacy violations [28]. In this proposed model, all the data is stored on blockchain smart contracts due to keeping the integrity and privacy of distributed health-

TABLE 1. Related work comparative.

Article	Technology	Unique ID	Cryptography	Hashcode	Privacy	Design	Standard
Anne et al. [15]	Iris scanning	HIV Patient Identification	Proprietary	Link to EHR	Controllable	Repository	No
Ambadiyil et al. [16]	Fingerprint	Security document	N. I.	Convert to QRCode	Controllable	Repository	No
Mishra et al. [17]	Iris / Watermark	Person Identification	Custom	Iris + Personal Data	N. I.	Centralized	No
Ren et al. [18]	Multi-finger	Person Identification	N. I.	Multi-finger	N. I.	Permanent	No
Hung et al. [19]	Documents	Patient Identification	Custom	Personal Data	Controllable	Permanent	No
Nguyen et al. [20]	Documents	Patient Identification	Custom	None	Controllable	Permanent	No
Majumder et al. [21]	Documents	Patient Identification	Open Source	Id	Controllable	Permanent	No
Afaq et al. [22]	Documents	Patient Identification	Proprietary	N. I.	Controllable	Repository	No
George et al. [23]	Documents	Patient Identification	Proprietary	N. I.	Controllable	Permanent	No
Do et al. [24]	Documents	Patient Identification	Proprietary	Id	Controllable	Permanent	No
ID-Care (this work)	Documents, Biometry, Blockchain	Patient Identification	Open Source	Documents and Biometry	Controllable	Permanent	GS1

care data sharing. Patients can have privacy control of their data. Using a blockchain to store healthcare data provides several benefits like supporting complete, consistent, timely, accurate, and easily distributed data, and agreements without the involvement of a unique trusted mediator.

- **longevity of records:** Blockchains are tamper-evident and tamper-resistant digital ledgers. This ensures that changes in the blockchain healthcare data are transparent to all members of the blockchain network and that all data inserted are immutable. In addition, any unauthorized changes can be detected easily due to the implementation without a central repository or authority such as a company, or government [29]. Blockchain applications can permit a community of users to record transactions in a shared ledger in which no transaction can be changed once published [30], and have the benefits of avoiding performance bottlenecks in contrast to the possible single point of failure of other models.

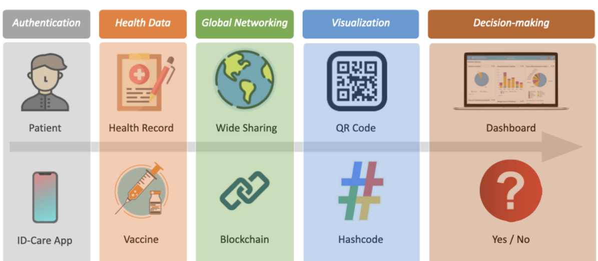

FIGURE 1. Global ID.

The overview of the ID-Care model is composed of seven components: Health Professionals, Hospitals, ID-Care Desktop, and mobile application, blockchain network, ID-Care QR Code, and Patient, as described as follows:

- **Health Professionals:** Professionals such as doctors, nurses, physical therapists, psychiatrists, and assistants. These professionals work in hospitals or other healthcare facilities. They usually attend to patients and operate the ID-Care Desktop of mobile software.
- **Hospitals:** organizations that can be geographically distributed places between countries and continents such as hospitals, clinics, and laboratories. Each organization can enroll new patients on ID-Care software by a desktop application or app. Each hospital has its health professionals and staff. The ID-Care software verifies if the patient is already enrolled, according to documents and biometric data when a member of hospital staff registers an appointment.
- **ID-Care Desktop:** Software running on hospitals that allow enrollment or querying 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 App:** Mobile App that the patient may use to identify himself or herself as a global unique patient through a QR Code generated by the ID-Care Software. This app is available globally, for all persons around the world.
- **Blockchain Network:** A decentralized network supporting blockchain smart contracts such as Hyperledger or Ethereal.
- **ID-Care QR Code:** QR-Code generated by the ID-Care software based on a global unique hashcode from patient's documents and biometric data.
- **Patient:** A person who goes to a healthcare facility because they need health services. This person will be enrolled on ID-Care software if not already enrolled. The ID Care is the same in all countries for the same person.

B. GLOBAL ID HEALTHCARE MODEL COMPONENTS

The proposed model has 5 layers: Legal Document, Biometry, ID Services, and Visualization (Figure 2).

- **Legal Document:** this layer is responsible for the legal traceability of a person. According to the country of origin, several documents can be accepted. For instance, a national id, health id, and passports are widely used by countries for citizen identification. To register a patient in ID-Care, it is necessary that they legally exist and that it is traceable, no matter where he was born. One of the

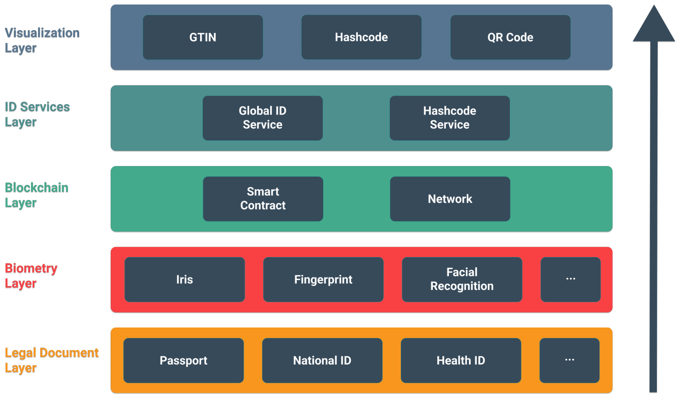

FIGURE 2. Global ID Model.

ways to guarantee this is by using documents from the country of origin or current residence. This layer is the base for the other layers because one person must legally exist and be mapped to only one single record in the world.

