An agent-based secure privacy-preserving decentralized protocol for sharing and managing digital health passport information during crises

Akram Y. Sarhan Corresp. [1]

[1] Department of Information Technology, College of Computing and Information Technology, University of Jeddah, Jeddah, Saudia Arabia

Corresponding Author: Akram Y. Sarhan
Email address: asarhan@uj.edu.sa

The aim of this paper is to identify a range of changes and challenges that present-day technologies often present to contemporary societies, particularly in the context of crisis management and logistics. The long-term consequences of the COVID-19 Pandemic, such as life losses, economic damages, and privacy and security violations demonstrate the extent to which the existing designs and deployments of technological means are inadequate. In fact, there is a need for restructuring the entire gamut, and forging more effective procedures in accordance with the gravity of the crisis. With this in mind, the paper proposes a privacy-preserving decentralized, secure protocol, which can both safeguard individual boundaries and supplies governments and public health organizations with cost-effective information, particularly in terms of vaccination. The contribution of this paper is threefold: (i) conducting a systematic review of most of the privacy-preserving apps and their protocols created during Pandemics, and we found that most apps pose privacy violations. (ii) proposing an agent-based, decentralized private set intersection (PSI) protocol for anonymously protecting and sharing individual digital personal and health information through digital passport during a crisis, the proposed scheme is called Secure Mobile digital passport agent (SMDPA) and (iii) providing a simulation measurement of the proposed protocol to assess performance. Unlike other digital passport protocols, our protocol combines the following core needed features (i) interoperability, (ii) fit privacy standards and regulations,(iii) fault tolerance, and (iv) data minimization.

An agent-based secure privacy-preserving decentralized protocol for sharing and managing digital health passport information during crises

AkramY.Sarhan

Department of Information Technology, College of Computing and Information Technology, University of Jeddah, Jeddah, Saudi Arabia

Abstract

The aim of this paper is to identify a range of changes and challenges that present-day technologies often present to contemporary societies, particularly in the context of crisis management and logistics. The long-term consequences of the COVID-19 Pandemic, such as life losses, economic damages, and privacy and security violations demonstrate the extent to which the existing designs and deployments of technological means are inadequate. In fact, there is a need for restructuring the entire gamut, and forging more effective procedures in accordance with the gravity of the crisis. With this in mind, the paper proposes a privacy-preserving decentralized, secure protocol, which can both safeguard individual boundaries and supplies governments and public health organizations with cost-effective information, particularly in terms of vaccination.

The contribution of this paper is threefold: (i) conducting a systematic review of most of the privacy-preserving apps and their protocols created during Pandemics, and we found that most apps pose privacy violations. (ii) proposing an agent-based, decentralized private set intersection (PSI) protocol for anonymously protecting and sharing individual digital personal and health information through digital passport during a crisis, the proposed scheme is called Secure Mobile digital passport agent (SMDPA) and (iii) providing a simulation measurement of the proposed protocol to assess performance. Unlike other digital passport protocols, our protocol combines the following core needed features (i) interoperability, (ii) fit privacy standards and regulations,(iii) fault tolerance,and (iv) data minimization.

Introduction

The internet has made the world a small, global village, enabling people and businesses to interact and exchange ideas in order to solve various challenges on the planet Earth. However, unpredictability, ambiguity, and complexity are significant issues of modern life in the 21st century (Hassankhani et al., 2021). For example, the death toll and economic damages due to unpredictable crises related to climate change and widespread diseases show how vulnerable humans are in the face of such calamities. Furthermore, the paucity of effective standardized international planning, policies, tools, strategies, and protocols to deal with sudden changes and disturbances (Hassankhani et al., 2021) makes it extremely difficult to interact adequately and efficiently with various phenomena. It, therefore, stands to reason to argue that, not only could innovative technology be a promising tool for addressing potential disasters, but also the need for efficient data and information management is essential—for example, SARS-CoV, H1N1, MERS-CoV, Ebola, Zika, and SARS-CoV-2 viruses.

The digitization of the healthcare process has also played a crucial role during crises in enhancing the healthcare systems via various emerging technology, such as telemedicine, augmented reality, artificial intelligence, big data, electronic health records, and mobile health (Hassankhani et al., 2021). Moreover, the Pandemic crisis of the Covid-19 has accelerated the digitization of social life to the extent that E-learning, remote working, and remote services were all core tools in coping with the adversity (Van et al., 2020).

Besides data management and coordination, digital technology adoption has been essential to the collection of data for better crisis management strategies. Many applications have been deployed for contact tracing, screening, health data information collection, symptom monitoring, facial recognition, global positioning system (GPS) data extractions, and facemask detection (Whitelaw et al., 2020; Elsayed et al., 2021). The integration of emerging technologies such as 5G wireless technology, artificial intelligence (AI), Blockchain, big data, drone (Al-Gburi A, Abdullah O, Sarhan A Y,) and cloud computing into crisis-based applications plays an indispensable role in handling crises,be it monitoring, preventing, or controlling. However, several issues and concerns have been raised, including the absence of robust interoperability, and the lack of global standardization on data collection between databases (Greene et al., 2021), privacy, security (Borra S, 2020), weak and insecure infrastructures (Raisaro et al., 2020) app storage, and implementation models.

The existence of global standards and interoperability between database institutions at the local or international level could enable intersectoral collaborations (Shokoohi, Osooli&Stranges, 2020) and support effective coordination and decision-making process at wide (Luengo-Oroz et al., 2020).However, the current technical limitation in interoperability and standardization, including privacy and security, restricts the scope of coordination between nations. As Professor AriLightman from Carnegie Mellon stated, “As data becomes more of an asset, it becomes difficult to exchange that data across multiple different parties in an ecosystem” (Hern, 2021). Thus, apps interoperability, including backend servers, must be essential for practical cross-border infection tracking and monitoring; however, there are some issues concerning whether to choose the centralized or decentralized model, the data sharing mechanisms, the mass of the public participant, the technical difficulties and functioning of the apps, and the reliability of smartphones sensors and components, such as GPS, and the Bluetooth signals (Ciucci & Gouardères, 2020).

Privacy-preserving is yet another important matter that has raised serious concerns during the COVID-19 Pandemic. Mobile apps have been considered an essential tool in many nations as to deal effectively with crises. However, such technologies have sparked privacy concerns about the mass information collection, the sharing, and exposing of personal data with or without the consent of the user, as well as, of the storing of such data in a centralized database, or passing them to a trusted third-party server (TTP) (Borra S, 2020). To cite an example, in the COVID-19 Pandemic, there have been several concerns regarding the abuse in the contact tracing apps-based centralized model. Several individuals' sensitive personal information and metadata have been collected, stored in a centralized database, and shared between local institutions. Furthermore, population movement has been tracked using several tools, such as credit card records, smartphone signals, CCTV footage, and mobile location data (Borra S, 2020). Such collected information is vulnerable to a data breach, unwanted surveillance, and commercial advertisements (Sun et al., 2020).

Several countries introduced immunity passports to ease the lockdown policies and enable people to resume everyday life courses. The passport is a digital certificate that is granted to an individual as to show that he/she is believed to have received complete vaccination, immunization, or some form of protection against the virus. However, despite the enormous benefits of such a digital health passport, several challenges have been raised concerning people's civil liberties, including ethical and practical difficulties (Brown et al., 2020).

Although several papers have examined security and privacy features relating to crisis apps and digital health or immunity passports, to the best of my knowledge, there has not been a decentralized protocol for securely outsourcing sensitive data that uses agent-based technology as to provide the solutions, ideas, and features that are proposed in this paper.

The motivation of this paper, therefore, is to design a secure digital health passport protocol that has the characteristics and that serves the following purposes: To (i) perform anonymized data intersection among passengers' traveler's digital health passports and local and international institutions while preserving complete privacy; (ii) ensure secure shared information with full retention of user and apps data; (iii) propose a data retention policy that increases user trust and reduces privacy leakages and data storage cost; (iv) provide Interoperable autonomous cross-border privacy-preserving digital solution to deal with cross-border international data protection standards and regulations and minimize or eliminate surveillance; (v) minimize surveillance and provide anonymity for travels health and personal information data during an interaction with cross borders agent, (vi) avoid having to register in any third party app and ensure free movement; and finally (vii) protect against abused for discrimination ((profiling), eliminate restrictions, and minimizing economic damage. However, our proposed protocol has limitations described in five and six. The paper is structured into seven sections. Besides the first section of the Introduction, Section 2 is the relevant literature review. Section 3 presents a systematic review of crisis-based privacy-preserving Apps while Section 4 states the paper's core problem. Section 5 describes the architecture and design of the proposed scheme, and Section 6 provides the simulation experimentation of the proposed solution. Section 7 concludes the paper, highlighting future directions of inquiry.

Literature Review

Digital Crisis Management Platforms and their Privacy-Preserving

Digital Crisis management Platforms provide the colossal potential to respond timely during a crisis. MicroMappers (MM), for example, is a digital volunteer platform that uses AI for disaster response. Its associated tools for mining crisis-related information were submitted via volunteers and placed on the map. Google Crisis Map (GCM) contains a USA-based set of layers concerning crises related to hazards, weather, response, and emergency preparedness. Other tools and platforms created by Google for crisis management are Google Person Finder, Google Maps Engine Lite, Google Earth, and Google Public Alerts. However, such crowdsensing platforms must be integrated with encryption technology, as they are vulnerable to security threats and data leakages, insecure data dissemination, and systems malfunction (Halder et al., 2017).

Digital Crisis management mainly relies on smartphones, since they have expanded worldwide and altered how people live. Owing to their enormous utility and usefulness, they have become must-have tools, particularly in crisis-ridden times like ours. Furthermore, they have played an essential role in assisting authorities in terms of crisis management. Smartphones, nevertheless, are associated with many risks that have been an ongoing concern regarding these apps (Chan et al., 2020). Examples include collecting information without permission (Gnadinger, 2014); and extracting unneeded unrelated purposes' personal information through mobile app services and sometimes without users' knowledge jeopardizes users' sensitive data and making it vulnerable to data leakages and hardware control (Zhu et al., 2016). Insecure software apps have been criticisedon account of several well-known cases presented as follows: (i) Poor implementation (Fischeral et al., 2017) and authorization, (ii) session management issues (Jain &Shanbhag, 2012), (iii) ineffective encryption, including the misuse of cryptography APIs and deployment model (EGELE et al., 2013), and (iv) poor-skills software programmers.

Smartphone apps Data Privacy and Security regulations

The development of smartphone apps as to combat crises started first in 2011 by Jon Crowcroft and EikoYoneki at Cambridge University (Borra S, 2020). Several countries have proposed privacy, security, and data protection regulations and frameworks so as to govern, regulate and ensure compliance with how information is being collected, maintained, used, and disseminated. Nevertheless, mobile app development has obstacles to bridging technical knowledge and privacy regulations. Such a lack of app privacy awareness for the user and developer has not facilitated the development process of privacy-based apps. Yet, protecting the confidentiality of data during usage and dissemination continues to be a challenge. In addition, the massive data collection practice of mobile user data has raised serious concerns. Thus, several privacy-preserving digital data policies and regulations have been implemented so as to cope with data collection, storage, dissemination, and retention issues (Michael & Abbas, 2020; Hatamian, 2020).

Privacy-Preserving apps deployment model

Privacy-preserving apps developed during COVID-19 have relied on centralized, decentralized, or hybrid models (Shubina et al., 2022). The centralized deployment model relies on TTPs for data processing, computation, and storage of anonymous data and identities, including their cryptographic processes. Nonetheless, it is a bottleneck and a single point of failure, and is prone to several attacks, including side-channel and correlation attacks (Avitabileet al., 2020). In addition, its centralized storage databases are controlled by authority. Thus several decentralized and multilevel security protocols have been proposed to tackle this issue (Sarhan & Carr, 2017; Sarhan, 2017; Sarhan&Lilien, 2014; Sarhan, 2017; Sarhan A & Jemmali M; 2023; Sarhan, Jemmali& Ben Hmida, 2021; Sarhan A, 2023). Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) (Rimpiläinen, Thomson & Morrison, 2020), Blue Trace, and Robust and Privacy-Preserving Proximity Tracing Protocol (ROBERT) (Aisec, 2020) are the most common crisis-based app protocols that rely on the centralized model.

On the other hand, in the decentralized deployment model (Sarhan&Carr, 2017), the data is owned and controlled by data owners via their smart mobile devices. Decentralized models eliminate the drawback of centralized models, such as centralized data processing, storage, and computations. No data is supposed to transfer to a centralized server or database for further actions. However, most of the current decentralized protocol relies on a centralized server at one point or the other. The most common protocols that rely on the decentralized model are the Apple-Google protocol (Michael & Abbas, 2020), Distributed Privacy-Preserving Proximity Tracing (DP-3T) (Troncoso, et al., 2005), and the privacy-Sensitive Protocol and Mechanism for Mobile Contact Cracing (PACT) (Chan et al., 2022). For example, in Google and Apple, data is not stored in a centralized database;instead, it’s stored on the people’s phones. Finally, Contra Corona (Bay et al., 2020), Epione (Trieu et al., 2020), and DESIRE (Bielova et al., 2020) are examples of hybrid-based protocols that combine both centralized and decentralized solutions.

