International Journal of
Geo-Information

Technical Note

Technical Analysis of Contact Tracing Platform Developed by Google–Apple for Constraining the Spread of COVID-19

Abdul Majeed

Department of Computer Engineering, Gachon University, Seongnam 13120, Korea; ab09@gachon.ac.kr;
Tel.: +82-10-9503-9597

Abstract: Amid the ongoing COVID-19 pandemic, technical solutions (e.g., smartphone apps, web-based platforms, digital surveillance platforms, etc.) have played a vital role in constraining the spread of COVID-19. The major aspects in which technical solutions have helped the general public (or health officials) are contact tracing, spread prediction, trend forecasting, infection risk estimation, hotspot identification, alerting people to stay away from contaminated places, hospitalization length estimation, clinical severity analysis, and quarantine monitoring, to name a few. Apart from other services, contact tracing has been extensively performed with the help of Bluetooth and GPS-powered smartphone applications when vaccines were unavailable. In this article, we technically analyze the contact tracing platform developed by Google–Apple for constraining the spread of COVID-19. We suggest unexplored technical functionalities that can further strengthen the platform from privacy preservation, service scenarios, and robustness point of view. Lastly, some AI-based and privacy-assured services that can be integrated with the platform to control the pandemic adequately are suggested. The technical analysis demonstrates that while the Google–Apple platform is well-engineered, it is not free of vulnerabilities, weaknesses, and misconfigurations that may lead to its poor adoption in real-life scenarios. This work can serve as a guideline for further enhancing the practicality of contact tracing platform to effectively handle future infectious diseases.

Keywords: COVID-19 pandemic; contact tracing; spread prediction; infection risk estimation; GPS- and Bluetooth-based smart apps; digital surveillance platforms; privacy preservation

Citation: Majeed, A. Technical Analysis of Contact Tracing Platform Developed by Google–Apple for Constraining the Spread of COVID-19. *ISPRS Int. J. Geo-Inf.* **2022**, *11*, 539. https://doi.org/10.3390/ijgi11110539

Academic Editor: Wolfgang Kainz

Received: 3 September 2022
Accepted: 23 October 2022
Published: 28 October 2022

1. Introduction

The ongoing coronavirus disease 2019 (COVID-19) pandemic is one of the toughest challenges humanity has ever faced in terms of infectious diseases. During this period (from January 2020 until the present), most people have stayed at home, and leisure activities, such as large gatherings, travel abroad, concerts, etc., have been canceled/postponed [1]. In the early days of the pandemic, most countries developed digital solutions to fight the pandemic [2]. Most technical developments were made to trace the contacts of infected individuals as soon as possible to curb the spread of the virus [3]. However, in most countries, contact tracing technology was not welcomed by the general public due to privacy concerns (See Table 1 for further details) [4].

Table 1. Overview of the leading contact tracing applications/platforms developed in many countries.

App Name	Main Technology	Deployment Country	Adoption Rate
TraceTogether	Bluetooth	Singapore	High
HaMagen	GPS	Israel	High
COVIDSafe	Bluetooth	Australia	Medium
Arogyan Setu	GPS, Bluetooth	India	Low
COVID Tracker	GPS, Bluetooth	Ireland	Low
NZ COVID Tracer	QR Codes	New Zealand	Low
BeWare	GPS	Behrain	Low

Afterward, many efforts were made to store data locally or collect as little data as possible. Apart from contact tracing, other latest technologies especially AI-based techniques have played a vital role in many aspects [5].

As shown in Table 1, the adoption of most contact tracing apps was not high due to the fine-grained data collection that can enable the tracking of individuals' movements. Due to privacy issues, most countries failed to achieve their targets of 60% of citizens installing and using contact tracing apps [6]. Apart from the apps, comprehensive platforms were also developed in many countries across the globe for lowering the effects of COVID-19 [7]. For example, South Korea developed an integrated epidemic investigation support system (EISS) to disclose the information of people who have contracted the virus [8]. In this platform, data are obtained from multiple stakeholders and used for tracing the contacts of infected people (See Figure 1 for further details).

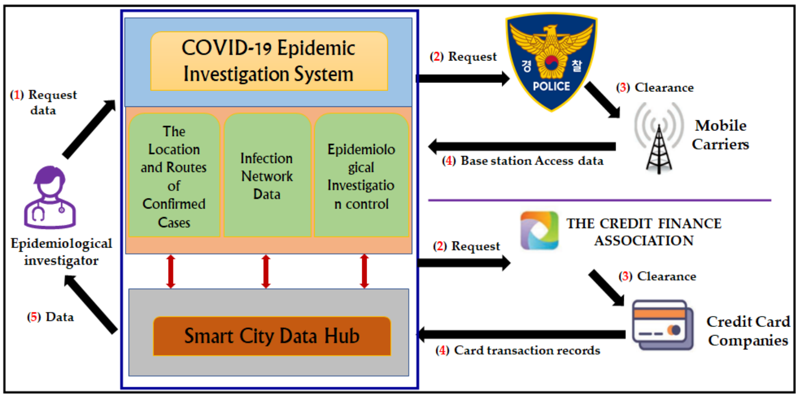

COVID-19 Epidemic Investigation System
The Location and Routes of Confirmed Cases
Infection Network Data
Epidemiological Investigation control
Smart City Data Hub
(1) Request data
Epidemiological investigator
(5) Data
(2) Request
POLICE
(3) Clearance
Mobile Carriers
(4) Base station Access data
THE CREDIT FINANCE ASSOCIATION
(2) Request
(3) Clearance
Credit Card Companies
(4) Card transaction records

Figure 1. Overview of the EISS developed by Korea to fight the COVID-19 (Adopted from [9]).