- **Biometry:** Various countries use different biometric 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. Note, for example, that there are many forms of face recognition, but they all result in a number or string that can be used as a primer 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 biometry layer is used in the model according to each country because 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 main 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. The implementation of ID Services in API format can allow future integration with government health services applications of all interested countries or academic research studies conducted by universities or international health organizations.
- **Visualizarion Layer:** In the visualization layer, GTIN, hashcode and QRCode visualizations 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.

IV. MATERIAL AND METHODS

For the evaluation of this work, we proposed a use case of a global vaccination campaign against the COVID-19 virus. The World Health Organization recognizes and suggests policy considerations for implementing a risk-based approach to international travel in the context of COVID-19 [31]. The health data about worldwide patients are distributed in a continent geographical space. This simulation of a global vaccination scenario has the objective to verify if the proposed model supports the requirements to address the challenges of healthcare integration data using a global healthcare unique id strategy. For this, as follows we describe in detail this scenario, the implementation of each layer (ID Services, Legal Document, Biometry, Blockchain, ID Services, Visualization), and the development of the prototype mobile application for the use of the people.

A. GLOBAL SHARING DATA SCENARIO

To evaluate the model a use case is proposed, namely 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 define some important steps necessary to achieve this objective:

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

B. LEGAL DOCUMENT LAYER

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 Social Security Number (SSN) in the USA or Cadastro de Pessoas Físicas (CPF) in Brazil. In general, the IDs have requirements for validation. For instance, in the USA the SSN has the following requirements:

- It contains 9 digits.
- It can be divided into 3 blocks separated by a hyphen.
- The first block must have 3 digits and cannot be 000, 666, or between 900 and 999.
- The second block must have 2 digits and it is between 01 to 99.

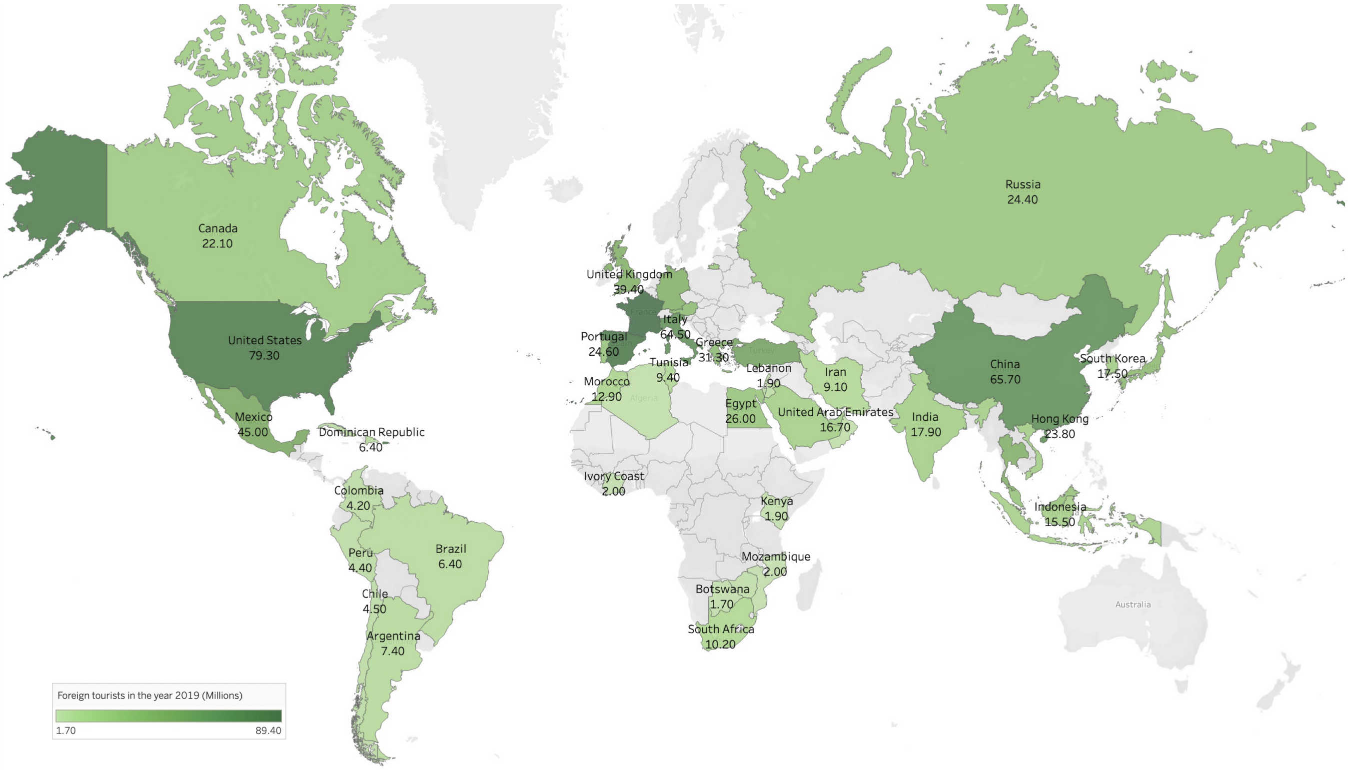

FIGURE 3. Number of foreign tourists by country in 2019 (Millions).