Cross-border privacy-preserving apps

Since mobile phones have become ubiquitous, they have become an essential tool for data crisis management, so effective collaboration can be performed to respond to a crisis. Therefore, collecting appropriate mobile phone data, including the data gathered by service providers, mobile apps, and embedded sensors, is a required input for practical crisis management tools (Wang et al., 2020). Such behavior, nevertheless, leads to several privacy and security violations.

Interoperability is the primary concern for crisis management, since it has become a critical success—Daniel et al. proposed a multi-criteria decision analysis (MCDA) method for the public sector to meet interoperability requirements. We mean by Apps Interoperability is the ability of apps to work together, or to allow integrated operations among different entities to pursue common beneficial goals. An effective crisis management response depends on the level, speed, and precision of exchanged information and the integration of additional services. Enterprise Interoperability Assessment (EIA) measures the degree of interoperation between entities (Avanzi et al., 2017). Many crisis management interoperability apps have been deployed to cope with a crisis. For example, KATWARN sends its users warning messages in case of an impending crisis depending on their GPS coordinates (ION et al., 2020). At the same time, NINA uses GPS or Wi-Fi coordinates to signal its users with warning or recommendations messages (EGELE et al., 2013), and other apps like Disaster Alert, Safeture, Facebook Safety Check, Cell Broadcast, SoftAngel, and safeREACH(Grinko, Kaufhold& Reuter, 2019). Despite the criticism received by many crisis based-COVID-19 apps due to the lack of security, privacy, and interoperability, Tauhidi et al. proposed a privacy-preserved interoperable blockchain-based database for contact tracing and GIS data analysis(Tauhidi et al., 2022).

Privacy-Preserving using Privacy Set Intersection (PSI)

Private sets, or multisets computation, has become popular, and has been in existence for decades, since research has worked on improving its computations and communications (SHAMIR, 1984). It is a cryptography secure, or privacy-preserving computation technique of the intersection, union, and element reduction operations (Kissner& Song, 2005). It was first deployed by Google to securely compute the online advertisements conversion rate (SHAMIR, 1984; ION et al., 2020) and later was applied in many applications and scenarios, such as genome tests, Online matching, mobile malware detection service, etc. PSI protects private sets shared by two or more parties by performing a privacy-preserving computation. For example, PSI allows two or more app users to compare their data sets and find intersections without revealing their data. PSI is implemented using many protocols such as public-key, circuit, Oblivious transfers (OT), and other variations mentioned in(Baldi et al., 2011). Berke et al. use PSI for contact tracing so users will be informed if they come across a COVID-19-diagnosed candidate. However, their scheme can be practical only if it has been widely adopted (Tamrakar et al., 2017). Trieu et al. proposed Epione, a PSI-cardinality-based contact tracing app that is designed to be practical in case of an intersection between a large server database and a small client one (Trieu et al., 2020).

Privacy-Preserving using Mobile Agent

Agent technology has been used extensively in crisis management (TMNU et al., 2020; Zhou et al., 2021; Kadinski et al., 2022; Castro et al., 2020). In addition, agent and multiagent systems have been used extensively by integrating several emerging technologies to model and provide solutions for complex problems. For example, during the crisis of covid-19, mobile agent systems have been applied to deal with several issues related to the crisis, for water distribution system contamination response (Kadinskiet al., 2022), to analyze the spread processes of the COVID-19 epidemics in open districts (Castro et al., 2020), and to provide visions for public health policies and interference (Hotton et al., 2022). TMNU et al. (TMNU et al., 2020) proposed a scheme that uses an IoT- based robotic Agent for disabled and infected people. The Agent uses sensors to identify the patient's gestures. Finally, Zhou et al. (Zhou et al., 2021) integrated an agent-based solution with a susceptible-exposed-infected-recovered (SEIR) model to assess the transmission of the Covid-19 viruses inside the city, and suggest a vaccine distribution strategy.

Privacy-Preserving based Digital Health Passport

A digital vaccine passport, digital health passport, or immune passport has been widely adopted post-COVID Pandemic in order to respond to the need of resuming international travel. It is a type of official digital document that stores personal information related to individual personal information, including travel history, health information, vaccination status, and diagnostic tests (Angelopoulos, Damianou&Katos, 2020). Thus, its carried data must be anti-fraud, interoperable, privacy-preserved, and manageable (Karopoulos et al., 2021).Many digital health passport solutions have been proposed during the covid-19 Pandemic to deal with travel policies, and other restriction policies introduced during the Pandemic. Most of the proposed solutions privacy-preserving underlying technologiesrely on traditional practical public key cryptography and blockchain technologies. However, they encounter many issuesas a result of their implementation, or deployment models. Hicks et al. (Hicks, et al., 2020) proposed a decentralized-based public key cryptography scheme called "SecureABC" for immunity certificates. Bansal et al. presented (Bansal, Garg &Padappayil, 2020) a blockchain-based immunity certificate that protects end-users' privacy and store testing-related facilities and hospitals. The idea of implementing a standard for interoperability was introduced by Electoral Commission in the EUROPEAN PARLIAMENT. A PKI-based digital COVID Certificate (EUDCC) presented by the European Commission to include the following features: (i) Digital and/or paper format (ii) uses QR code (iii) free of charge (iv) bilingual (v) safe and secure (vi) interoperable in all EU countries. Such interoperable digital passport permits free movement within European countries (Commonpass, 2021). The idea of protecting against fraud through tests and certificates validation process proposed by the CommonPass platform. The platform also validates if the digital certificates are acceptable for international cross-border entry requirements (AOKPass, 2022). AOKpass is a blockchain-based digital passport scheme introduced to enable cross-border interoperability in which users can officially provide digital and authenticated credentials through a QR code to a government authority (AOKPass, 2022).

Table 1:

Crisis apps major comparison, features, and privacy-preserving underlying technologies

Table 2:

List of acronyms for feature terms in Table 1

Table 3:

Privacy-Preserving risks/threats impact level

Table 4:

Data sensitivity levels for popular crisis apps

Crisis-Based Privacy-Preserving Apps Systematic Review

This section provides a brief evaluation study that highlights the pros and cons of the current existing platforms, and compares them with the proposed scheme. Due to climate changes, widespread diseases, and unpredictable disasters, which cause life losses, economic damages, and privacy and security violations, many tools have been developed to cope with such issues. However, despite the numerous advantages gained by such tools, their contributions only minimize the impact of the incidents. In other words, no single solution is considered fully practical to tackle most problems. The common drawbacks of the proposed solutions are as follows: (i) data security and privacy leakages, (ii) failure to comply with international privacy and data protection standards, (iii) surveillance, (iv) sharing data with trusted and untrusted parties, (v) poor functionality, (vi) limitation in computational power, (vii) untrusted deployment model.

Table 1 shows a concise evaluation that compares different crisis-based management apps to address most problems affecting them. Although this research aims to cover issues pertinent to digital health passports, the researcher reviewed thirty-six applications deployed in various domains, such as immunity passports, contact tracing, and monitoring, as shown in table 1 and table 2. The evaluation criteria considered many factors, such as data privacy and security, deployment models, underlying technology, privacy protection complaints, domain, interoperability, and level of sensitivity of data.

The presented comparative study is based on the platform's domain, deployment models, underlying technology, privacy and security violations, threats, and interoperability. The evaluation of the deployment model shows that, the decentralized model is far better than the centralized one. Centralized-based platforms rely on the central server design, which has received much criticism, because of their serious privacy violations. TraceTogether in Singapore and Canada, AarogyaSetu in India, and COVIDSafe are examples of centralized-based design solutions (Lodders& Paterson,2020; NORTON ROSE FULBRIGHT, 2020; Aarogya S, 2020). They have been built to assist in coping with crises, seeking treatment, and making people accomplish everyday activities promptly. Thus, such solutions pose many drawbacks, including data leakages, surveillance, and side-channel attacks.On the other hand, decentralized-based protocols have been adopted to tackle the issues presented in TTB-based ones. Decentralized protocols have gained privacy and security advantages by allowing users to store and manage their data on their mobile devices without interacting with TTP. It relies on distributed storage or servers. It protects identities against an untrusted party and protects data against exposure. For example, SwissCOVID, Safepaths in USA, WeTrace in Philpine, and CovPass (von et al., 2020; Raskaret al., 2020; Gassmann, 2020; Hernández et al., 2021) are platforms built based on decentralized design. Apple–Google, BlueTrace (Bay et al., 2020), DP-3T, and PEP-PT are examples of the popular decentralized protocols that should overcome issues presented by the centralized one. Nevertheless, several platforms built based on such protocols have been vulnerable to security and privacy flaws, health data leakage, GDPR compliance issues, replay attacks, and trust (Wymantet al., 2021; Messai et al., 2020). Furthermore, some solutions consideredcombining both models to develop a hybrid approach of building apps relying on centralized and decentralized protocols; for example, CT-RSA (Srithas& Navaratnam, 2020). Yet, as is shown in table 3, such apps are vulnerable to surveillance, Man in the middle attack, and key recovery issues.

Evaluating the apps listed in Table 1 based on ethical and data protection principles showed that none fully complied with international data protection acts. For example, platforms such as

(Hernández et al., 2021; Trusted Travel, 2021) only comply with data protection standards inside the European Union countries.

Besides privacy and security concerns, other challenges have been presented when evaluating the selected platforms based on functionality, performance, computing resource usage, complexity, and usability. For example, AarogyaSetu, WeTrace, Safepaths, and Covid-19 KP showed poor functionality. Moreover, WeTrace, Magnetometers Trace (Kuk, Jeon & Kim, 2017) experienced drain battery issues. RFID-based Contact tracing (Mehta et al., 2020) encountered storage limitations. Other platforms (Jung &Agulto, 2021; Jeong, Kuk & Kim, 2019) struggled with technical and training skills requirements and operation complexity.

This evaluation intends to select applications relying on different underlying technology such as GPS, Bluetooth, BLE, Wi-Fi, Machine learning, magnetometer, RFID, RSSI, Cellular network (5G), IoT, Blockchain, SDN, and Machine learning. Therefore, the researcher noticed that, most selected platforms that relied on GPS as an underlying technology experienced sensitive data and health leakages, for instance, REACT, Iranian AC19 (Messai et al., 2020), and Apple-Google (Wymant et al., 2021). Moreover, platforms relying on Cellular networks, Wi-Fi, GPS, or Bluetooth recorded severe data privacy violations. Only a few offered an optional data deletion feature, for example, CovPass, Surokkha(Surokkha App, 2022), and IO platforms(IO, 2022).

Another evaluation intends to evaluate the platforms regarding interoperability and privacy protection act complying. For example, we observed that only an international application like the one jointlybuilt by private companies Apple-Google (Apple & Google, 2020; Michael & Abbas, 2020;)could be practically functioned worldwide to overcome cross-border app interoperability. such a platform, nonetheless, has raised serious concern among French parliamentarians (Storeng KT & de Bengy P A, 2021), pointing out that it could be used to share and sell health data, including digital sovereignty. Other applications like CovPass and the one-based Blockchain are only interoperable inside European countries. (Hernández et al., 2021; CovPass, 2021). Furthermore, MyCOVID Pass (Covid Pass, 2021) operates interoperability only inside African countries.

Other solutions Versus CONTRIBUTIONS OF THIS PAPER

The proposed secure mobile digital passport agent (SMDPA) includes the following features: It (i) securely shares personal and health information with international authorities;(ii) uses a mobile agent to disseminate data associated with their security and privacy policies; (iii) supports international privacy standards and regulations via the use of intelligent data minimization feature; (iv) uses privacy set intersection technique to provide confidentiality and integrity of the carried data and relies on a mobile agent fault tolerance feature to support data availability; (v) uses data evaporation feature to expire health vaccination information when applicable; (vi) supportsinteroperability to relax international travel; (vii) protects against discrimination by providing anonymous, secure interaction between users and authorities so limited information can be shown (viii) provides recommendation for safe travel zone based on a traveler stored health information and general health conditions.

Figure 1: General architecture of current crisis apps platforms interaction

Figure 2: Secure Mobile digital passport agent (SMDPA) high-level architecture

Problem Statement

Current digital health passports, immune passports, or vaccine passport apps include limited health information that neither can be shared anonymously (due to massive surveillance) nor grant an individual an ideal free movement or be processed autonomously. This problem can be modeled as a privacy set intersection in which two mobile agents can represent two parties to securely compute the intersection of digital health passport data and institutional distributed servers or databases datasets. As discussed previously, SMDPA is a digital health passport mobile agent that directs its owner to mobilize according to the intersection results between SMDPA and the institutional distributed databases or servers agent.

This research defines a digital health passport as a passport holding an individual's personal and health information. The information includes medical health records, including conditions, infections, symptoms, medical drug lists, vaccination status, and risk factors. Unlike many proposed digital health passport solutions, SMDPA, as an intelligent agent, interacts autonomously with other parties (e.g., other agents) on behalf of its owner in a decentralized manner. This should overcome issues inherited from a client-server model concerning internet traffic and bandwidth overhead. Moreover, its privacy policy involves a data minimization function that deals with cross-border data privacy regulation and standards compliance.

Let *M* be a party owning a set of private information concerning an individual personal and health information. Let *A* be an authority, institutional, service provider, or governmental agency holding encrypted information stored in distributed databases. *M* and *A* want to apply an exact join for their data without revealing unnecessary information. This means that the only information learned by *M* about *A* and information learned by *A* about *M* is $M \cap A$. Let assume *M* be a source contains a set of elements (m_1, m_2, m_3, ….m_n), and *A* contains (a_1, a_2, a_3…., a_n). PSI can be used if both parties want to apply to join on their private sets without revealing any data except the elements in the intersection data.