When most contact tracing apps faced criticism due to privacy concerns, then many options, such as data protection laws, consent-based data use, privacy-aware analytics, and secure data sharing were introduced by the software developers to alleviate those privacy concerns. However, these solutions failed to achieve the desired objectives of installation because either explicit identity-related information was collected, or most data are processed in a black-box manner. Hence, a new privacy-aware system was inevitable to alleviate privacy concerns while curbing the spread of COVID-19. To help health authorities and governments across the world, Google and Apple decided to develop a privacy-preserving contact tracing (PPCT) platform. This platform uses Bluetooth technology to exchange random identifiers when people made close contact with each other. Although the PPCT platform is superior to stand-alone contact tracing apps, it has various technical shortcomings.

Since the start of the pandemic, there has been a debate on the usage of Bluetooth-based and/or GPS-based contact tracing apps from two different angles: (i) are such contact tracing apps good for digital contact tracing, and contribute to containing the spread of the pandemic, or (ii) these digital tools may lead to unbearable inequalities and function/surveillance creep? Since PPCT is the only OS-level technology until present, it is vital to provide technical analysis of it from multiple perspectives to further enhance the technical level of this technology. Although many PPCT have been developed, such as EISS in South Korea, Trace Together in Singapore, and COVID Safe in Australia (Further details can be learned from [10]). However, in those platforms, either fine-grained data (i.e., credit card data, cell phone signals, and CCTV data) were utilized in tracing the contacts of infected people, or explicit location data (GPS, QR-codes) were used to find the exposed contacts. Due to fine-grained data collection and processing, these apps face serious adoption obstacles by the general public (https://www.brookings.edu/techstream/contact-tracing-apps-face-serious-adoption-obstacles/) (accessed on 5 August 2022). In contrast, PPCT developed by Apple and Google does not use any identity/explicit location-related data, and is more privacy conscious than any other such tools. Therefore, we provide extended knowledge about this tool so that it can become a community-beneficial technology to fight future infectious diseases in a privacy-preserved way. Our analysis and technical description can pave the way for improving many technical aspects (computing complexity, scalability, storage consumption, robustness, privacy issues, etc.) of this platform. Furthermore, PPCT has the potential to become a commercial technology shortly, which is why is it very important to technically analyze it for spotting vulnerabilities/performance bottlenecks.

In this paper, our contribution is five-fold:

- We provide the technical analysis of the PPCT platform developed by Google and Apple to lower the spread of COVID-19.
- We suggest various technical unexplored functionalities to enhance the persuasiveness and performance of the PPCT platform to fight future infectious diseases in a privacy-preserved way.
- We suggest practical services that can be a valuable addition to the PPCT platform to serve mankind effectively and to lower the consequences of pandemics/epidemics.
- The contents enclosed in this perspective can contribute to enhancing the service level of this platform in four dimensions: (i) enhancing service scenario (s) beyond contact tracing; (ii) reducing computational complexities, scalability, and other performance bottlenecks; (iii) solving data fragmentation and silos problems; and (iv) enhancing the performance of this platform on resource-constrained devices by preventing function (or surveillance) creeps.
- To the best of the author's knowledge, this is the first work that systematically highlights the working of the PPCT platform, pinpoints invisible deficiencies of the PPCT platform, and suggests additional AI-based services which can be a valuable addition to this platform which has huge potential in becoming a commercial technology in the coming years.

The remainder of this paper is structured as follows. Section 2 presents a technical analysis of the contact tracing platform made by Google and Apple. Section 3 discusses the unexplored additional functionalities in the Apple–Google contact tracing platform. Section 4 provides an analysis of privacy-preserved and AI-based services that can be a valuable addition to Google and Apple's contact tracing platform. Section 6 concludes this paper.

2. Analysis of Privacy-Preserving Contact Tracing Platform Made by Google and Apple

Google and Apple developed a privacy-preserving contact tracing platform, named Exposure Notifications System (https://covid19.apple.com/contacttracing) (accessed on 9 August 2022) (ENS) to curb the spread of COVID-19 through a shared sense of responsibility. It is the first OS-assisted ENS with strong privacy guarantees [11]. The ENS protects the privacy of users by not collecting any location/identity-related data, most processing is done locally without a central server, and only legitimate health authorities use the system under strict rules. Due to these characteristics, ENS is highly secure and privacy-preserved. In addition, it empowers people to decide whether to use the ENS or not. The ENS has seven main modules which jointly work to accomplish the task of contact tracing without revealing any sensitive data: (i) setting up the app on the local devices, (ii) computing keys on the local devices using elegant cryptography concepts, (iii) exchanging keys with the nearby devices in a seamless manner, (iv) uploading keys to the server in case of infection with proper consent, (v) sending exposure notification to the potentially exposed people of a certain locality, (vi) downloading keys and matching the possibility of contact with an infected individual, and (vii) seeking medical help from nearby hospitals. In the next subsections, we provide concise details about each main module.

2.1. Setting Up the App on the Local Devices

In the first step, the app is downloaded from the Google/Apple app store. Afterward, required permissions (e.g., opt-in) are granted from the local devices. A conceptual overview of setting up a contact tracing app by user *A* is shown in Figure 2. After downloading the app, users need to enable exposure notification (EN) on a local device through the opt-in option. During the installation process, a key is generated for each device that is used for tracing purposes. For privacy preservation and to minimize the chances of tracking, the key is changed frequently. During app installation, no directly identifiable information is collected from users, and thereby chances of privacy breaches are restrained.