- The third block must have 4 digits and it is between 0001 to 9999.

A regular expression to recognize a SSN would be viable however it would not be uniquely viable on a global scale as each different document format would require a different validation.

Each country has its own system of identification, including a different method of validation. For example National identity cards are issued by the governments of all European Economic Area (EEA) member states except Iceland Denmark, and Ireland however the exact underpinning technologies may differ widely. In China, the Resident Identity Card is an official identity document for personal identification in the People's Republic of China. The identity card contains basic information like full name, gender, ethnicity, birth date, domicile, and personal photo. Since 1999, there is a citizen identification number consisting of an 18-digit code. This number is formed by the first five numbers of the address code, the next 8 numbers the birth date, and the next 3 digits, a code used to disambiguate people with the same birth date and address code, and the last one a verification code. Furthermore, in some countries around the world other documents are often used, like health identification numbers, driver's licenses, and so on. Because of this, in the implementation of this work, the definition of ID-Care supports a validation method for each document and country.

C. BIOMETRY LAYER

A wide variety of biometric technologies may be found in use around the globe. The main technologies are: fingerprinting scanning, iris recognition, and facial recognition. Even, the same technology such as facial recognition can have many different algorithmic implementations.

The way different biometric systems are used together can also vary. For instance, in Brazil, the election is implemented by an electronic ballot box. The person that will vote must be enrolled in a fingerprint-based authentication software, as a requirement. This fingerprint, and face recognition system, currently can be used to identify a citizen in other government software applications.

Within the European Union fingerprints and facial images are often mandatory in ID cards of EU citizens and residence cards of their non-EU family members and, depending on the country, can be used for regulatory purposes in several domains, such as identification, fully qualified digital signatures, and a number of private and public services such as opening a bank account or requesting birth certificates.

Although each country has its own system of biometry, the result is generally a string or number representing the image, so the ID-Care software must have a comparison method to test if this result is equal to or different than the stored data of a patient.

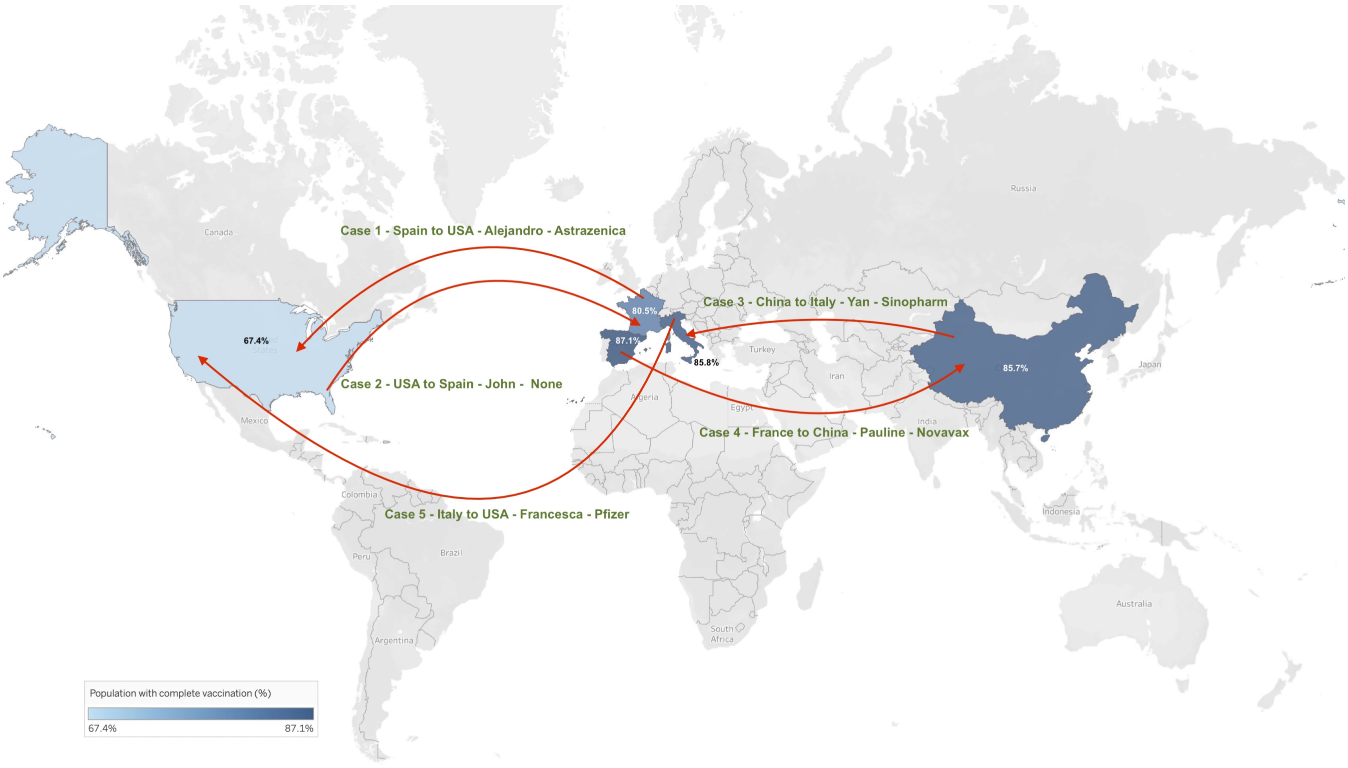

FIGURE 4. Vaccination use cases.