This research design a protocol in which the datasets *M* and *A* obtain the intersection under privacy constraints, which states the protocol must not reveal elements in the intersection. Furthermore, the proposed protocol avoids relying on a TTP to compute the intersected elements between *M* and *A*. Instead, it is a decentralized protocol that relies on a mobile agent as an autonomous entity to act on behalf of the travel passenger when interacting with other parties.

The researcher assumes that, international cloud repositories, or distributed databases, are deployed, decentralized, managed based on multiagent systems, and hold information concerning crises, including health conditions and requirements. For example, an institution party (such as hospital and school) can update information (e.g., local lockdown, restricted and green zones) in this repository. Such shared information can benefit passengers using SMDPA.

The current proposed protocol uses PSI to allow SMDPA users to compare their digital health passport set of elements (*M*) with the data stored in an internationally distributed cloud database server (*A*) without revealing any information concerning their privacy. Hence, PSI allows SMDPA users to check whether their digital health passport data and privacy policy (*M*) intersect with data and privacy policy stored in "*A,*" a distributed database, without revealing *M* datasets.

Although unbalanced PSI (Cristina A, Resende D &Aranha, 2021) seems the best to suit the proposed approach in this paper; yet, this paper does not focus on the implementation, or modification aspect concerning PSI,for that is left for future investigation. Furthermore, the intersected data sets are not balanced, because the data elements in the digital passport represented by SMDPA contain a limited set of data compared to the one stored in an institution's server.

Table 5:

Privacy set intersection based on enrichment case

Architecture and Design of the Proposed Scheme

Protocol design

The protocol security design in this research relies on public-key cryptography based unbalanced-PSI. The protocol deals with unbalanced datasets since the amount of data carried by the secure mobile digital health passport app (SMDPA) is less than those stored in an institutional distributed repository. Hence, despite many existing PSI protocols, a one-way PSI protocol seems the best to fulfill the requirement in this research; therefore, only SMDPA should know the intersection result. Bloom filter (Bloom, 1970), Cuckoo filter (CF) compressions, Cuckoo hashing (Fan et al., 2014), Original Quotient Filter (QF), or Rank and Select based Quotient Filter (RSQF) (Pandey et al., 2017), can be integrated with the one-way PSI to decrease the amount of transmitted data or stored data by SMDPA. Measuring the best filter that suitsour protocol's design is outside this paper's scope and plans for future work. The setting of our protocol is as follows:

1) Use unbalanced PSI since we assume that one party has a set with tens or few hundred of data (SMDPA) and the other party might have a set with a few million to billion data records.

2) Assume a One-way PSI protocol to interact with the server agent to minimize the amount of overhead inherited by the two parties (mutual).

Assume a PSI-based enrichment scenario since both parties, the SMDPA and the server agent, want to (i) apply joint between their datasets without revealing any unnecessary information and (ii) enrich joined records with variables fromboth SMDPA and the server agents. For example (see table 5), Given set A= {age:8-60,4-80, 17-50,17-45; DH: Covid19,Ebola, Type2 Diabetes, Hepatitis C; HR: One-dose, two-doses, Quarantine, Health Insurance; GZA: USA, Germany, KSA,,}, and set M= {PN:p12, age:32, DH:covid19, HC: one-dose, date: 1/1/2023, TH: China, USA, KSA, UAE). Thus, $M \cap A$ = {P12, 32, USA, Germany, KSA, Mall, Restaurants, Hospitals, one-dose, 1/1/2023, China, USA, KSA, UAE}. An example of elements that should remain outside the intersections {Nationality, Religion, and Travel history}; such information can be subject to discrimination, refusal of employment, social media, racial, religious profiling, advertisements, or scams. The goal of this protocol is to prove eligibility while hiding an individual no essential identity. While several existing PSI protocols and variations encounter many computational and communication overhead issues, SMDPA should overcome communication and computation overhead as a mobile agent. An agent can allow code and data to carry their security or protection mechanisms wherever they travel. This improves traditional security solutions, where a stationary platform manages security and protection. Let us Consider the following examples. An immigration and immunization service department or health care agency:

1) Want to ensure that passengers have no severe health cases, so they can be allowed entry but denied or directed toan international event. Neither the passenger nor the agency wants to disclose their data, but both want to know the intersection.

2) Compare their databases of common health diseases with tourists while respecting international and local privacy laws that prevent them from exchanging or revealing information. Thus, they can share minimum allowed information related to subjects of interest matter.

3) Identify visitors who visited countries with high infection rates without identifying the countries or placing travel restrictions.

4) Check its database of hazardous diseases against foreign air carrier-passenger digital health passports without both parties revealing their set of data. Such passengers might be denied flying into a particular restricted zone.

To design the PSI protocol, the following points are to be taken into consideration:

1) The size of the dataset in both parties. For example, the size of *M* and *A*. SMDPA datasets M is expected to be small compared to those owned by an institution or interacted agency.

2) The level of privacy and security needed to tackle any adversarial attacks.

3) The resource-constrained or computational power for smart mobile devices since multiple cycles of interactions are not recommended. SMDPA is not required to download large datasets nor perform an intensive computation that might drain the battery.

Figure 3: The component of SMDP solution

Algorithm 1

Table 6:

SMDPA Algorithm Description

Algorithm 2

Table 7:

Enhanced SMDPA Algorithm Description

Example 1

In this example, let'sassume there are two datasets. Set A contains private data that are encoded as integers and have {0,5,10,15,20,25,30,35,40,45,50}, and Set B includes information related to site restriction and health requirements that are also encoded as integers as follows {0, 4,8, 12,16, 20, 24, 28,32,36,40}. So set A ∩ Set B = {0, 20, 40} and hence the intersection size (*IS)* is 3.

We assume that *IS* a factor that determines the place of visit for an individual in a crisis-based situation. Based on *IS*and the intersection matching result (IMR) values, three levels of Bit Passing Coin (BPC) are generated. BPC is a single access permit value that permits an individual to access an institutional area (say, an airport, hospital, school, etc.). Each level is represented by a color described as follows: Green color means an individual is fully permitted to enter any place in the green zone based on his health status determined from the set intersections. BPC_G denotes BPC passing for green zone areas. Yellow means an individual is free to access the yellow zone area. BPC_Ysymbolizes BPC passing for yellow zone areas. Red indicates an individual is permitted to access the red zone area. BPC_Rimplies BPC passing for red zone areas. IMR contains interesting elements describing specific medical and personal data. Note that the number of generated BPC varies from person to person, which considers individual health and personal information such as medical history, age, vaccination, etc. Therefore, it depends on a particular health condition. There is a threshold *TH*value that manages the generated BPC. *TH* categorizes BPC into three levels described above, which are represented as Level 1 (L1), level 2 (L2), and level 3 (L3), as shown in Algorithm 1, table 6.

Example 2

Let's assume a scenario in which *IS*& IMR indicates an induvial can visit the green zone area assuming *IS* & IMR ≤ L1. In this case,an individual granted $nBPC_G$ to be deposited in his Coin Passing Wallet (CPW)as $n(BPC_G)$. This means he can access only n green zone areas daily. Note that the number of generated BPC depends on other factors, such as individual health, data records, and vaccinations. It is specifically determined during the first privacy set intersection, which is assumed to be at the airport's first entry point. Let Abe anencoded dataset of ten elements {1,2,3,4,5,6,7,8,9,10}, B encoded dataset of nine elements {0,1,3,4,5,6,7,8,9,10}. A ∩ B = {1,3,4,5,6,7,8,9,10}. Assume the threshold TH sets its first level L1 to be at nine or more for a green zone. In this case, n BPC_G is generated and deposited into CPWsince*IS≤L1 (*9≤9 *)*and *IS* {elements} € IMR. TH also can be arranged to generate the number of allowed BPC for L2 and L3,described as the yellow and red zones.

Algorithms Description

Table 6 and Table 7 show the algorithms presented in this scheme. Table 6 algorithm is described as follows: (i) The result of the sets intersection size of SMDPA and the Airport agent stored in variable *IS*. (ii) There are three levels of Threshold presented as L1, L2, and L3 such that L1 is the largest, L2 the second largest, and L3 the lowest. (iii) Using the random number generation function to generate n BPC, then getting stored in CPW according to the three branching logic so as to determine the order. The logic compares the largest, median, and smallest threshold with the set intersection size, and generates n BPC according to the fact that the largest the intersection, the more BPC will be generated, and then stored in CPW. CPW modeled as an Arraylist object. Table 7 shows algorithm 2, which presents an enhancement of the proposed scheme. It takes the average of L1 and L2, and compares the result with *IS*. Else takes the average of L2 and L3 and compares the result with *IS.*

Figure 4:Basic PSI Protocol Adapted from (Angelou N, et al. 2020)

System Model

This sub-section presents the components of the proposed SMDPA solution (see Fig. 3).

1) *Secure Mobile digital passport agent (SMDPA):* is a software construct based on a mobile agent that encapsulates data and its privacy and security operations policy. The proposed scheme modified the solution proposed in (Sarhan&Carr, 2017) as follows: (i) PSI employed as a data protection scheme that also manages the privacy access policy and data evaporation. We assume two attributes labeled as time and location managed by privacy policy to control the time and location to trigger the data minimization procedure. This should deal with issues related to privacy compliance. To balance the CIA-Triad, a self-destruction feature (Sarhan&Carr, 2017) was excluded as we feel that such a powerful feature is against the data security policy in maintaining data availability. The proposed solution inherits the data evaporation feature presented by (Othmane&Lilien, 2009), which we call data minimization.

1a) SMDPA-Sub-Components & Features:

1a-1)Java agent development framework (JADE):Jade is an open-source agent framework that includes numerous built-in and add-on functions and libraries. It can be utilized to develop distributed applications, support the J2ME platform and wireless environment, and provide decentralization environments in many operating systems. Its rich communication protocols are capable of providing inter-platform and intra-platform messaging (Bellifemine F, Caire G & Greenwood D, 2007).

1a-2) Jade Leap Add-on: Jade leap is multiagent systems environment combined with Jade to support mobile phones.

1a-3) Java J2ME: Java 2 Platform, Micro Edition or (J2ME) is a java version or edition designed to address limitations on the application running on embedded systems and mobile devices with limited processing power and memory. Many devices support J2ME because it is simple and easy to implement. It is used for portable code for embedded and mobile devices.

2a) *SMDPA*-Security policy: SMDPA, like ADB (Sarhan&Carr, 2017), encapsulates a privacy and security policy with the digital health passport data. The policy protects and controls digital health passport data's security, privacy, and anonymity. In addition, it controls how data are being intersected and minimized when interacted with other parties. The decentralized cryptographic protocol that protects data is described next:

2a-1) *Private set intersection (PSI)*: SMDPA protects its data using PSI, a robust, secure multiparty computation or privacy-preserving protocol that makes two partiescompute the intersection of their data and output only the intersected data. The purpose of using PSI is to share and process data anonymously between two parties and guarantee flexible control movement of individuals during a crisis. For example, travel passengers might be directed partially to visit certain areas and restricted from entering others. PSI can ease traveling while providing anonymity for travel passengers. This should deal with profiling or any form of discrimination concerning race or other discriminatory cases. For example, Asian Americans have experienced anti-Asian discrimination fueled by the crisis of COVID-19(Gover, Harper &

Langton, 2020). Also, SMDPA policy uses two attributes for privacy minimization service described next.

2a-2) time attributes: SMDPA uses time attribute to deal with specific lockdown scenarios or travel policies. The time attribute can be used as an example to remove any travel data restriction concerning vaccination against certain diseases. For instance, post covid19, some countries imposed travel requirements for air passengers that requestedtravelers to wait 14 days after a specific dose of vaccine (CDC, 2019).

2a-3) location attribute: SMDPA uses location attributes to deal with travel policies imposed by some geographical regions and privacy policies like the General Data Protection Regulation (EU GDPR), which address data transfer outside the EU. For example, the SMDPA data minimization featurecan evaporate data concerning individual health status and data privacy under specific time and location requirements

2a-4) Bit passing coin (BPC): BPC is an idea that is presented fromthe Coin Vending Game Machine. It states that the result of a set intersection between SMDPA and the entry point (airport) distributed repository server agent should generate BPCs in three colors: Green, yellow, and Red. For example, Green BCP should permit a person to move freely and access a protected zone during a crisis. Yellow BCP should allow a person to pass through a particular area. Red BCP should restrict an individual from passing through most of the area and only access effective protected zone. Each individual crossing a border should receive several BCP in various colors. Such numbers can be determined based on the crisis condition.

2) *Blockchain*: Blockchain is a peer-to-peer technology based on a distributed ledger. It can record the participants' activities in its network. It relies on several cryptographic applications, such as encryption, hash functions, and digital signature. In Blockchain, data is signed digitally as transactionsand then broadcasted. All broadcasted transactions are timestamped, grouped, and hashed in order into blocks forming unique identifiers of blocks. Integrating Multiagent Systems into Blockchain has many benefits, including (i) addressing scalability issues in Blockchain, (ii) managing the large datasets stored in the distributed database servers that SMDPA,for instance, has to interact with; and (iii) improving digital health passports and healthcare management;(iv) fixing any security limitation in MAS; and (v) adding more flexibility to MAS (Calvaresi et al., 2018).Details about integrating the proposed scheme with Blockchain are outside the scope of this research. However, for future work, we plan to study the idea of serialization and deserialization of SMDPA agents in the form of a Blockchain. Serialization means turning SMDPA agents into data format, which can be saved into storage and deserialized where applicable.