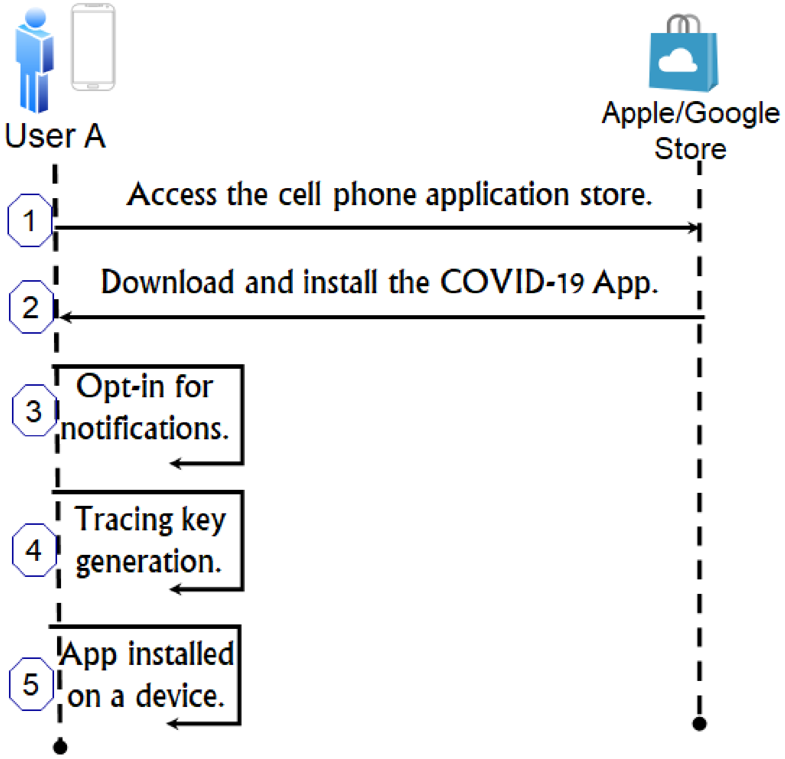

User A
Apple/Google Store
1
Access the cell phone application store.
2
Download and install the COVID-19 App.
3
Opt-in for notifications.
4
Tracing key generation.
5
App installed on a device.

Figure 2. Installing a contact tracing app (i.e., OS-assisted ENS) on a local devices.

2.2. Computing Keys on the Local Devices Using Elegant Cryptography Concepts

In this subsection, we describe the mechanism of key generation using cryptography concepts. In the ENS, there are three main types of keys, tracing key (tk), daily tracing key (dtk), and rolling proximity identifier (rpi). tk is used to derive other keys and assist in maintaining the privacy of users. A conceptual overview of how keys are generated is shown in Figure 3. The formalization of all keys is given in Equations (1)–(3).

$$tk = hash(u) \tag{1}$$

where u can be any English letter. The size of tk is 32 bytes after applying a hash to it.

$$dtk = hash(u + d) \tag{2}$$

where d is any date/day of the month. For example, if the date is 30 then $d = 30$. The size of dtk is 16 bytes after applying a one-way hash to it.

$$rpi = hash(u + d + w_i) \tag{3}$$

where w_i is the respective time window depending on the time of the day. For example, if the time is 10:00 AM then w_{60} = 10:00 AM. The size of rpi is relatively longer compared to the previous two cases.

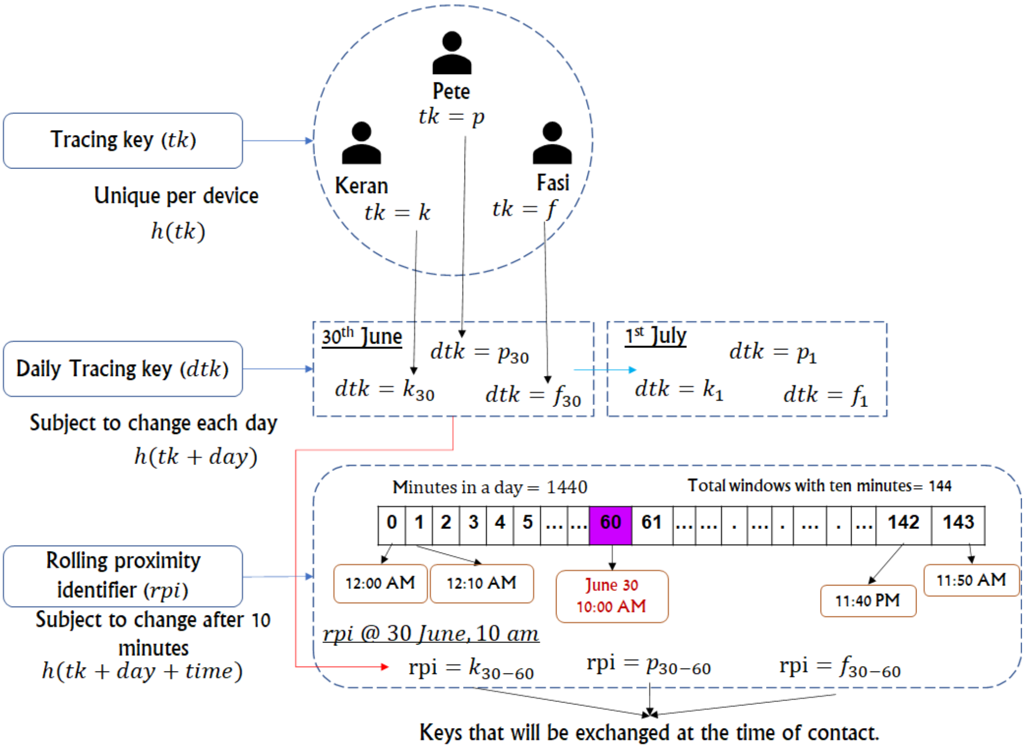


Figure 3. Overview of different keys generation for contact tracing purposes.