D. BLOCKCHAIN LAYER

The blockchain layer is divided into two parts: network and smart contracts. The network part consists of a private hyperledger blockchain model defined by Costa et al. [32]. The main feature of this module is to include a peer, remove a peer and authenticate peers and users, according to the health facilities organization. In the smart contract module, coded to the Go language, it is possible to register and insert new information about the patients and vaccination processes. There are several smart contracts dealing with the solution. The smart contracts created are included in the Listing 2

E. ID SERVICES LAYER

There are two modules in ID Services: the Hashcode Service and the Global ID service. In the first one, the Hashcode Service is responsible to generate the global id hashcode based on the EPC Global GS1 Standard. The format is shown in Figure 5. There are 7 parts to this hashcode: country code, document type, document number, biometry data, biometry number, birth date, and validator. A summary of fields can be visualized in Table 2.

- **Country Code:** The country code is the standardized GS1 code that the patient was born. In our hypothetical vaccination scenario, including USA, 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 the documents available to use. For instance, 001 id, 002 driver's license, 003 passport, and so on. For our hypothetical scenario, the values chosen 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 is formed by 11 digits. Once the field is composed of 14 numbers (Table 2, we need to include 000 on the left of the number of patients in this country. The hypothetical values are 00098765678912, 00000463786537, 00008356789871, 00599287656839, and 00000006543287.
- **Biometry data:** The biometric type is a 3 digits code representing the 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 possibility. For our scenario, the values are 002, 001, 002, 001, and 001 respectively.
- **Biometry number:** Biometric number represents the result of the image of the biometry chosen (ie.:the last 48 of fingerprint, iris, or face image), if greater than this number (For example, Table 3.
- **Birth date:** The birth date represents the date of birth of a patient in the format "year month day". The values in the scenario are 19940212, 19850430, 19720915,

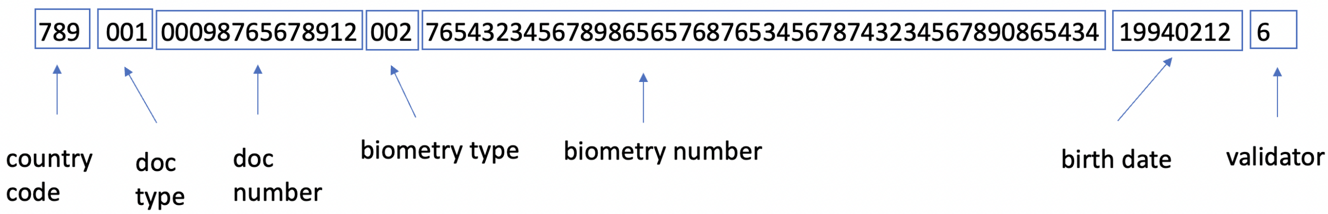

FIGURE 5. Hashcode Implementation.

TABLE 2. Summary of ID-Care 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	765432345678986565768765345678743234567890865434
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	Id-care://1b0517faa833231f92a23104800e92f5eeeb296f3346da9e1e68b7a2...

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 [25]. To generate the validator is necessary to follow these steps:
  - **Step one:** Set up a table with 80 columns, and put the number to be checked, 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 if the digit is the smallest value necessary to round the result of Step Five up to the nearest multiple of 10. Figure 5 shows the first hashcode generated in our scenario. The Listing 1 is the completed code for validation.

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

F. VISUALIZATION LAYER

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

- **hashcode:** The visualization in hashcode format is shown in the Figure 5. This format allows the investigation of the fields that form the patient data. It is stored in a blockchain with privacy control.
- **GTIN:** The GTIN format is the hashcode with a SHA512 cryptography algorithm forming the Global ID, including a prefix "id-care://". The objective is to point the address to the use of an app or software to manipulate this address.
- **QR Code:** The QR Code format is generated by the application from the Global ID Data.

G. PROTOTYPE

The requirement for this process is to support globally unique patient identification. 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. The screens of the prototype for the use of patient is shown in Figure 7. The following actions (Figure 7 b)) can be made by the patients: login, schedule vaccination, get the vaccine, show your global ID, and see your profile.

- **Login:** the login process (Figure 7 a))is made through a user name and password or by the cell phone biometry. These logins are registered by the hospital staff during the first use of the patient.
- **Schedule vaccination:** This option allows the patient to schedule a vaccine shot by entering the vaccine type, date, time, and local (hospital, clinic, etc.) application (Figure 7 c)).
- **Get the vaccine:** It is used in the vaccination process. If everything is right, is shown the Passed! message (Figure 7 g)) including the vaccination data, otherwise the Failed message (Figure 7 f)) and the reason for failure.
- **Global ID:** This option shows the patient Global ID QR Code and hashcode (Figure 7 d)) to optimize the service.
- **Profile:** This selection shows all the patient profile data (Figure 7 e)), and is used to the patient know your data and make sure it is correct.

In the next subsections, we will analyze each one of the layers considering this use case and hypothetical scenario, as

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3249109

TABLE 3. 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 4. Global ID from hashcodes.

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

Patient 1 Patient 2 Patient 3 Patient 4 Patient 5

FIGURE 6. ID-Care QR Code of Patients.

shown in Figure 8.

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 application 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 the patient's information in the ID-Care registration application, it is verified that the patient does not yet have a global id. Then, the application generates a new ID associated with this patient and authorization for the first access by the application. Data validation takes place through documents and/or biometric data that are entered according to the patient's information provided.