3) Preliminaries

Fig. 4 shows the basic PSI Protocol Adapted from (Angelou N, et al. 2020). The protocol combines Diffie-Hellman (DDH), based PSI, and PSI-Cardinality; and uses Bloom filter compression in order to minimize the communication time.

SMDPA Simulation Experimentation

Simulation Setup

Table 8 :

The configuration of the computing environment for SMDPA

Table 8 lists the simulation environment specification. SMDPA system is simulated, using a personal desktop with a single processor with 8 GB of RAM. The desktop includes the Jade platform and several add-on libraries described in the previous section. Since JADE cannot function properly on small devices, the LEAP add-on is integrated with JADE; hence, the Jade runtime environment was modified so as to form JADE-LEAP that can be deployed thereafter on a wide range of small devices. J2ME Configuration uses either connected limited configuration (CLDC) or connected device configuration (CDC). Cell phones or PDA device versions can use either technology depending on memory availability. For example, devices with low memory use *CLDC*, and devices with better memory use CDC. The researcher used CLDC of Java Micro Edition (J2ME CDC) in order to form the JADE-Leap. The configuration of Jade Leap is based on MIDP, which runs on devices that support Java-enabled cell-phones. The simulation management of the SMDPA and the distributed server agent is carried out through Agent.GUI. Agent.GUI also records the interaction performance measurements among SMDPA and the distributed server agent (Derkson, Branki&Unland, 2011).

Figure 5: SMDPA approach execution in run time environment

SMDPA UML Diagram Design

In this experiment, JADE-LEAP is executed in split execution mode. The Jade container, as shown in Fig. 5, is split into a Backend that runs on a local host and a Frontend that runs on the mobile device. Such split of execution suits wireless devices that demand resource constrained (LEAP USER GUID, 2003). In this research, he proposed solution was designed by using five jade containers, as shown in Fig. 5. Besides the split container described above, four additional jade containers were built to model an airport, a restaurant, a school, and hotel facilities. An external agent manages each container. For instance, an airport officer agent represents an immigration officer at an airport, and operates the airport container. Likewise, the hotel agent manages the hotel container while the restaurant agent manages the restaurant container, and so does the school agent to the school container.

Figure 6:SMDPA UML sequence Diagram

Fig. 6 shows a model interaction among the entities involved in the SMDPA protocol. The process goes as follows. First, a travel passenger arrives at an airport, and requests a border officer to assess his digital health passport digitally. Next, the officer performed a cross-border joint PSI interaction with the passenger. Then, based on the intersection described above in example 2, n BPC is generated, and deposited into the travel passenger CPW. Finally, the passenger uses one BPC_G to be granted safe entry. Before interacting with the border immigration officer, a function might be triggered to evaporate data that does not comply with the privacy protection acts. The process is conducted through the location attributes that check the IP address of the destination, and that decide what data are needed to be evaporated before performing a joint privacy set intersection with the border officer. The travel passenger, afterward, moves freely. However, he might be restricted from visiting certain zones, or being granted a few visits to others. This depends on the PSI result of the first interaction with the border officer. For example, Fig. 9 demonstrates that, travelers want to visit a green area zone place, say a restaurant, a request is sent to the restaurant agent, the restaurant agent demands a $BPC_{G,}$ the passenger checks his BWC account, and deposits one BPC_G, Restaurant agent, then, permits the passenger to enter the restaurant. In another scenario as shown in Fig. 9, the passenger wishes to enter a school, and finds out it is modeled as a yellow zone area. The passenger sends a request, asking to deposit BPC_Y. The school agent, then, permits the travel to access the school campus. In a third scenario, the passenger wishes to stay at a hotel. He sends a request, and finds out that the hotel is modeled as a red zone area. He sends a bid ,and is asked to deposit BPC_R, which he deposits, and is, then, granted access. Note that, as described above, the number of issued BPC and their levels is predicated largely upon both the passenger's personal and health information, on the one hand, and the visited countries' rules and restrictions, on the other hand, and all interactions are expected in a secure private manner.

Prototype of SMDPA Solution

The proposed scheme was prototyped using the JADE agent framework (Bellifemine F, Caire G & Greenwood D, 2007) as a decentralized environment, and relied on several add-on libraries that each has its own purpose. For example, Lightweight Extensible Agent Platform (or LEAP) to modify the JADE kernel in order to support run time environment for developing the jade app for mobile devices with limited resources. The JADE-Leaps splits the execution environment into two parts: a Front end that runs on the mobile, and a backend that acts as a mediator. As is shown in Fig. 5, the researcher created five containers, and implemented five agents, using java classes that each manages the communication of the message with SMDPA. The investigator used two Array List populated with integers so as to simulate set intersections among the SMDPA and the Airport officer agent. He also implemented JADE behaviors to manage the messages exchanged among agents. He used another add-on library “Agent.Workbench,” (Agent.WorkBenach; 2017) to simulate and measure the developed prototype performance. Table 8 summarizes the computing environment the researcher used in order to implement and deploy our solution.

Figure 7: CPU Load's performance for SMDPA and the AirportAgent interaction

Figure 8: CPU Load Time for SMDP and the AirportAgent

Results

SMDPA Prototype evaluation using JADE and Agent.Workbench

In this research, the prototype of the integrated architecture of the proposed scheme was evaluated by using “Agent.Workbench”. The CPU usage is analyzed to track the agents' CPU load on the machines. This should account for CPU resource consumption, and help enhance interaction and intersection algorithms. Fig. 7 and Fig. 8 show a performance chart for monitoring the experiment performance metric. It measures CPU Load's performance during the interacting and set interaction between the AirportAgent and SMDPA. The performance metrics parameters are delta CPU time in milliseconds for the user, delta CPU time in milliseconds for the system, and the total CPU times for the user and total CPU times for the system. The idea is to track and observe the ways in which the proposed approach consumes CPU based on the set intersection. The "Agent.Workbench" tool generated two hundred seventy-eight samples. The presented chart illustrates a slow increase in the CPU load during the interaction between the Airport Agent and SMDPA. Hence, agents' average CPU usage is lower than the device's total CPU load. Nevertheless, CPU user time refers to the time processor performs in order to execute agents' code, such as intersection, messaging, migration, and code libraries. time. CPU system time refers to the execution time for running code in the operating system kernel. Hence, the total CPU time combines the agent action CPU time, and the kernel system calls time. Likewise, CPU delta time represents CPU times spent during intervals. Note that the sampling interval in our experiment was 0.5 seconds.

Figure 9: SMDPA Algorithms average time

SMDPA Algorithms Evaluations

In the architecture and design section, the investigator described two algorithms for SMDPA communication and interaction with other agents. In this section, the performance of these algorithms is measured. The two algorithms are implemented using Java, and precisely measure the elapsed time for code execution using Java.System.nanoTime(). System.currentTimeMillis().A java random number generation function was used to model the stream generation of Bit Passing Coin (BPC) and used an ArrayList object to model CPW, so storing the generated stream of BPC. Three for loops were used to create three BPC levels, and; hence, measure their elapsed time. The researcher generated 250 instances for each of Algorithm 1 and Algorithm 2. Fig. 9 indicates that, enhanced SMDPA Algorithm 2 has a better average execution time than Algorithm 1.

Discussion

Simulation Limitation

The result shows the viability, and practicality of the proposed approach; however, the researcher simulated the PSI protocol using a set of integers on the grounds that he assumes data can be encoded as integers. It falls outside the scope of this work to extend any PSI protocol, as the main purpose of this paper is to highlight the practicality of agent-based solutions in modeling crises. The researcher holds the view that, the most suited PSI protocol for this work should be a one-way PSI in which interaction is performed at the SMDPA. The emulator used is to prove the concept of the proposed solution. As for future inquiries, the researcher plans to use smart mobile device-based android. The split execution mode used to simulate the proposed work could affect the result in contrast to the stand-alone execution mode, where a complete container could be executed on the device Execution mode. The investigator used the split execution mode as recommended by (LEAP USER GUID, 2003) as the most effective when running JADE-LEAP on personal CLDC device where mobility features are needed.This research focused on measuring the performance overhead of SMDPA and the Airport agent or first agent to interact with SMDPA, asserting that the highest overhead time should occur during the set intersection process.

Conclusions

In this paper, a decentralized solution for secure digital health passports is designed.The solution encapsulates data and its privacy policy by using privacy set intersection, disseminates and controls their movements by means of multiagent systems. The proposed SMDPA assists its owner in managing his movement during a crisis. It uses the concept of Bit Passing Coin, in which several digital passing coins can be issued during the user's initial interaction with a cross-border entity.

Asystematic review ofthe thirty-sex crisis-based platforms is conducted. As discussed earlier, most apps lack proper privacy protocol settings, and are vulnerable to several privacy attacks. The proposed protocol addressed the commonissues seen on many typical crisis-based mobile applications, such as data leakage, surveillance, security, privacy attacks, privacy compliance, interpobitilty, and performance. A sample prototype is developed by using Java and other add-ons like JADE, and JADE-Leap. Finally, an experimental evaluation of the proposed protocol is administered in order to prove the concept of the proposed work, and find the results acceptable. For future work, the reseacher plans (1) to deploy the proposed work on a real smart mobile app; (ii) to try different PSI settings and filters, and find the best that can suit the purpose of his work; and (iii) to Integrate the proposed solution with Blockchain, and study saving SMDPA as a deserialized copy in the Blockchain. (iv) Also, updating the BPC numbers, in general, is also outside the scope of this research.

References

Hassankhani M, Alidadi M, Sharifi A, Azhdari A. 2021. Smart city and crisis management: Lessons for the COVID-19 pandemic. *International Journal of Environmental Research and Public Health*, 18 :7736.

Van Wyk B, Mooney G, Duma M, Faloye S. 2020. Emergency Remote Learning in the Times Of Covid: A Higher Education Innovation Strategy. In: Proceedings of the European Conference on e-Learning, Berlin. Berlin, Germany, pp. 28–30.

Whitelaw S, Mamas M. A, Topol E, Van Spall H. G. 2020. Applications of digital technology in COVID-19 pandemic planning and response. *The Lancet Digital Health*, 2:e435-e440.

Elsayed E. K, Alsayed A. M, Salama O. M, Alnour A. M, Mohammed H. A. 2021. Deep learning for covid-19 facemask detection using autonomous drone based on IoT. In 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE). Khartoum, Sudan. pp. 1-5. DOI: 10.1109/ICCCEEE49695.2021.

CiucciM, Gouardères F. 2020. National COVID-19 contact tracing apps.Available at. http:// europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI(2020)652711_EN.pdf (accessed 10 July 2022).

Greene D. N, McClintock D. S, Durant, T. J. 2021. Interoperability: COVID-19 as an impetus for change. *Clinical Chemistry*, 67: 592-595.

Luengo-Oroz M, Hoffmann P, Bullock J, et al. 2020 Artificial intelligence cooperation to support the global response to COVID-19. *Nature Machine Intelligence*, 2: 295–297.

Hern A, Gadgets have stopped working together, and it's becoming an issue. Available at.https://www.theguardian.com/technology/2021/may/30/gadgets-have-stopped-working-together-interoperability-apple(accessed Jul. 10 2022).

Raisaro J. L, Marino F, Troncoso-Pastoriza J, et al. 2020. SCOR: A secure international informatics infrastructure to investigate COVID-19. *Journal of the American Medical Informatics Association*, 27: 1721-1726.

Shokoohi M, OsooliM, Stranges S. 2020. COVID-19 pandemic: what can the west learn from the east?. *International Journal of Health Policy and Management*, 9:436.

Borra S. 2020. COVID-19 apps: Privacy and security concerns. *Intelligent Systems and Methods to Combat Covid-19*, pp. 11-17.

Bay J, Kek J, Tan A, Hau C. S, Yongquan L, Tan J, Quy T. A. 2020. BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders. *Government Technology Agency-Singapore, Tech. Rep*, 18:1.

Brown R. C, Savulescu J, Williams B, Wilkinson D. 2020. Passport to freedom? Immunity passports for COVID-19. *Journal of Medical Ethics*, 46: 652-659.

Sun R, Wang W, Xue M, Tyson G, Camtepe S, Ranasinghe D , Vetting Security and Privacy of Global COVID-19 Contact Tracing. *arXiv preprint arXiv:2006.10933*

Apple Google. 2020. Privacy-Preserving Contact Tracing. Available at https://www.apple. com/covid19/contacttracing. (accessed Aug. 15 2022).

Singapore Government Blog. 2020. Help speed up contact tracing with TraceTogether. Available at https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether (accessed Aug. 15 2022).

Gnadinger K. 2014. The Apps Act: Regulation of Mobile Application Privacy. *SMU Sci. & Tech. L. Rev*. 17:415.

Zhu K, He X, Xiang B, Zhang L, Pattavina A. (2016). How dangerous are your smartphones? App usage recommendation with privacy preserving. *Mobile Information Systems*, *2016*.

Chan J, Gollakota S, Horvitz E, et al. 2020. Pact: Privacy sensitive protocols and mechanisms for mobile contact tracing. *arXiv preprint arXiv:2004.03544*.