Since privacy preservation is included in the design of the ENS and only randomly produced keys (e.g., *tk*, *dtk*, and *rpi*) are exchanged with other devices. Therefore, ENS provides more privacy compared to traditional centralized contact tracing apps. ENS can yield higher adoption because it does not collect any identity-related information and most processing is performed on local devices.

2.3. Exchanging Keys with the Nearby Devices in a Seamless Manner

In this subsection, we describe the key exchange method through which keys are exchanged with nearby devices. Since Bluetooth is operational within a 30 m distance, and, therefore, keys can be exchanged with nearby devices only. Figure 4 demonstrates the procedure of exchanging keys with nearby devices in a seamless manner.

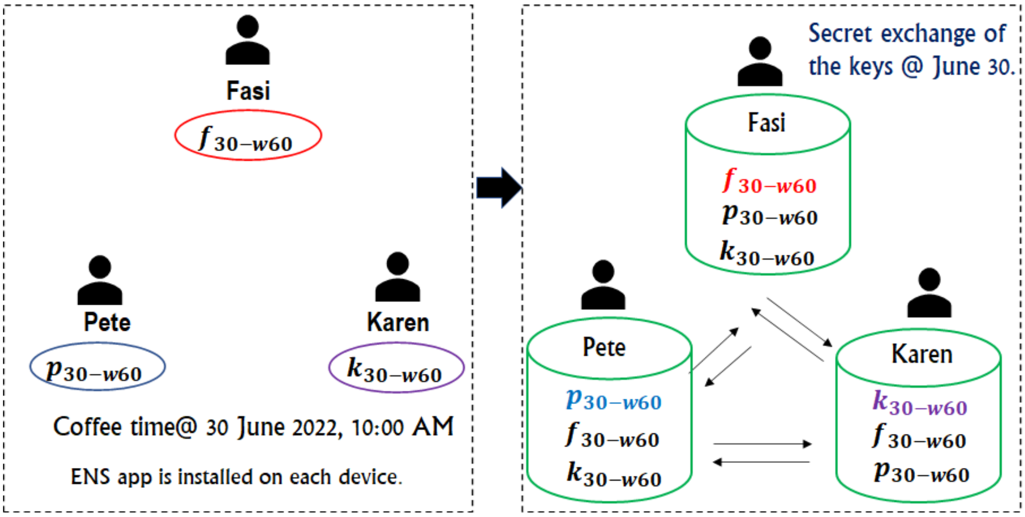


Figure 4. Example of key exchange between three friends in ENS for contact tracing purposes.

In this example, three friends planned to have coffee together at 10:00 AM at the coffee shop. During the meet-up, their cell phones exchanged random keys with each other which can be helpful to constrain the virus spread if one of them tested positive for COVID-19 afterward. As shown in Figure 4, data are stored on local devices, and, therefore, the risk of personal data misuse is minimal. In addition, users of the ENS have less difficulty in maintaining the keys because all keys are exchanged upon close contact seamlessly.

2.4. Uploading Keys to the Server in Case of Infection with Proper Consent

Once a person tests positive for COVID-19, his/her keys are uploaded to the server with proper consent. The main purpose to upload these keys to the server is to find the exposed people as quickly as possible. In the previous example (e.g., three friends had coffee together), and one friend tested positive for COVID-19 the next morning then his/her keys are shared with the legitimate health authorities (see Figure 5 for details). Since servers are located in some locality, and, therefore, contact tracing can be performed for the desired region only.

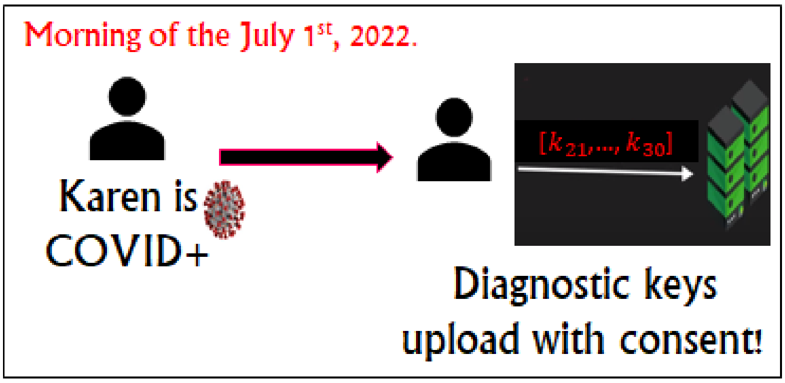

Morning of the July 1st, 2022.
Karen is COVID+
$[k_{21},\ldots,k_{30}]$
Diagnostic keys upload with consent!

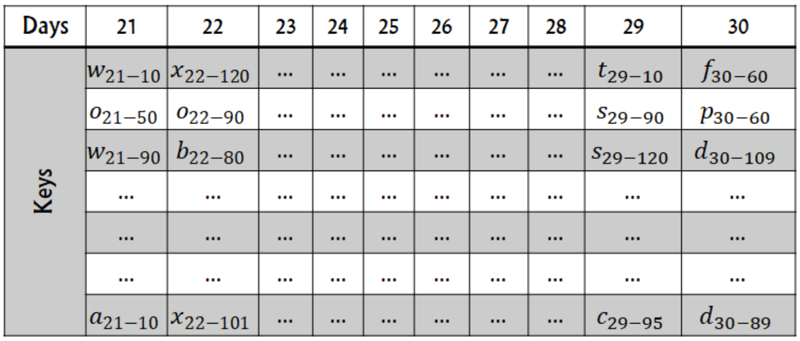
Figure 5. Example of uploading keys to exposure server after infection.