V. RESULTS

A. VACCINATION SCENARIO RESULTS

The results of the implementation of the hypothetical scenario are shown as follows.

A case study was made 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 5 steps: select countries participating in the proposed scenario, collect relevant tourism and population data, gather COVID-19 vaccination data, define possible tourism mobility use cases, and analyze the proposed scenario suggesting possible protective sanitary measures. These steps are described as follows:

1) **Select 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 5). The objective of the selection of 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 3).

TABLE 5. 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 its relevant tourism and population data:** The next step is to gather official inbound tourism data from different countries. We have carefully chosen the number of tourists in 2019, before the pandemic, to represent the normal tourist demand in these countries

FIGURE 7. ID-Care Prototype.

TABLE 6. 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**

[33]. Regardless of these countries, we can see the huge demand for a global healthcare identification ID by analyzing the number of tourists around the world in millions of foreign visitors (Figure 3) and the international income revenue of this countries in 2019 (before pandemic) and 2020 (after pandemic) seen in Table 6.

Numbers within asterisk are estimated. For the tourism and population data we used the Eurostat [34] [35] for Europe, World Data [36] [37] for China, and Statista [38], and [39] for the USA. The revenue data comes from The World Bank [40]. These sources are based on official numbers of respective governments, except China.

3) **Gather COVID-19 vaccination data:** For the collection of vaccination data, The website Our World of Data [41] from the University of Oxford is a world reference, as it contains a huge compilation of vaccination data in various formats, from text, maps, and graphics, and is well-known for its data update on vaccination of the COVID-19 [42]. We include the data

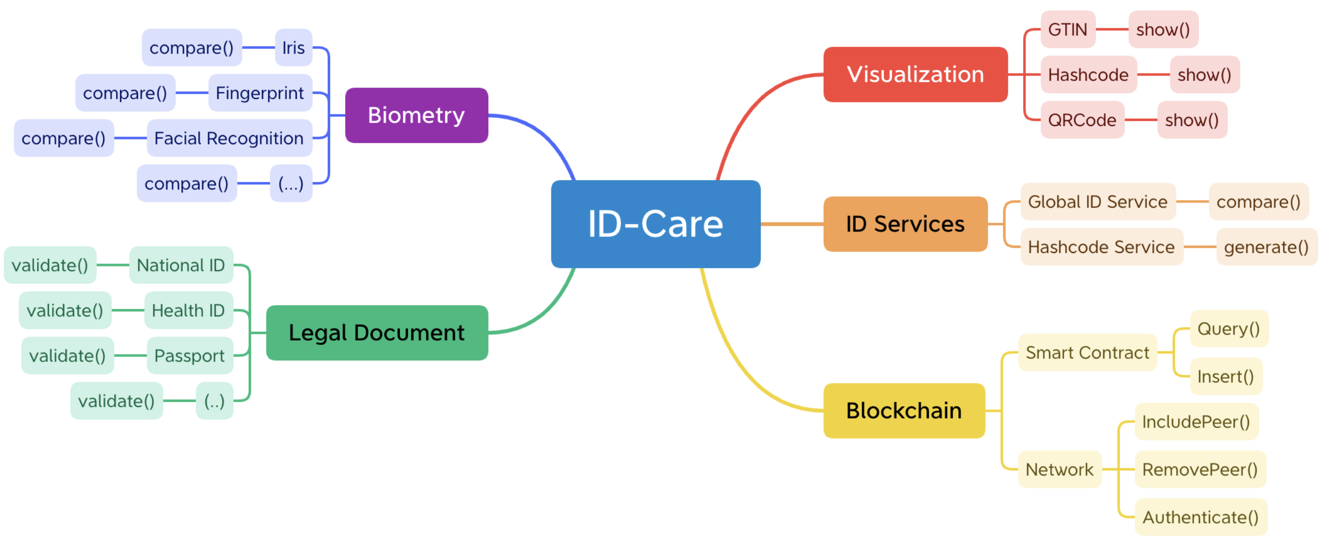

FIGURE 8. Taxonomy of ID-Care Model Services.

of vaccination until August 31, 2022, as seen in Tables 7, and 8. We also considered each country has chosen a different brand of vaccines. Furthermore, there are some differences in the time and number of doses administered (Table 9).

TABLE 7. 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%

TABLE 8. 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%

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 4, and are described as follows:
   - **Case 1:** Alejandro is a 32-years-old Spaniard who is traveling from Spain to the USA. He was vaccinated with AstraZenica 30 days ago.
   - **Case 2:** John is a 22-years-old American traveling from 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 may be applied by the health authority. For example, after a tourist arrives there could be 3 standard recommendations after analyzing the global tourist identification information provided by the Global ID Vaccination software: 1 - accept without restrictions the entry of the traveler, 2 - deny the traveler entry, or 3 - apply a requirement such as give a booster dose of the COVID-19 vaccine or another preventive sanitary measure, to accept the traveler's entry into the country. Analyzing case 1, Alejandro is trying to enter the USA, and he is vaccinated with AstraZenica. Because there is no AstraZenica vaccine in the USA (Table 9), the Global ID software suggests the health authority of this country to give a booster Dose of Pfizer, and after that accept the traveler. The case 2, John, a young American is arriving in Spain. The Global ID software recognizes john as a COVID-19 unvaccinated. So, the software suggests denying entry into the country. Case 3 is about Yan, an old Chinese man that is arriving in Italy. The Global ID software detects his old age and recognizes he is vaccinated with Sinopharm. The software suggests a booster dose of

TABLE 9. 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

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 to the health authority of China give a booster dose of Sinopharm and accept the traveler due to Novavax still being given to a low percentage of people in the world. 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 because he is vaccinated with Pfizer, a vaccine recognized in the USA. Considering the scenario which Id-Care model is used, and the vaccine were ready to use, approximately 80% of all incoming tourists were able to enter the analyzed countries.