Fischer F, Böttinger K, Xiao H, et al. 2017. Stack overflow considered harmful? the impact of copy&paste on android application security. In: Proceedings of 2017 IEEE Symposium on Security and Privacy (SP), pp:121–136.

Jain A K, & Shanbhag D. 2012. Addressing security and privacy risks in mobile applications. *IT Professional,*14:28–33.

Sarhan A Y , and Carr S. 2017. A highly-secure self-protection data scheme in clouds using active data bundles and agent-based secure multi-party computation. In:Proceedings of the 4th International Conference on Cyber Security and Cloud Computing (CSCloud*)*. pp. 228-236.

Sarhan A Y and Lilien L T. 2014. An Approach to Identity Management in Clouds without TrustedThird Parties. Transaction of the 11th Western Michigan IT Forum. *arXiv preprint arXiv*:1904.008801:18-27. EID: 2-s2.0-85093192788.

Sarhan AY. 2017. "Protecting Sensitive Data in Clouds Using Active Data Bundles and Agent-Based Secure Multi-Party Computation," Ph.D. dissertation, Western Michigan University.DOI: 10.1109/CSCloud.2017.36.

SHAMIR A. 1984. Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology: Springer.

ION M, KREUTER B, NERGIZ A E, et al. 2020. On Deploying Secure Computing: Private Intersection-Sum-with-Cardinality. In: *IEEE European Symposium on Security and Privacy (S&P)*, pp. 370–389.

EGELE M, BRUMLEY D, FRATANTONIO Y, KRUEGEL C. An Empirical Study of Cryptographic Misuse in Android Applications.2013. In: ACM Conference on Computer and Communications Security (CCS), pp. 73–84.

Michael K, R Abbas. 2020. Behind COVID-19 Contact Trace Apps: The Google-Apple Partnership, *IEEE Consumer electronics magazine*,9: 71–76

TMNU A, Jyoty WB, Siddik M, Newaz NT, Al Wahid SKA, Mesbahuddin S M. 2020. IoT based low-cost robotic agent design for disabled and Covid-19 virus affected people. In: Proc. World Conf. Smart Trends Syst. Secur. Sustain. WS4 2020, p. 23–6.

Zhou S, Zhou S, Zheng Z, Lu J. 2021. Optimizing spatial allocation of COVID-19 vaccine by agent-based spatiotemporal simulations. *GeoHealth*, 5: e2021GH000427.

Kadinski L, Berglund E, Ostfeld A. 2022. An Agent-Based Model for Contamination Response in Water Distribution Systems during the COVID-19 Pandemic. *Journal of Water Resources Planning and Management*, 148: 04022042.

Castro B M, de Melo Y D A, Dos Santos N F, da Costa Barcellos A L, Choren R, Salles R M. 2021. Multiagent simulation model for the evaluation of COVID-19 transmission. *Computers in Biology and Medicine*, 136: 104645.

Hotton A L, Ozik J, Kaligotla C, et al. 2022. Impact of changes in protective behaviors and out-of-household activities by age on COVID-19 transmission and hospitalization in Chicago, Illinois. *Annals of Epidemiology*. 76: 165-173.

Rimpiläinen S, Thomson J, Morrison C. 2020. Global Example of COVID-19 Surveillance Technologies. Flash Report; Technical Report for Digital Health & Care Institute, Available at https://strathprints.strath.ac.uk/72028/ (accessed Jan. 24 2023).

Aisec F. 2020. Pandemic Contact Tracing Apps: DP-3T, PEPP-PT NTK, and ROBERT from a Privacy Perspective. *Cryptology ePrint Archive.*

Troncoso C, Payer M, Hubaux J P, Salathé M, Larus J, Bugnion E, Lueks W, Stadler T, Pyrgelis A, Antonioli D, et al. 2005. Decentralized Privacy-Preserving Proximity Tracing. *arXiv 2020, arXiv:2005.12273*.

Shubina V, Holcer S, Gould M, Lohan E.S. 2020. Survey of decentralized solutions with mobile devices for user location tracking,proximity detection, and contact tracing in the covid-19 era. *Data*, 5: 87

Surokkha App. 2022, Available at https://surokkha.gov.bd/. (accessed Jan. 24 2023).

Trieu N, Shehata K, Saxena P, Shokri R, Song D, Epione: Lightweight contact tracing with strong privacy.

arXiv2020, arXiv:2004.13293v3. Available at https://arxiv.org/abs/2004.13293 (accessed Oct. 1 2022).

Bielova N, Boutet A, Castelluccia C, Cunche M, Lauradoux C, Metayer D.L, Roca V.2020. DESIRE: A Third Way for a European Exposure Notification System; Technical Report, Available at https://arxiv.org/abs/2008.01621 (accessed Oct. 1 2022).

Avitabile G, BottaV, Iovino V, Visconti I. 2020. Towards Defeating Mass Surveillance and SARS-CoV-2: The Pronto-C2 Fully Decentralized Automatic Contact Tracing System. Cryptology ePrint Archive.

IO. 2022, Available at https://io.italia.it/

LoddersA, Paterson J.M. 2020. Scrutinising COVID Safe Frameworks for evaluating digital contact tracing technologies. *Alternative Law Journal*. 45: 153–161.

von WylV, Höglinger M, Sieber C, Kaufmann M, Moser A, Serra-Burriel M, Ballouz T, Menges D, Frei A, Puhan M.A. 2020. Are COVID-19 proximity tracing apps working under real-world conditions? Indicator development and assessment of drivers for app (non-) use. *medRxiv*.

Reelfs J H, Hohlfeld O, Poese I. 2020. Corona-Warn-App: Tracing the Start of the Official COVID-19 Exposure Notification App for Germany, *arXiv:2008.07370*. Online at https://arxiv.org/abs/2008.07370(accessed Oct. 1 2022).

WymantC, Ferretti L, Tsallis D, Charalambides M, Abeler-Dörner L, Bonsall, D.; Hinch R, Kendall M, Milsom L, Ayres M, et al. 2021. The epidemiological impact of the NHS COVID-19 App. *Nature*, 594: 408–412.

MessaiM, Seba H. 2020. Short Paper: Privacy Comparison of Contact Tracing Mobile Applications for COVID-19.*arXiv**2020**, arXiv:2010.03232v1*. Available at https://arxiv.org/pdf/2010.03232.pdf(accessed Oct. 1 2022).

Raskar, R.; Schunemann, I.; Barbar, R.; Vilcans, K.; Gray, J.; Vepakomma, P.; Kapa S, Nuzzo A, Gupta R, Berke A, et al. Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic. *arXiv**2020**, arXiv:2003.08567.* Available at https://arxiv.org/abs/2003.08567 (accessed Oct. 1 2022).

Azad M.A, Arshad J, Akmal A, Riaz F, Abdullah S, Imran M, Ahmad F.2020. A First Look at Privacy Analysis of COVID-19 Contact Tracing Mobile Applications. *arXiv**2020**, arXiv:2006.13354*. Available at https://arxiv.org/abs/2006.13354(accessed Oct. 1 2022).

Srithas S, Navaratnam S. 2020. Facedrive Health's Contact Tracing Platform, "TraceSCAN" to Help Mitigate and Forecast Future COVID-19 Outbreaks. Available at https://www.businesswire.com/news/home/20200528005281/en/Facedrive-Health\ T1\textquoterights-Contact-Tracing-Platform-\T1\textquotedblleftTraceSCAN\T1\textquotedblright-to-Help-Mitigate-and- Forecast-Future-COVID-19-Outbreaks. (accessed Oct. 1 2022).

Trusted Travel, My Covid Pass. 2021, Available at https://africacdc.org/trusted-travel/. . (accessed Oct. 1 2022).

Wu, P.L. China's Coronavirus Health Code Apps Raise Concerns over Privacy. Available at https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy. (accessed Oct. 1 2022).

Trivedi A, Zakaria C, Balan R, Becker A, Corey G, Shenoy P. 2021. WiFiTrace: Network-based Contact Tracing for Infectious Diseases Using Passive WiFi Sensing. In: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies: New York, NY, USA, 5:1-26.

Prasad A, Kotz D. 2017. ENACT: Encounter-based architecture for contact tracing. In: Proceedings of the WPA 2017, 4th International Workshop on Physical Analytics, Co-Located with MobiSys, Niagara Falls, NY, USA, pp. 37–42.

Zhang C, Xu C, Sharif K, Zhu L. 2021. Privacy-preserving contact tracing in 5G-integrated and blockchain-based medical applications. *Computer Standards Interfaces*, 77: 103520

Roy A, Kumbhar F.H, Dhillon H S, Saxena N, Shin S.Y, Singh S. 2020. Efficient Monitoring and Contact Tracing for COVID-19:A Smart IoT based Framework. *IEEE Internet of Things Magazine*. 33: 17–23.

Angelopoulos C M, Damianou A, Katos V. 2020. DHP Framework: Digital Health Passports Using Blockchain Use case on international tourism during the COVID-19 pandemic. *arXiv:2005.08922*. Available at https://arxiv.org/abs/2005.08922(accessed Oct. 1 2022).

Jung Y, Agulto R. 2021. A Public Platform for Virtual IoT-Based Monitoring and Tracking of COVID-19. *Electronics*,10: 12.

Kuk S, Jeon Y, Kim H. 2017. Detecting outdoor coexistence as a proxy of infectious contact through magnetometer traces. *Electronics Letters*, 53: 1293–1294.

Mehta S, Grant K, Atlin C, Ackery A. 2020. Mitigating staff risk in the workplace: The use of RFID technology during a COVID-19 pandemic and beyond. *BMJ Health Care Informatics*, 27: 3.

JeongS, Kuk S, Kim H. A. 2019. Smartphone Magnetometer-Based Diagnostic Test for Automatic Contact Tracing in Infectious Disease Epidemics. *IEEE Access* 7:20734–20747.

XiongL, Shahabi C, Da Y, Ahuja R, Hertzberg V, Waller L, Jiang X, Franklin A. 2020. REACT: Real-time contact tracing and risk monitoring using privacy-enhanced mobile tracking. In The *SIGSPATIAL Special*, 12:3–14.

Narvaez A A, Guerra J G. 2021. Received Signal Strength Indication—Based COVID-19 Mobile Application to Comply with Social Distancing Using Bluetooth Signals from Smartphones. In Data Science for COVID-19, Elsevier.

Halder B. 2017. Crowdsourcing crisis management platforms: a privacy and data protection risk assessment and recommendations.

Hatamian M. 2020. Engineering privacy in smartphone apps: A technical guideline catalog for app developers. *IEEE Access*, *8*, 35429-35445.

Wang Y, Li J, Zhao X, Feng G, Luo X. R. 2020. Using mobile phone data for emergency management: A systematic literature review. *Information Systems Frontiers*, 22: 1539-1559.

Avanzi D, Foggiatto A, dos Santos V. A, Deschamps F, Loures, E. D. F. R. 2017. A framework for interoperability assessment in crisis management. *Journal of Industrial Information Integration*, 5: 26-38.

Grinko M, Kaufhold M A, Reuter C. 2019. Adoption, use and diffusion of crisis apps in germany: A representative survey. In: Proceedings of Mensch und Computer,pp. 263-274.

Tauhidi SI, Abubakar A, Ishola A, Babate A I, Tanko M A. A, Abdulkadi A. M.et al. 2022. ABAFOR: A Blockchain-based Privacy-Preserving Architecture for Efficient Contact Tracing and GIS Analysis. *European Journal of Electrical Engineering and Computer Science*, 6:88-102.

Kissner L, Song D. 2005. Privacy-preserving set operations. In: Annual International Cryptology Conference, pp. 241-257.

Hernández-R, J L, Karopoulos G, Geneiatakis D, Martin, T., Kambourakis, G., &Fovino, I. N. 2021. Sharing pandemic vaccination certificates through blockchain: Case study and performance evaluation. *Wireless Communications and Mobile Computing*, 2021:1-12

Trieu N, Shehata K, Saxena P, Shokri R, Song D. 2020. Epione: Lightweight contact tracing with strong privacy. *arXiv preprint arXiv:2004.13293*.

CovPass, Jan. 2021, Available at https://play.google.com/store/apps/details?id=de.rki.covpass.app.

Karopoulos G, Hernandez-Ramos J. L, KouliaridisV, Kambourakis G. 2021. A survey on digital certificates approaches for the covid-19 pandemic. *IEEE Access*, 9: 138003-138025.

Hicks C, Butler D, Maple C, Crowcroft J. 2020. SecureABC: Secure antibody certificates for COVID-19, *arXiv:2005.11833*. Available at https://arxiv.org/abs/2005.11833 (accessed on Dec. 20 2022).

Bansal A, Garg C, Padappayil R. P. 2020. Optimizing the implementation of COVID-19 'immunity certificates' using blockchain, Journal of Medical Systems, 44: 1–12.

Commonpass.https://play.google.com/store/apps/details?id=org.thecommonsproject.android.commonpass&hl=en&gl=US(accessed Jul. 15 2022).

AOKPass. Available at https://www.aokpass.com/(accessed Jul. 15 2022).

Certify Health. Available at https://eithealth.eu/project/certify-health/(accessed Jul. 15 2022).

Othmane L B, Lilien L. 2009. Protecting privacy of sensitive data dissemination using active bundles. In: *2009 World Congress on Privacy, Security, Trust and the Management of e-Business*, pp. 202-213.