2.5. Sending Exposure Notification to the Potentially Exposed People of Certain Locality

In the previous example, three people had a gathering. Since one friend tested positive for COVID-19, the other two friends need a COVID test also. However, they are unaware that their friend has tested positive for COVID-19. The health authorities will send an exposure notification based on the region's information. After receiving a notification of a possible infection they can further analyze the situation by requesting the keys of infected people. The exposure notification can be sent to many people, but some may not need the test. Therefore, some analysis is performed locally to determine whether one needs to be tested or not.

2.6. Downloading Keys and Matching the Possibility of Contact with an Infected Individual

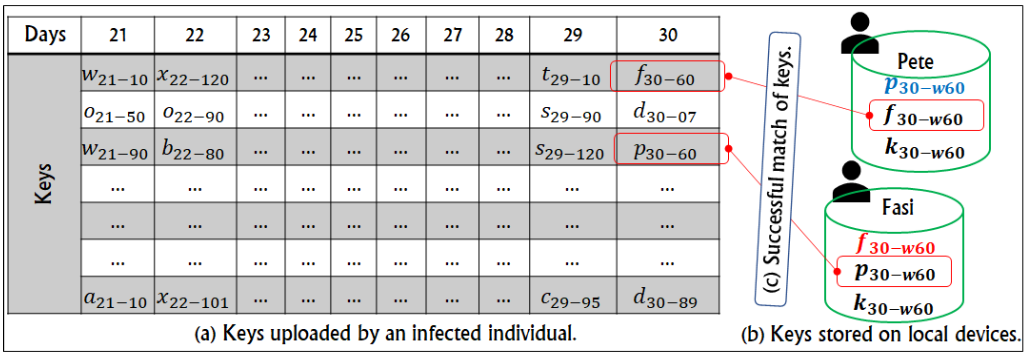
In this step, tracing keys (also known as diagnosis keys) uploaded by an infected individual are downloaded by relevant individuals on their cell phones. After downloading keys, matching is performed between the downloaded keys and the keys stored on the local phones. If a match is found then individuals are asked to take the test or stay in quarantine. From the previous example, a sample of keys uploaded to the server by Keran is shown in Figure 6.



Days	21	22	23	24	25	26	27	28	29	30
Keys	w_{21-10}	x_{22-120}	…	…	…	…	…	…	t_{29-10}	f_{30-60}
	o_{21-50}	o_{22-90}	…	…	…	…	…	…	s_{29-90}	p_{30-60}
	w_{21-90}	b_{22-80}	…	…	…	…	…	…	s_{29-120}	d_{30-109}
	…	…	…	…	…	…	…	…	…	…
	…	…	…	…	…	…	…	…	…	…
	…	…	…	…	…	…	…	…	…	…
	a_{21-10}	x_{22-101}	…	…	…	…	…	…	c_{29-95}	d_{30-89}

Figure 6. Example of diagnostic keys uploaded to the server by an infected individual.

A conceptual overview of matching between downloaded keys and keys already stored on local devices is shown in Figure 7. In this example, Keran met with Pete and Fasi on 30th June, and, therefore, their keys are matched successfully. After a successful match, the individuals are requested to take the test at a nearby center or wait at home for the sample collection. Since most computation is performed on local devices, the chances of privacy breaches are very small.



Days	21	22	23	24	25	26	27	28	29	30
Keys	w_{21-10}	x_{22-120}	…	…	…	…	…	…	t_{29-10}	f_{30-60}
	o_{21-50}	o_{22-90}	…	…	…	…	…	…	s_{29-90}	d_{30-07}
	w_{21-90}	b_{22-80}	…	…	…	…	…	…	s_{29-120}	p_{30-60}
	…	…	…	…	…	…	…	…	…	…
	…	…	…	…	…	…	…	…	…	…
	…	…	…	…	…	…	…	…	…	…
	a_{21-10}	x_{22-101}	…	…	…	…	…	…	c_{29-95}	d_{30-89}

(a) Keys uploaded by an infected individual.

(b) Keys stored on local devices.

Figure 7. Example of checking key matches on local devices.

2.7. Seeking Medical Help from Nearby Hospitals

After successful matches of the keys, relevant people are advised to take a test (or stay in quarantine) at nearby hospitals. In some cases, medical staff collects samples from home to restrict the spread of COVID-19. The process discussed in all seven subsections contributes to controlling the pandemic effectively. Furthermore, contact recording and matching are performed without any directly identifiable information, and, therefore, privacy is ensured, and tracking is minimized. Finally, the Apple–Google platform is OS-assisted software (information about potential exposure and a positive case does not encompass any identifying information) and is purely built on cryptographic concepts [12,13]. Since the Apple–Google platform is privacy-preserved, people feel less hesitation in using compared to traditional contact tracing platforms. A conceptual overview of the main modules of the Apple–Google contact tracing platform is shown in Figure 8. Some of the contents discussed in Section 2 are reformulated (or redrawn) from the previous studies (citations are included where necessary for research integrity) to systematically demonstrate the working of this PPCT platform. Furthermore, we derive a scenario by taking the example of three users to highlight the working of this platform in a more systematic way. To the best of our knowledge, this is the first work that discusses the detailed working of this platform along with a realistic and practical scenario. In the next section, we suggest 15 different enhancements to this platform that can be a valuable addition to this community-beneficial technology.