In addition, different from related works, we demonstrate that this proposed model is feasible for implementation due to its standardization and usefulness in an healthcare environment that has a large number of foreign visitors from several countries and several specificities involved. Another differential is that this model supports any technology used for identification in the country of origin, from national identification numbers to patient biometrics data.

VI. DISCUSSION

The ID-Care proposed model combined several features for implementing the support for unique global identification patients with a focus on healthcare.

In the case of vaccination scenario results, the use of Global ID software can match historical data from the profile of travelers with global vaccination data and help the health authority of participant countries to establish a dynamic decision-making strategy based on global information knowledge about vaccines and people to decide about health public politics.

These differential results of the Global ID come from the unique characteristics of the model, such as the support of smart contracts and decentralized network. While some related works implemented controllable privacy and security, they do not support decentralized data sharing and traceability. This lack of feature affects the the gaps in the longevity of records and privacy/security concerns found in the current literature.

Another important challenge found 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 a 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 the related health data, the speed of service was instantaneous and this proposes the reduction of several costs and the possibility of adopting important sanitary protection measures.

With the implementation of a global ID, some issues need to be addressed. The documents of identification of people will almost vary in type, format, and length of numbers. The related works do not provide any strategy to deal with different documents coming from different places. Some countries use a national id, and individual taxpayers' numbers, among others. The biometry technology involved with this identification, such as fingerprinting or face recognition must be considered because it provides an important level of security and unique identification. The majority of related works support some type of biometry identification, but different of this proposal only supports one unique biometry, generally fingerprinting or iris recognition. The proposed model implements the support of several biometry technologies simultaneously and together with id 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 standards. None of all the related works supports a global standard. The proposed model was developed to support the EPC Global GS1 Standard, which is widely known. We implemented all the code numbers according to the GS1 guidelines, including the validation code of the hashcode proposed. The hashcodes generated in the scenario are examples of this standard applied.

A piece of relevant information considered was the number of tourists in the year 2019 in the top 5 tourists who arrived in the countries. this number varies from 64.5 million (Italy, in fifth place) to 89.4 million (France, first place). It implies a huge potential necessity for vaccination for foreign tourists. In the scenario proposed, we can notice that different brands of vaccines are applied to the people according to each country. Pfizer leads in France, Spain, the United States, and Italy. Janssen was the only vaccine of unique shot and could be advantaged, but only Italy and Spain were applied.

The prototype results, ensure the feasibility of the applications. Some data such as the fields Country, Doc Type, Doc Number, Bio Data, Bio Number, Birth Date, and Validator supported the enrolment of patients from different countries successfully.

These fields only contain immutable data such as the birth date and country of origin. The field validator ensures that all other fields are with integrity. The use of blockchain smart contracts helps the reliability, privacy, and security of the data. The support of GS1 standards is another differentiation from related works.

The use of a blockchain network and an open source SHA512 algorithm to cryptography of the original hashcode hides sensitive information from a not authorized person at the same time that creating a unique and generated number with support of privacy.

For general use, and visualization, the model implemented a QR code generated from the GTIN number. This allows for a better user interface for patients and health professionals, which can only need a smartphone with a camera and internet connection to use the features quickly. The set of unique features, such as the traceability of documents together with the support of biometry technologies of the model differentiates from standard approaches found in the related works.

Considering the proposed scenario of vaccination of inbound tourists of the top 5 tourist countries in the world, taking 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 value of 79.3 millions of visitors is similar, and China with 65.7 million of visitors, this proposed work has the potential to contribute for implementation of global scale sharing healthcare data strategies. The huge number of visitors and the implementation of this Global ID model on a global scale has the potential of reducing costs, time, and efforts to help to control and mitigate the effects of threats like possible pandemics or even any disease that depends on vaccination or any other healthcare data sharing global scenario.

VII. CONCLUSION

We implemented a globally unique identifier for patients in a scenario of global scale sharing for healthcare data. In addition, we analyzed tourism data in the five most visited countries in the world and compared it with known COVID-19 vaccination data. The results have shown that the use of a global identification architecture for health can generate several useful suggestions in public health policies depending on the specifics of each country and the health data shared with the participants. In short, the proposed architecture can help reduce costs, time and efforts, especially in the context of a pandemic. Future work includes implementing additional features such as a web application to support global information for governments, healthcare providers and Universities for supporting research. We will also implement more features such as machine learning prediction and the study of privacy and security issues involved. This model supports multiple global health data-sharing scenarios, not limited to tourism, pandemics, or vaccination. Some examples are emigration, international collaboration in research in health, and public health policies.

ACKNOWLEDGMENTS

The authors would like to thank the Coordination for the Improvement of Higher Education Personnel - CAPES (Finance Code 001), the National Council for Scientific and Technological Development - CNPq (Grant Numbers 309537/2020-7 and 40572/2021-9) for supporting this work, and Instituto Federal de Educação, Ciência e Tecnologia (IFRS) for funding parts of this study. This work was supported in part by FCT/MCTES through national funds and when applicable co-funded EU funds under the project UIDB/EEA/50008/2020. This work was supported in part by the Fundação para a Ciência e a Tecnologia under Project UIDB/04111/2020. We would like to thank Seed Funding ILIND—Instituto Lusófono de Investigação e Desenvolvimento, project COFAC/ILIND/COPELABS/3/2020.