CDC. Requirement for Proof of COVID-19 Vaccination for Air Passengers. Available online at https://www.cdc.gov/coronavirus/2019-ncov/travelers/proof-of-vaccination.html#faq (accessed on Dec. 20 2022).

Gover A R, Harper S B, Langton L. 2020. Anti-Asian hate crime during the COVID-19 pandemic: Exploring the reproduction of inequality. *American journal of criminal justice*, *45*:647-667.

Fan B, Andersen D G, Kaminsky M, and Mitzenmacher M. 2014. Cuckoo Filter: Practically Better Than Bloom. In: Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies, pp 75–88.

Bloom B H. 1970. Space/Time Trade-offs in Hash Coding with Allowable Errors. *Communications of the ACM*, 7:422–426.

BaldiP, Baronio R, De Cristofaro E, Gasti , Tsudik G. 2011. Countering gattaca: efficient and secure testing of fully-sequenced human genomes. In: Proceedings of the 18th ACM conference on Computer and communications security, pp. 691-702.

NORTON ROSE FULBRIGHT. 2020. Contact tracing apps in Canada. Available at https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/canada-contact-tracing.pdf (accessed Oct. 1 2022).

Pandey P, Bender M.A, Johnson R, Patro R. 2017. A General-Purpose Counting Filter: Making Every Bit Count. In: SIGMOD Conference, pp. 775–787.

Gassmann A. 2020. WeTrace. Available at https://github.com/AndreasGassmann/WeTrace#decentralized(accessed Jun. 4 2022).

AarogyaSetu. 2020. available at https://www.mygov.in/aarogya-setu-app/ (accessed Jun. 4 2022).

Storeng K T & de Bengy P A. 2021. The Smartphone Pandemic: How Big Tech and public health authorities partner in the digital response to Covid-19. *Global Public Health*, 16: 1482-1498.

LEAP USER GUID. 2003. Available at http://emmanuel.adam.free.fr/jade/doc/tutorials/LEAPUserGuide.pdf (accessed Dec. 1 2022).

Agent.WorkBenach. 2017. Available athttps://enflexit.gitbook.io/agent-workbench(accessed Dec. 1 2022).

Calvaresi D, Dubovitskaya A, Calbimonte J P, et al.2018. Multi-agent systems and blockchain: Results from a systematic literature review. In: Proceedings of the 16th International Conference on Practical Applications of Agents and Multi-Agent Systems, pp. 110-126

Angelou N, et al. 2020. Asymmetric private set intersection with applications to contact tracing and private vertical federated machine learning. arXiv preprint arXiv:2011.09350.

Al-Gburi A, Abdullah O, Sarhan A Y, & Al-Hraishawi H. 2022. Channel Estimation for UAV Communication Systems Using Deep Neural Networks. Drones, 6:326.DOI: 10.3390/drones6110326

Sarhan A and Jemmali M. 2023. Novel intelligent architecture and approximate solution for future networks. *Plosone*, 18(3):e0278183. .https://doi.org/10.1371/journal.pone.0278183

Sarhan A, Jemmali M, and Ben Hmida A. 2021. Two routers network architecture and scheduling algorithms under packet category classification constraint. In: Proceedings of the 5th International Conference on Future Networks & Distributed Systems (ICFNDS ’21). Dubai, UAE, pp. 119-127.DOI: 10.1145/3508072.3508092

Sarhan A, "A novel smart multilevel security approach for secure data outsourcing in crisis," PeerJ computer science, 2023.

Bellifemine F, Caire G & Greenwood D.2007. Developing multi-agent systems with JADE. John Wiley & Sons

Figure 1

General architecture of current crisis apps platforms interaction

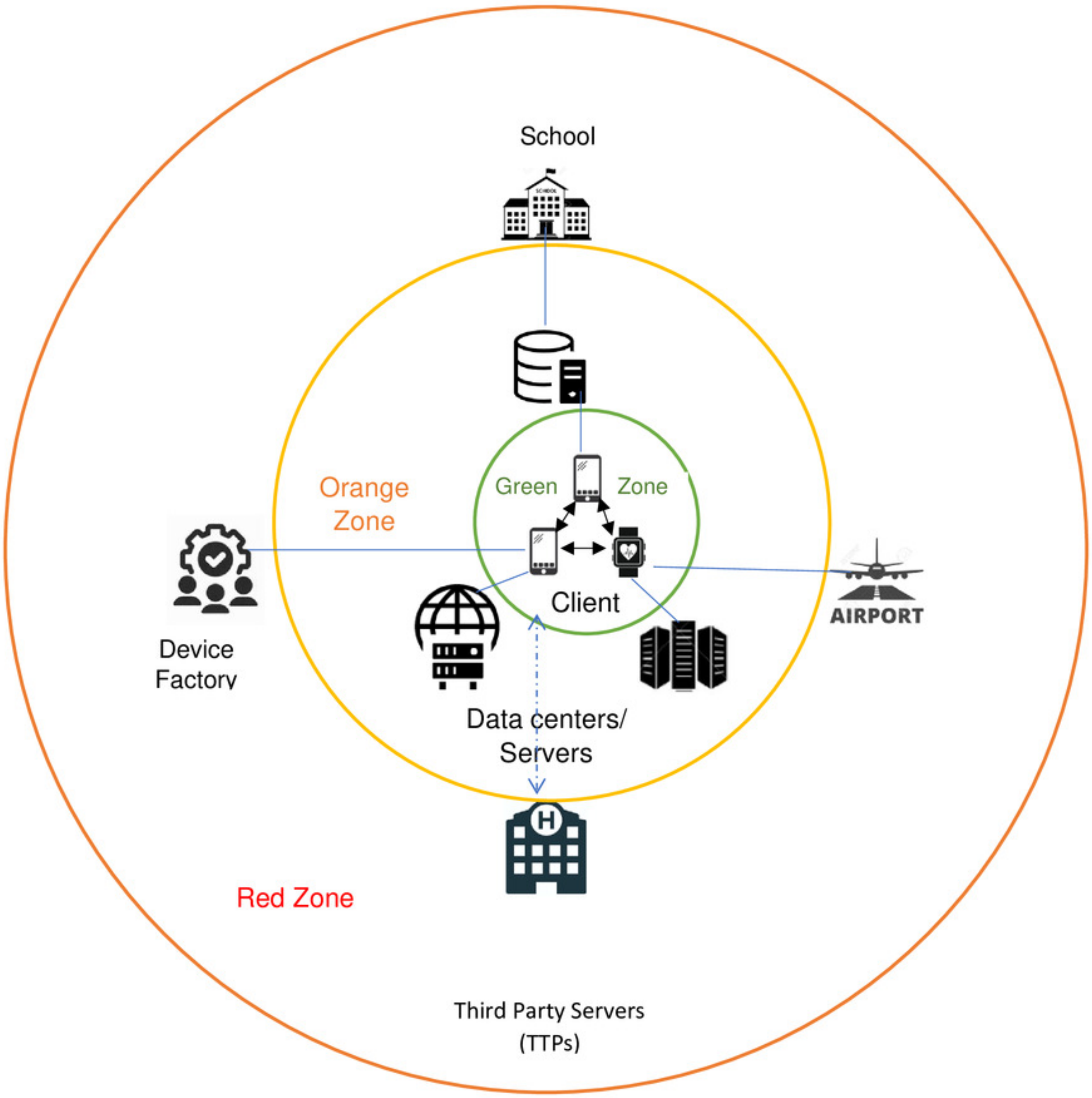

School
Orange Zone
Green Zone
Device Factory
Client
AIRPORT
Data centers/ Servers
Red Zone
Third Party Servers (TTPs)

Figure 2

Secure Mobile digital passport agent (SMDPA) high-level architecture

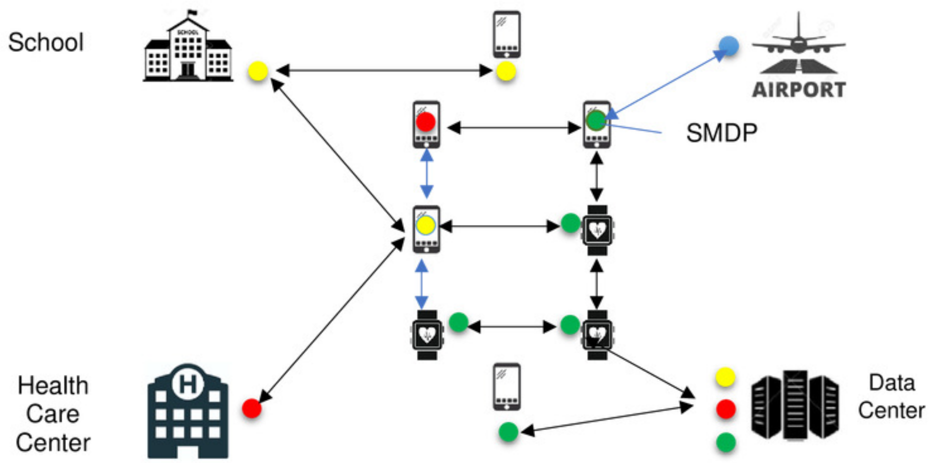

School
AIRPORT
SMDP
Health
Care
Center
Data
Center

Figure 3

The component of SMDP solution

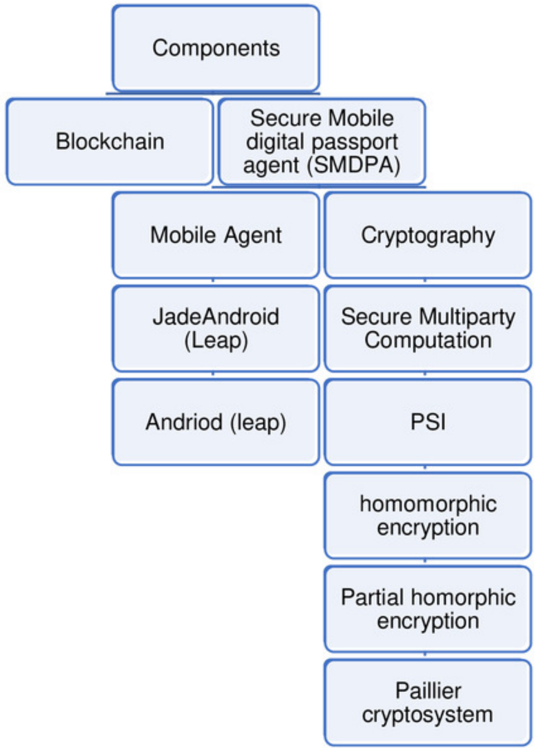

Components
Blockchain
Secure Mobile digital passport agent (SMDPA)
Mobile Agent
Cryptography
JadeAndroid (Leap)
Secure Multiparty Computation
Andriod (leap)
PSI
homomorphic encryption
Partial homorphic encryption
Paillier cryptosystem

Figure 4

Basic PSI Protocol Adapted from (Angelou N, et al. 2020)

Parameters: (i) cyclic group G , (ii) hash function H, and (iii) boolean flag Show the Intersection.

Server Agent, Input: a set $A = \{a_1, \ldots, a_{n1}\}$ SMDPA, Input a set $M = \{m_1, \ldots m_{n1}\}$

Server setup:

1. Server picks random number $\alpha \leftarrow_S Z_q$
2. Server compute $uj = H(a_i)\ \alpha$ such that $j \in [N]$
3. Server insert $\{ uj,\ j \in [N] \}$ into a filter of type x

Protocol :

1. SMDPA samples $\alpha \leftarrow Z_q$ randomly, for each $m_l \in M$ sends D_j to the server agent
2. Agent Server computer $D_j^{'} = D_j^{\alpha}$
3. Agent Server sends $\{ D_j^{'},\ j \in [N] \}$to SMDPA if Show the Intersection is true
4. SMDPA computer $v_j = (D_j^{'})^{1/r}$ for each , $j \in [N]$
5. SMDPA queries the filter for each v_j and computes $Z = \{ j \in [N] \mid v_j \in \text{filter } x\}$