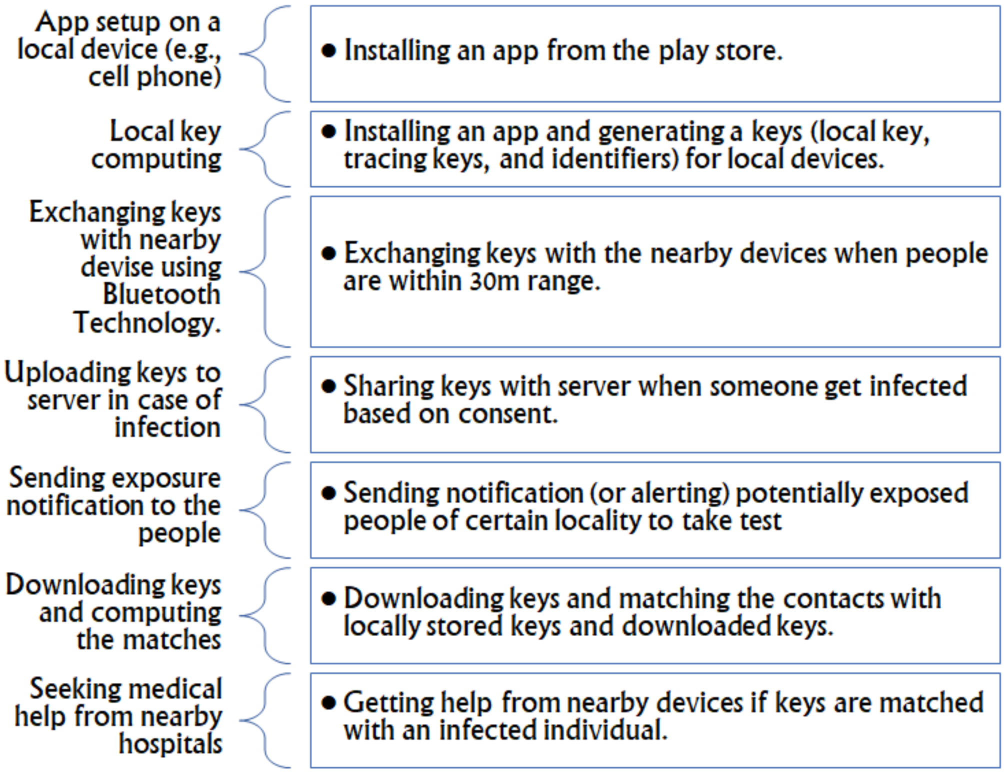
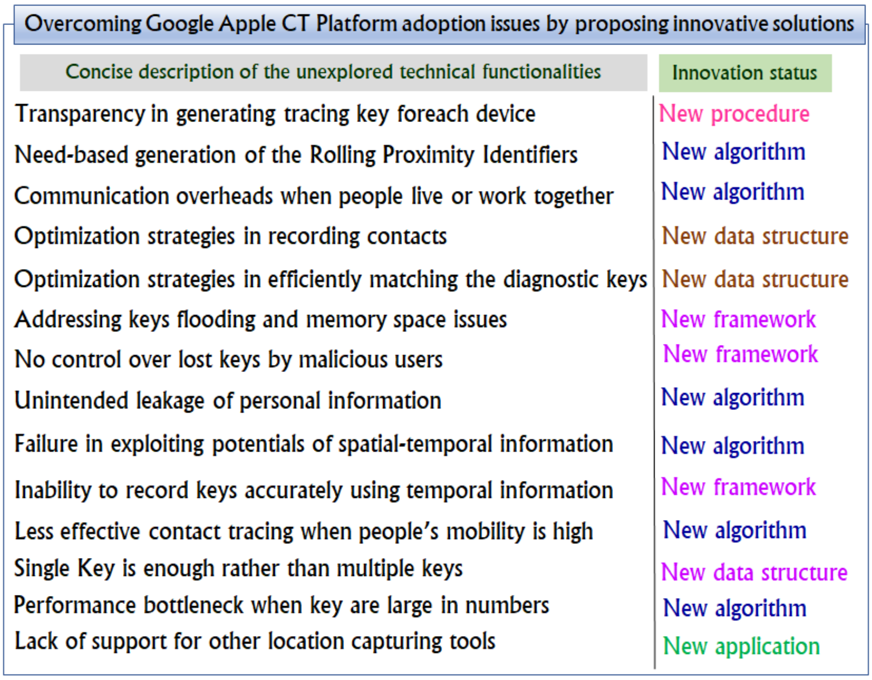

App setup on a local device (e.g., cell phone)
● Installing an app from the play store.
Local key computing
● Installing an app and generating a keys (local key, tracing keys, and identifiers) for local devices.
Exchanging keys with nearby devise using Bluetooth Technology.
● Exchanging keys with the nearby devices when people are within 30m range.
Uploading keys to server in case of infection
● Sharing keys with server when someone get infected based on consent.
Sending exposure notification to the people
● Sending notification (or alerting) potentially exposed people of certain locality to take test
Downloading keys and computing the matches
● Downloading keys and matching the contacts with locally stored keys and downloaded keys.
Seeking medical help from nearby hospitals
● Getting help from nearby devices if keys are matched with an infected individual.

Figure 8. Conceptual overview of main modules of the Apple–Google contact tracing platform.

3. Unexplored Additional Functionalities in the Apple–Google Contact Tracing Platform

The generic idea of the Apple–Google contact tracing platform for alerting people in case of close contact with an infected individual is simple, transparent, elegant, and, therefore, likely to be welcomed by most users.