.

APPENDIX A CODE LISTING

```
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.

REFERENCES

[1] GS1, "About gs1," https://www.gs1.org/about, 2020.
[2] H. J. de Moura Costa, C. A. da Costa, R. da Rosa Righi, and R. S. Antunes, "Fog computing in health: A systematic literature review," *Health and Technology*, vol. 10, no. 5, pp. 1025–1044, 2020.
[3] B. K. Smith, H. Nachtmann, and E. A. Pohl, "Improving healthcare supply chain processes via data standardization," *Engineering Management Journal*, vol. 24, no. 1, pp. 3–10, 2012.
[4] J. Al-Jaroodi, N. Mohamed, and E. Abukhousa, "Health 4.0: On the way to realizing the healthcare of the future," *IEEE Access*, vol. 8, pp. 211 189–211 210, 2020.
[5] G. Leeming, J. Ainsworth, and D. A. Clifton, "Blockchain in health care: hype, trust, and digital health," *The Lancet*, vol. 393, no. 10190, pp. 2476–2477, 2019.

```
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"`
        ExpiryDays    int    `json:"expiryDays"`
    (...)
}

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.

[6] F. Pereira, P. Crocker, and V. R. Leithardt, "Padres: Tool for privacy, data regulation and security," *SoftwareX*, vol. 17, p. 100895, 2022.

[7] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Computing and Applications*, pp. 1–16, 2021.

[8] A. Rejeb and L. Bell, "Potentials of blockchain for healthcare: Case of tunisia," *Available at SSRN 3475246*, 2019.

[9] A. H. Mayer, V. F. Rodrigues, C. A. d. Costa, R. d. R. Righi, A. Roehrs, and R. S. Antunes, "Fogchain: A fog computing architecture integrating blockchain and internet of things for personal health records," *IEEE Access*, vol. 9, pp. 122 723–122 737, 2021.

[10] N. Vohra and N. Jain, "Synchronization of health informatics with "aadhaar"(uid: Unique identification)," in *International Joint Conference on Advances in Signal Processing and Information Technology*. Springer, 2011, pp. 201–204.

[11] V. Leithardt, D. Santos, L. Silva, F. Viel, C. Zeferino, and J. Silva, "A solution for dynamic management of user profiles in iot environments," *IEEE Latin America Transactions*, vol. 18, no. 07, pp. 1193–1199, 2020.

[12] "Ieee xplore," https://ieeexplore.ieee.org, 2021, accessed: 2021-07-09.

[13] "Science direct," https://www.sciencedirect.com, 2021, accessed: 2021-07-09.

[14] "Google scholar," https://scholar.google.com, 2021, accessed: 2021-07-09.

[15] N. Anne, M. D. Dunbar, F. Abuna, P. Simpson, P. Macharia, B. Betz, P. Cherutich, D. Bukusi, and F. Carey, "Feasibility and acceptability of an iris biometric system for unique patient identification in routine hiv services in kenya," *International journal of medical informatics*, vol. 133, p. 104006, 2020.

[16] S. Ambadiyil, K. Soorej, and V. M. Pillai, "Biometric based unique id generation and one to one verification for security documents," *Procedia Computer Science*, vol. 46, pp. 507–516, 2015.

[17] M. Mishra, A. Bhattacharya, A. Singh, and M. K. Dutta, "A lossless model for generation of unique digital code for identification of biometric images," in *2018 4th International Conference on Computational Intelligence & Communication Technology (CICT)*. IEEE, 2018, pp. 1–5.

[18] X. Ren, J. Yang, H. Li, and R. Wu, "Multi-fingerprint information fusion for personal identification based on improved dempster-shafer evidence theory," in *2009 International Conference on Electronic Computer Technology*. IEEE, 2009, pp. 281–285.

[19] J.-F. Hung, H.-H. Rau, C.-Y. Hsu, S.-C. Chen, D.-J. Tsai, Y. Fann, J. Park, and J. Eng, "Implementing globally unique identifier architecture in date collection for a health management study in taiwan aboriginal tribe," in *Future Information Technology-II*. Springer, 2015, pp. 121–127.

[20] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "A cooperative architecture of data offloading and sharing for smart healthcare with blockchain," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2021, pp. 1–8.

[21] A. Majumder, S. Saha, T. Bhowmik, and A. Basu, "A conceptual framework for blockchain-based intelligent healthcare data management," in *2021 IEEE Bombay Section Signature Conference (IBSSC)*. IEEE, 2021, pp. 1–6.

[22] K. M. Afaq, Y.-Y. Tsai, Y.-C. Chen, Z.-Y. Shae *et al.*, "Mobile-based patient-centric emr sharing system using blockchain," in *2022 IEEE 4th Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS)*. IEEE, 2022, pp. 217–220.

[23] M. George and A. M. Chacko, "A patient-centric interoperable, quorum-based healthcare system for sharing clinical data," in *2022 International Conference for Advancement in Technology (ICONAT)*. IEEE, 2022, pp. 1–6.

[24] H. Do Hoang, T. C. Nhut, P. D. T. Quyen, P. T. Duy, V.-H. Pham *et al.*, "A blockchain-based secured and privacy-preserved personal healthcare record exchange system," in *2021 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT)*. IEEE, 2021, pp. 1–5.