Figure 5

SMDPA approach execution in run time environment

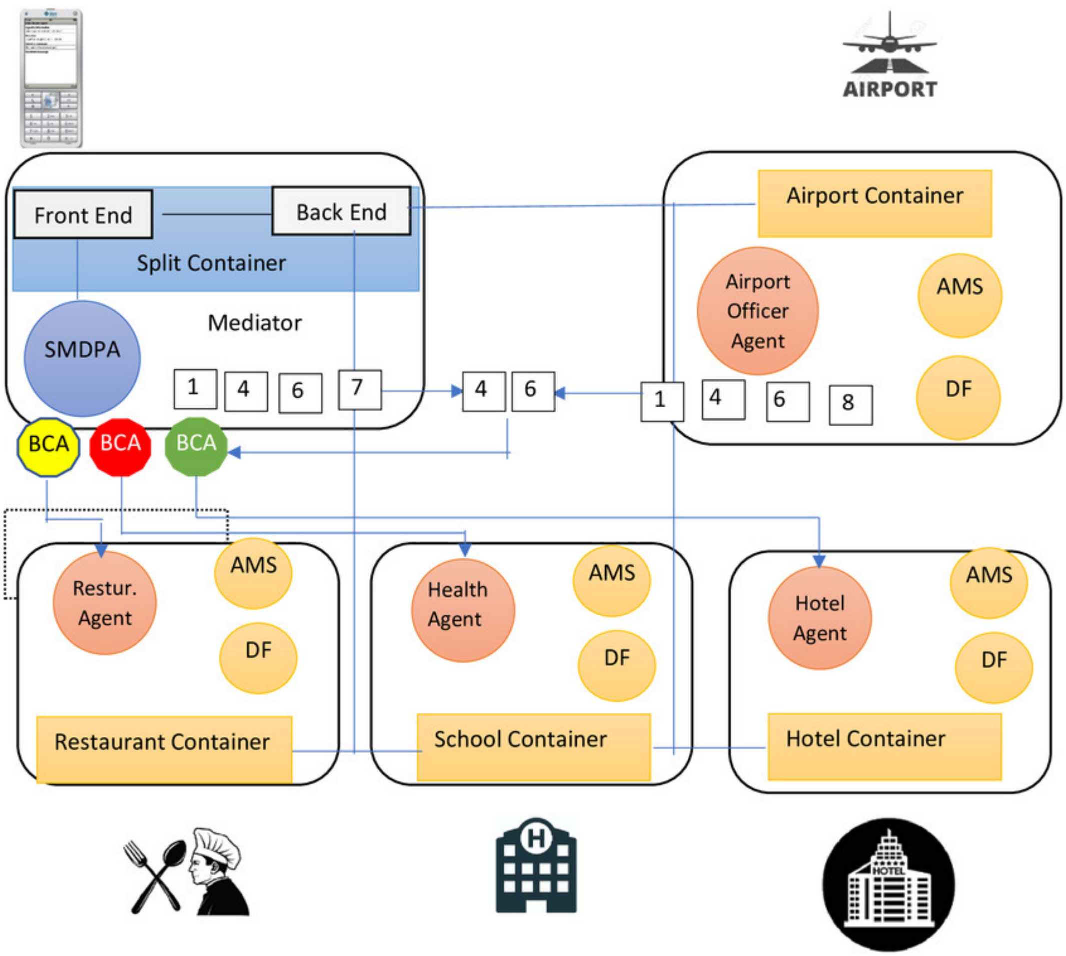

AIRPORT
Front End
Back End
Split Container
Mediator
SMDPA
1
4
6
7
4
6
Airport Container
Airport Officer Agent
AMS
DF
1
4
6
8
BCA
BCA
BCA
Restur. Agent
AMS
DF
Restaurant Container
Health Agent
AMS
DF
School Container
Hotel Agent
AMS
DF
Hotel Container
HOTEL

Figure 6

SMDPA UML sequence Diagram

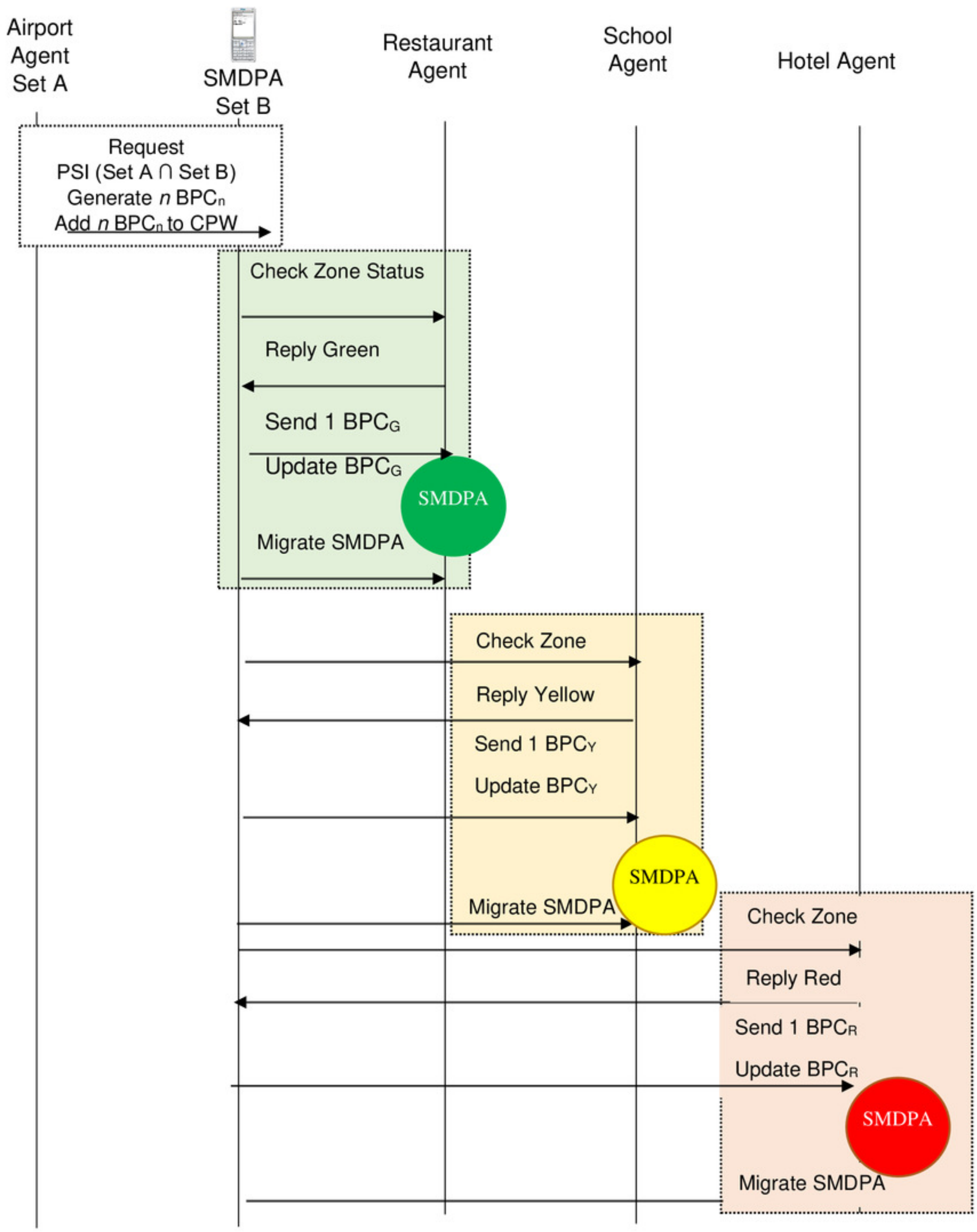

Airport Agent Set A
SMDPA Set B
Restaurant Agent
School Agent
Hotel Agent
Request
PSI (Set A ∩ Set B)
Generate n BPCn
Add n BPCn to CPW
Check Zone Status
Reply Green
Send 1 BPCG
Update BPCG
SMDPA
Migrate SMDPA
Check Zone
Reply Yellow
Send 1 BPCY
Update BPCY
SMDPA
Migrate SMDPA
Check Zone
Reply Red
Send 1 BPCR
Update BPCR
SMDPA
Migrate SMDPA

Figure 7

CPU Load's performance for SMDPA and the AirportAgent interaction

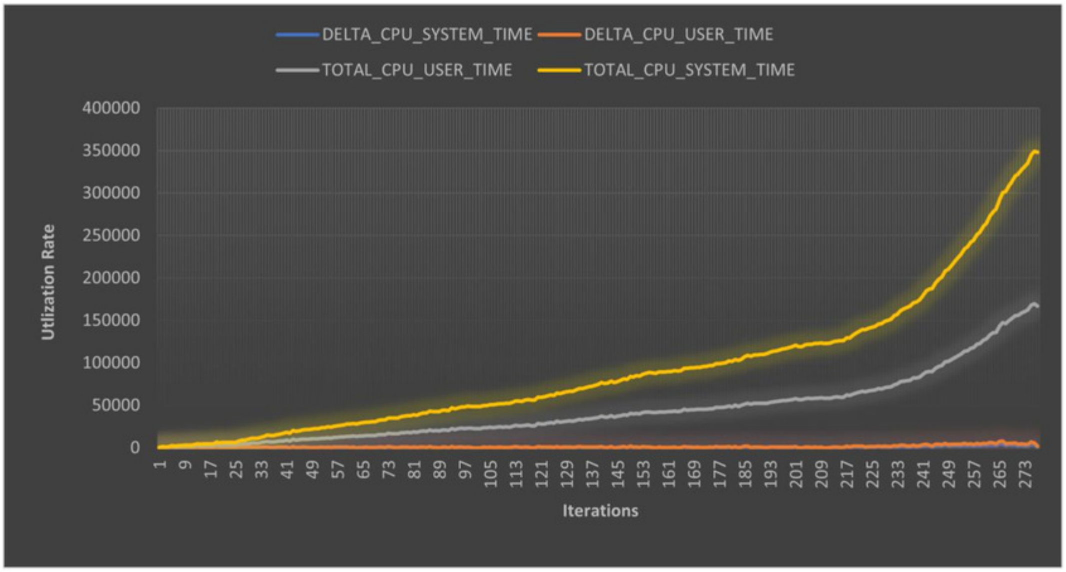

DELTA_CPU_SYSTEM_TIME
DELTA_CPU_USER_TIME
TOTAL_CPU_USER_TIME
TOTAL_CPU_SYSTEM_TIME
Utlization Rate
Iterations

Figure 8

CPU Load Time for SMDP and the AirportAgent

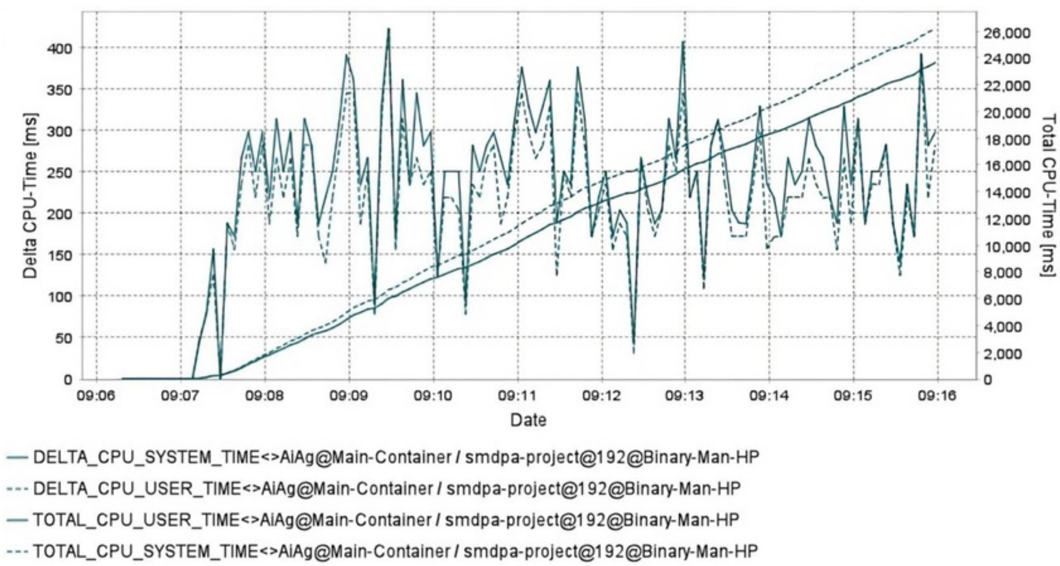

Delta CPU-Time [ms]
Total CPU-Time [ms]
Date
09:06
09:07
09:08
09:09
09:10
09:11
09:12
09:13
09:14
09:15
09:16
DELTA_CPU_SYSTEM_TIME<>AiAg@Main-Container / smdpa-project@192@Binary-Man-HP
DELTA_CPU_USER_TIME<>AiAg@Main-Container / smdpa-project@192@Binary-Man-HP
TOTAL_CPU_USER_TIME<>AiAg@Main-Container / smdpa-project@192@Binary-Man-HP
TOTAL_CPU_SYSTEM_TIME<>AiAg@Main-Container / smdpa-project@192@Binary-Man-HP

Figure 9

SMDPA Algorithms average time

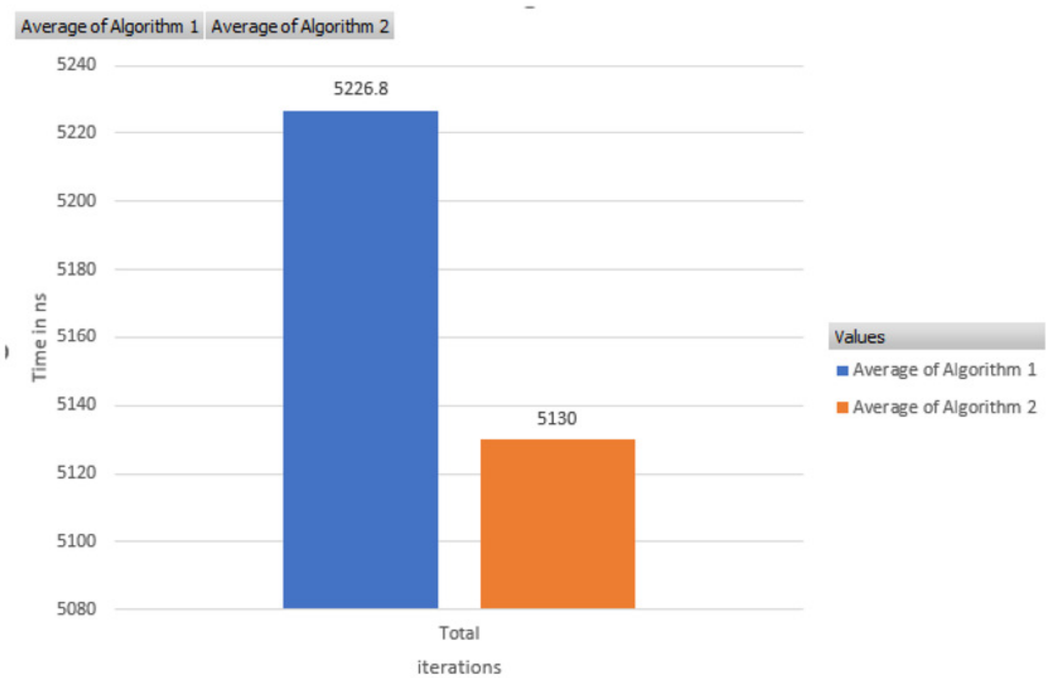

Average of Algorithm 1
Average of Algorithm 2
5240
5220
5200
5180
5160
5140
5120
5100
5080
Time in ns
5226.8
5130
Total
iterations
Values
Average of Algorithm 1
Average of Algorithm 2