However, we identify certain additional functionalities that remained unexplored in the design of the Apple–Google Contact Tracing platform and can be vital to enhance the robustness and privacy of platforms. We concisely present various unexplored additional functionalities in the Apple–Google Contact Tracing platform as follows. Figure 9 presents the contributions and novelty of this work in terms of new algorithms, data structures, framework, and application. For example, a new procedure that is more transparent can be used to enhance the transparency in generating the tracing key. Similarly, a new algorithm can be embedded into the existing CT platform that generates keys when needed rather than generating keys sequentially (e.g., 143 keys a day). A new algorithm or interface can be developed to mark the relative or acquittance as permanent contact to lower the communication overheads. The paper provides research contributions and novelty in terms of these new algorithms, data structures, frameworks, and applications for realizing these unexplored additional functionalities. By incorporating these new functions, the performance of the CT platforms can be enhanced two/three-fold.



Overcoming Google Apple CT Platform adoption issues by proposing innovative solutions

Concise description of the unexplored technical functionalities	Innovation status
Transparency in generating tracing key foreach device	New procedure
Need-based generation of the Rolling Proximity Identifiers	New algorithm
Communication overheads when people live or work together	New algorithm
Optimization strategies in recording contacts	New data structure
Optimization strategies in efficiently matching the diagnostic keys	New data structure
Addressing keys flooding and memory space issues	New framework
No control over lost keys by malicious users	New framework
Unintended leakage of personal information	New algorithm
Failure in exploiting potentials of spatial-temporal information	New algorithm
Inability to record keys accurately using temporal information	New framework
Less effective contact tracing when people's mobility is high	New algorithm
Single Key is enough rather than multiple keys	New data structure
Performance bottleneck when key are large in numbers	New algorithm
Lack of support for other location capturing tools	New application

Figure 9. Overview of new functionalities in the form of data structure, algorithm, and applications in the Apple Google CT platform.

3.1. Lack of Transparency in Generation of the Tracing Key

Upon installation of the Apple–Google contact tracing platform, a key is generated for each device. However, it is unclear which kind of information (e.g., cell phone numbers, IMEI numbers, or other information) is used in generating the tracing key. For example, if the cell phone is acquired at the time of key generation, it can lead to tracking and other kinds of disclosures. For example, in South Korea, almost all kinds of private data can be derived with the help of cell phone numbers. Therefore, further information/explanation regarding the transparency of generating the tracing key is required. In addition, most processing is performed in a black-box manner, and, therefore, transparency should be incorporated in the design of the tracing key mechanism.

3.2. Unnecessary Generation of the Rolling Proximity Identifiers

The Apple–Google contact tracing platform usually generates rpi every 10 min, even when no nearby devices are found. Therefore, it can be problematic in resource-constrained cell phones. To avoid unnecessary computations of the rpi, an intelligent mechanism is needed to generate need-based rpi (e.g., when a phone is detected nearby).

3.3. Extensive Communication Overheads When People Live or Work Together

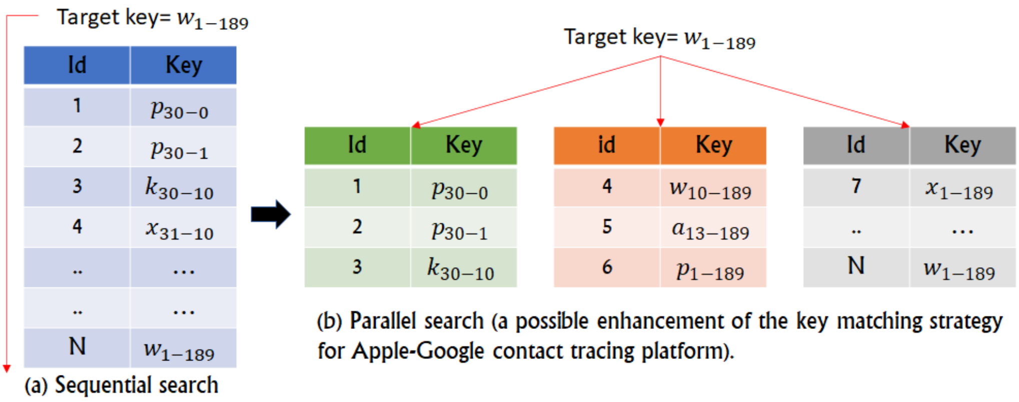
The Apple–Google contact tracing platform establishes and records the contacts when two phones are close to each other. However, in real-world cases, two phones can be close to each other for a long time in most cases due to living/working together. In this scenario, most keys can be exchanged which can introduce extensive communication overheads. In addition, it can slow the process of matching keys when a large number of keys exist in the local store.

3.4. Lack of Optimization Strategies in Recording Contacts (e.g., Exchanging Keys)

The Apple–Google contact tracing platform exchanges keys with nearby devices when both cell phones are close to each other. However, the possibility of infection is low when people cross the path with each other from the same direction or a distance of more than 2 m. Therefore, intelligent strategies are needed in the Apple–Google contact tracing platform to precisely determine the distance to exchange the key. Determining precisely when to exchange the key can contribute to saving computing power at the time of key matching. In addition, it can contribute to saving memory storage because the storage capacity of most cell phones is not large.

3.5. Lack of Optimization Strategies in Efficiently Matching the Diagnostic Keys

In the Apple–Google contact tracing platform, the keys are matched sequentially. In most cases, the key space is significantly large and the correct matches can be found in later indexes. Due to the latency issues, the identification of potentially infected people can be slow and thereby virus can spread at a rapid pace. To avoid latency issues, optimization strategies are needed to find the correct matches efficiently. A conceptual overview of the improvements in the key matching concept is shown in Figure 10. By using parallel search, desired keys can be matched quickly, and the suggested process is reliable when the size of the key space is large.