[25] "Check digit calculator. how to calculate a digit check manually," https://www.gs1us.org/DesktopModules/Bring2mind/DMX/Download.aspx?EntryId= 2022, accessed: 2022-07-13.

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

[27] D. Kritchanchai, S. Hoeur, and P. Engelseth, "Develop a strategy for improving healthcare logistics performance," in *Supply Chain Forum: An International Journal*, vol. 19. Taylor & Francis, 2018, pp. 55–69.

[28] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.

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

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

[31] "Technical considerations for implementing a risk-based approach to international travel in the context of covid-19," https://www.who.int/publications/i/item/WHO-2019-nCoV-Policy-Brief-Risk-based-international-travel-2021.1, 2021, accessed: 2022-09-06.

[32] H. J. D. M. Costa, C. A. Da Costa, R. D. R. Righi, R. S. Antunes, J. F. D. P. Santana, and V. R. Q. Leithardt, "A fog and blockchain software architecture for a global scale vaccination strategy," *IEEE Access*, vol. 10, pp. 44 290–44 304, 2022.

[33] W. T. Organization, "World tourism barometer," *World Tourism Organization*, vol. 18, 2020.

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

[35] "Population change - demographic balance and crude rates at national level," https://ec.europa.eu/eurostat/databrowser/view/tps00001/default/table, 2022, accessed: 2022-09-06.
[36] "China population 2019," https://www.worldometers.info/world-population/china-population/, 2019, accessed: 2022-09-06.
[37] "China population 2022," https://www.worldometers.info/world-population/china-population/, 2022, accessed: 2022-09-06.
[38] "Resident population of the united states from 1980 to 2021," https://www.statista.com/statistics/183457/united-states–resident-population/, 2019, accessed: 2022-09-06.
[39] "U.s. population estimated at 332,403,650 on jan. 1, 2022," https://www.census.gov/library/stories/2021/12/happy-new-year-2022.html, 2022, accessed: 2022-09-06.
[40] "International tourism, receipts (current us$) - united states, france, spain, china, italy," https://data.worldbank.org/indicator/ST.INT.RCPT.CD?end=2020&locations=US-FR-ES-CN-IT&start=1999, 2022, accessed: 2022-09-19.
[41] "Number of people vaccinated against covid-19 august 31, 2022," https://ourworldindata.org/covid-vaccinations, 2022, accessed: 2022-09-06.
[42] E. Mathieu, H. Ritchie, E. Ortiz-Ospina, M. Roser, J. Hasell, C. Appel, C. Giattino, and L. Rodés-Guirao, "A global database of covid-19 vaccinations," *Nature human behaviour*, vol. 5, no. 7, pp. 947–953, 2021.

HUMBERTO JORGE DE MOURA COSTA is a full professor at Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul - IFRS. He holds a Ph.D. degree in Applied Computing Graduate Program at Universidade do Vale do Rio dos Sinos - UNISINOS. He is a member of the ACM, and IEEE.

CRISTIANO ANDRÉ DA COSTA is a full professor at Universidade do Vale do Rio dos Sinos (Unisinos), Brazil, and a researcher on productivity at CNPq (National Council for Scientific and Technological Development). His research interests include ubiquitous, mobile, parallel and distributed computing. He obtained his Ph.D. degree in computer science from the UFRGS University, Brazil, in 2008. He is a member of the ACM, IEEE, and the Brazilian Computer Society.

RODRIGO DA ROSA RIGHI is assistant professor and researcher at University of Vale do Rio dos Sinos, Brazil. Rodrigo concluded his post-doctoral studies at KAIST — Korea Advanced Institute of Science and Technology, under the following topics: RFID and cloud computing. He obtained his Ph.D. degree in Computer Science from UFRGS, Brazil, in 2009. His research interests include load balancing and process migration. He is a member of IEEE and ACM.

RODOLFO STOFFEL ANTUNES is an assistant professor and researcher at Universidade do Vale do Rio dos Sinos (UNISINOS). He holds a B.Sc. degree in Computer Science from UNISINOS (2009) and a Ph.D. degree in Computer Science from the Universidade Federal do Rio Grande do Sul (UFRGS, 2016). His research interests include Internet-of-Things, Information-Centric Networking, Distributed Systems, and Mobile and Ubiquitous Computing.

PAUL ANDREW CROCKER graduated with a Ph.D. in Applied Mathematics from the University of Leeds in 1993. Since 1996 he is a Professor at the Department of Informatics at the University of Beira Interior. He is also a Researcher in the Institute of Telecommunications (IT), member of the RELiablE And SEcure Computation Group (RELEASE) and collaborator with the Space & Earth Geodetic Analysis Laboratory (SEGAL). His research interests are Information Security and Privacy, Operating Systems and Parallel and Distributed Programming, in particular blockchains, web services and cloud computing.

VALDERI REIS QUIETINHO LEITHARDT received the Ph.D. degree in computer science from INF-UFRGS, Brazil, in 2015. He is currently a Professor with the Polytechnic Institute of Portalegre and a Researcher Integrated with the VALORIZA – Research Centre for Endogenous Resource Valorization. Also a collaborating researcher of the Expert Systems and Applications Laboratory (Esalab) of the University of Salamanca, Spain. The mainline of research is in distributed systems with a focus on data privacy, communication, and programming protocols, involving scenarios and applications for the Internet of Things, smart cities, BIG DATA, cloud computing, and Blockchain.