Table 1 (on next page)

Crisis apps major comparison, features, and privacy-preserving underlying technologies

Platform	Domain	Deployment Model	Protocol	Underlying Technology.	Data Sensitivity level	Mandatory Data Minimization	Privacy Violation Level	Possible Target Attack risks Severity Factor	Interoperability
Tawakkalna	RBS,IP	Cent.	N/A	Bluet/GPS	1,5,6	NO	S	4	No
Apple&Google	CT NT	Dec.	Apple.Goog.	Bluetooth	N/A	NO	S	4, 13, 14	Yes
TraceTogether	CT	Cent.	BlueTrace	Bluetooth	1,2	NO	M	12,14	No
COVIDSafe	CT	Cent.	BlueTrace	Bluetooth	1	NO	M	5, 14	No
Aarogya Setu	CT	Cent.	N/A	Bluet/GPS	4,5	NO	S	1, 14, 15	No
ABTraceTogat.	CT	Cent.	BlueTrace	Bluetooth	4	NO	S	14	No
SwissCOVID	CT	Dec	AppleGoog. DP-3T	Bluetooth	1	NO	L	6	No
CoronaWarn	CT	Dec	DP3TPEPPT	Bluetooth		Yes	L	14	No
NHS-COVID19	CT	Dec	AppleGoogl.	Bluetooth	3	NO	L	2,3,4,12,13	No
WeTrace	CT	Dec		GPS Bluetooth	3,6	NO	S	2,3,14,15,1 6	No
Conrona-Korea	CT Self-D	Cent.		GPS	1,2,5	NO	S	2,3	No
USA Safepaths	CT	Dec		Bluet. GPS		NO	L	2,3,12, 15	No
Covid-19 KP	CT	Dec		Bluet/GPS		NO	S	12, 15	No
Iranian AC19	Self-D CT	Dec		GPS	1,5	NO	S	2,3	No
TraceScan	CT RAS	Hyb.		Bluet. Wear (ML)	4,7,8	NO	L	2,3	No
Chinese Alipay	RBS CT	Cent.		AI	1,3	NO	S	2,3	No
LeaveHomeSafe	CT	Dec		AI		NO	S	11	No
WifiTrace	CT	…		Wi-Fi			S	15, 1,7,8,9 10,2,3	No
ENACT	CT	Cent.		Wi-Fi-		NO	S	14,15	No
MagnetomTrace	CT			Magnetom.			M	15,16	No
PTBM	CT			5G-Block.					No
RFID-based CT	CT			RFID			S	17	No
IoT-based-CT	CT MOFU			IoT			S	1,15	No
SDN-Plat.	TeS	Cen		SDN			M		No
IoT.SDN-Plat.	MO	Cent.		IoT& SDN			M	18	No
Block.Magneto meter	CT	Dec		Magnetom eter			L	19	No
RSSI-based-SD	SD	N/A		Bluetooth RSSI	8		M	13,14	No
RSSI-based-SD	SD	N/A		Bluetooth RSSI (ML)	8		M	13,14	
REACT	CT	Cent.		GPS BLE	5	NO	S	2,3,14	No
MyCOVID Pass	IP [111]	Cen/ Dec.		N/A	N/A	N/A			AU
Blockchain.plat.	IP	Dec.		Blockchain	N/A		L		EU
IO app	IP[102]	N/A		N/A	N/A	Opt.	S	2	
Surokkha app	IP	Cen.		N/A	N/A	No	S	2, 14	No
Coronapas app	IP		PKI			N/A	S	2,3	No
CovPass	IP	Dec.		N/A	3	Opt.	L	11	EU
SMDPA	DHDP	Dec.	Agent-based PSI(PKI)		N/A	Yes	L	N/A	Yes

Table 2(on next page)

List of acronyms for feature terms in Table 1

Acronym	Term	Acronym	Term
RBS	Response Based System	TeS	Telemedicine Services
CT	Contact Tracing	RSSI	Received Signal Strength Indicator
NT	Notification Systems	Cent.	Centralized
MN	Monitoring	Dec	Decentralized
FU	Follow Up	Hyb.	Hybrid
SD	Social Distance	AU	African Union
IP	Immunity Passports	EU	European Union
RAS	Risk Alerting System	Self-D	Self-Diagnosis
DHDP	Digital Health and Data Passport		

Table 3 (on next page)

Privacy-Preserving risks/threats impact level

Name of Issues	Risk Impact Factor	Name of Issues	Risk Impact Factor	Name of Issues	Risk Impact Factor
Security & Privacy Flaws	1	Key Recovery	8	Single Point of Failure	14
Sensitive Data Leakage	2	Denial of Service	9	Poor Functionality	15
Health Data Leakage	3	Traffic Description	10	Drain Battery	16
Surveillance	4	QR Code Leak	11	Storage Limitation	17
Replay Attack	5	Data Sharing with TTP	12	Require Technical Skills	18
Linkage Attacks	6	Fail to comply with Privacy Act	13	High Installation and Operation Cost	19
Man in the Middle	7	Profiling	14		

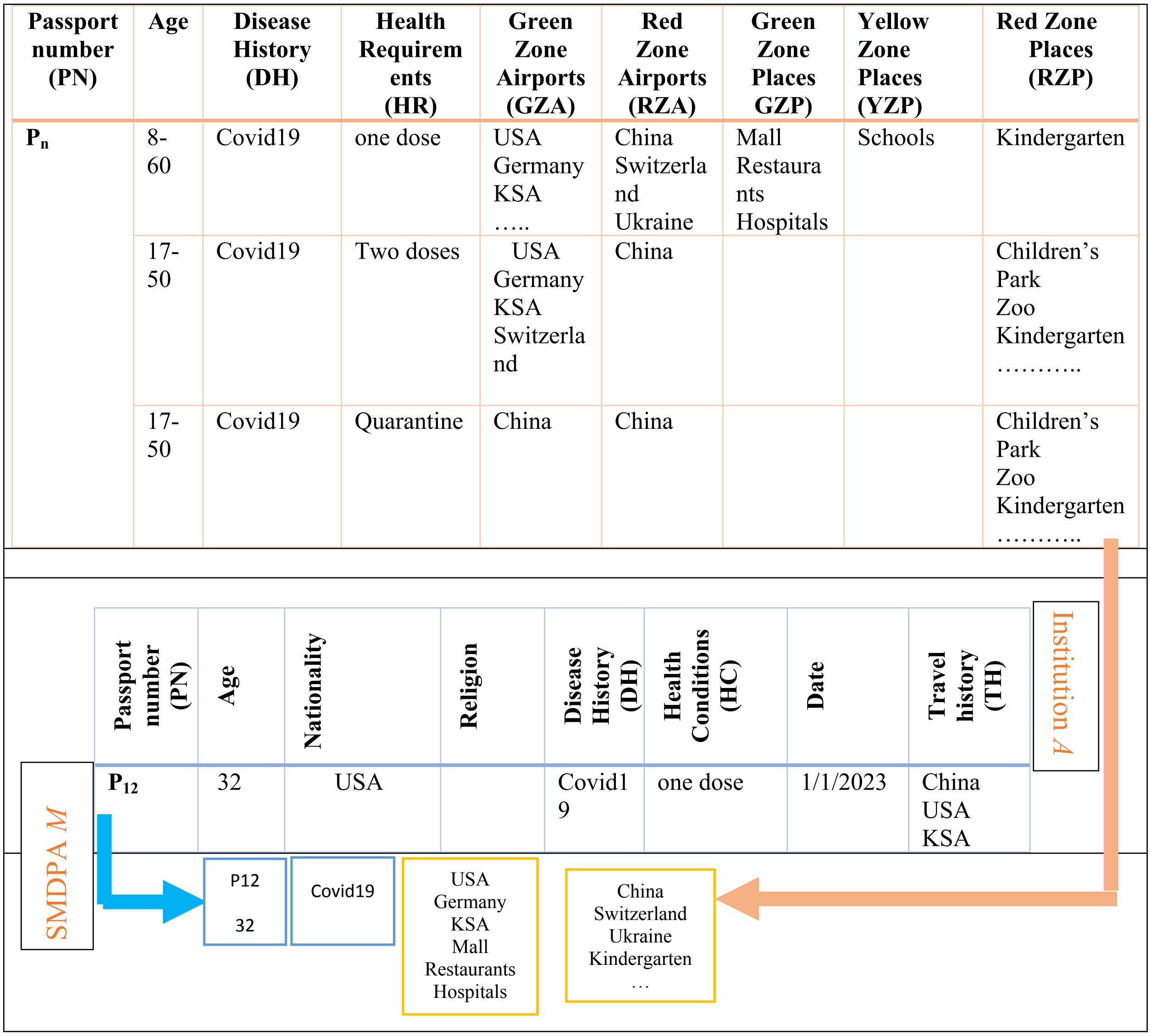
Table 4 (on next page)

Data sensitivity levels for popular crisis apps

Category of Leakage data	Data Sensitivity level	Category of leakage data	Data Sensitivity level
Personal & Identities Data	1	Location Data	5
Health Data	2	Device ID	6
QR code	3	Time	7
Bluetooth ID	4	Distance Information	8

Table 5 (on next page)

Privacy set intersection based on enrichment case


Passport number (PN)
Age
Disease History (DH)
Health Requirements (HR)
Green Zone Airports (GZA)
Red Zone Airports (RZA)
Green Zone Places GZP)
Yellow Zone Places (YZP)
Red Zone Places (RZP)
Pn
8-60
Covid19
one dose
USA Germany KSA …..
China Switzerland Ukraine
Mall Restaurants Hospitals
Schools
Kindergarten
17-50
Covid19
Two doses
USA Germany KSA Switzerland
China
Children's Park Zoo Kindergarten ………..
17-50
Covid19
Quarantine
China
China
Children's Park Zoo Kindergarten ………..
Institution A
Passport number (PN)
Age
Nationality
Religion
Disease History (DH)
Health Conditions (HC)
Date
Travel history (TH)
P12
32
USA
Covid19
one dose
1/1/2023
China USA KSA
SMDPA M
P12
32
Covid19
USA
Germany
KSA
Mall
Restaurants
Hospitals
China
Switzerland
Ukraine
Kindergarten
…

1

Table 6 (on next page)

SMDPA Algorithm Description

Algorithm 1. ***SMDPA*** **Algorithm**

A= SMDPA dataset elements
B= AgentServer dataset elements
C= A ∩ B
IS ← Size of C
TH ← Threshold L1, L2, L3
CPW ← store Coin Passing Wallet (BPC_G, BPC_Y, BPC_R)
if (IS ≥ L1) **then**
    Generate n BPC_G
    Add BPC_G to CPW
else
    if (IS >= L2 && IS < L1) **then**
        Generate n BPC_Y
        Add BPC_Y to CPW
    else
        if (IS >= L3 && IS < L2) **then**
        Generate n BPC_R
        Add BPC_R to CPW
        end if
    end if
end if
Calculate CPW
Return CPW

Table 7
(on next page)

Enhanced SMDPA Algorithm Description

Algorithm 2. Enhanced *SMDPA* Algorithm

A= SMDPA dataset elements
B= AgentServer dataset elements
C= A ∩ B
IS ← Size of C
TH ← Threshold L1, L2
CPW ← store Coin Passing Wallet (BPC_G, BPC_Y, BPC_R)
if (IS >(L1+L2)/2) **then**
Generate n BPC_G
Add BPC_G to CPW
else
if (IS < (L2+L32)/2) **then**
Generate n BPC_Y
Add BPC_Y to CPW
else
Generate n BPC_R
Add BPC_R to CPW
end if
end if
end if
Calculate CPW
Return CPW

Table 8(on next page)

The configuration of the computing environment for SMDPA

Hardware Specification	
CPU	Intel (R)i5-4750T @2.90 GHz
Physical Memory (RAM)	8.0 GB
Storage	1 TB
Software, API(s), Simulation Tools	
Operating system	Microsoft Windows 10 Home
JDK	19
JADE	4.6.0
JADE-LEAP	4.1.1
Java J2ME	2.5.2_01 for CLDC
AgentWorkbench	2.3.0
Communication Specification	
ZTE 5G Wireless Router	Download speed up to 150 Mbps/upload speed 50 Mbps
Communication Protocols	HTTP, RMI