Target key= w_{1-189}

Id	Key
1	p_{30-0}
2	p_{30-1}
3	k_{30-10}
4	x_{31-10}
..	…
..	…
N	w_{1-189}

(a) Sequential search

Target key= w_{1-189}

Id	Key
1	p_{30-0}
2	p_{30-1}
3	k_{30-10}

id	Key
4	w_{10-189}
5	a_{13-189}
6	p_{1-189}

Id	Key
7	x_{1-189}
..	…
N	w_{1-189}

(b) Parallel search (a possible enhancement of the key matching strategy for Apple-Google contact tracing platform).

Figure 10. A conceptual overview of enhancement in the key matching method of Apple–Google contact tracing platform: (**a**) checking the possibility of target key match with stored keys in a sequential form (e.g., one by one), (**b**) checking the possibility of target key match with stored keys in a parallel form (e.g., more than one at a time).

3.6. Keys Flooding and Memory Space Issues

In the Apple–Google contact tracing platform, most processing (key generation, distribution, matching) is performed at the end devices (e.g., cell phones). In some scenarios (let us say a gathering of thousands of people), a large number of keys can be exchanged, and memory space issues can occur in cell phones. Furthermore, there is a mechanism in the Apple–Google contact tracing platform to alert users when there is no space on mobile for storing contact keys. Due to these issues, important contacts can be missed, and virus containment can become tricky. In such circumstances, the deletion of outdated keys can assist to overcome memory space issues.

3.7. No Control over Lost Keys by Malicious Users

In the Apple–Google contact tracing platform, most processing is dedicated to the client devices (i.e., users of smartphones), and users can opt-out at any time from the tracing process. In this way, infected users can leave the tracing mechanism, and/or can delete the diagnostic keys stored on their cell phones. In such circumstances, the Apple–Google contact tracing platform has no control over recovering keys as well as identifying the infected users and their close contacts. To avoid such issues, partial information needs to be maintained in the platform for constraining the spread of COVID-19.

3.8. Unintended Leakage of Personal Information

In the Apple–Google contact tracing platform, no direct information is collected, and, therefore, privacy issues are small. However, there are some scenarios in which disclosure can occur. For example, if Alice and Bob met in a park and returned home without meeting anyone else. The next day, if Bob is diagnosed with COVID-19, Alice receives an exposure notification. Without any doubt, she can guess that Bob likely has been infected with COVID-19. Furthermore, in some cases, spatial information can also be disclosed. Hence, the Apple–Google contact tracing platform cannot guarantee privacy in most cases.

3.9. Failure in Handling All Possible Exposure by Not Considering Spatial-Temporal Information

In the Apple–Google contact tracing platform, keys are exchanged when two mobiles are very close to each other. However, the virus can spread even when two people do not make any contact. For example, person X used an elevator, and later person Y used the same elevator. In this case, if X is infected with COVID-19, the Apple–Google contact tracing platform cannot identify Y as the likely infected individuals because there are no keys in X and Y's cell phones about each other. Hence, the Apple–Google contact tracing platform cannot block all routes of infection (or virus spread).

3.10. Inability to Record Keys Accurately by Not Considering Temporal Information

In the Apple–Google contact tracing platform, random identifiers are exchanged between mobiles based on closeness regardless of people's mask status (or whether they had physical contact or not). By ignoring the precise information at the time of recording contact, the key space can be large and many unnecessary keys can be stored in each other devices which can lead to latency issues at the time of matching keys. Similarly, keys are recorded every time even when two same mobiles come into close contact after some time (e.g., five minutes later) at the same location/facility. To avoid many useless key storage issues, utilization of temporal information may assist in recording only minimal necessary keys for tracing purposes. Lastly, empowering users to record contacts/keys at some specific venues and/or times can also contribute to lowering key space thereby reducing latency issues at the time of matching keys.

3.11. Less Effective Contact Tracing When People's Mobility Is High

In the Apple–Google contact tracing platform, exposure notifications are sent to a relatively small area based on the information of infected individuals. However, in some cases, people's mobility can be high (i.e., business meetings at various places throughout a week), and exposure notification cannot be delivered to all potentially exposed people due to higher mobility (or differences in the locality). In such circumstances, virus spread cannot be constrained effectively, and it can spread to other regions through hidden routes. Hence, effective methods are needed to intelligently maintain the keys and use them in time of need.

3.12. Single Key Is Enough Rather Than Multiple Keys

The Apple–Google contact tracing platform cannot distinguish between two same people meeting for a long time, or multiple people meeting for short time in a subway station or on a bus. In the former, case one key is enough for tracing the possibility of infection subsequently. However, in the Apple–Google contact tracing platform keys are exchanged every time which can lead to excessive computation, communication, and processing overheads. In such circumstances, if the cell phone's location is not changed for a reasonable period, only a recent key can be stored rather than multiple keys for the whole duration of the meeting. By doing so, computing overheads can be controlled and contacts of an infected person can be traced quickly.

3.13. A Performance Bottleneck When Keys Are Large in Numbers (e.g., A Socially Active Person Scenario)

In the Apple–Google contact tracing platform, the number of keys for a socially active person can be very large in numbers. The infection of such a person can raise a performance bottleneck for other clients (e.g., cell phones) as the number of keys to be matched can be very large in number. To avoid performance bottlenecks, the Apple–Google contact tracing platform can provide computational offloading facilities for the users to match keys efficiently and overcome performance bottlenecks. Furthermore, parallel searching of keys and divide and conquer concepts can further ease the performance issues in matching keys in such circumstances.

3.14. Lack of Support for Other Location Capturing Tools to Seamlessly Provide Accurate Positioning Information

In the Apple–Google contact tracing platform, contacts are established based on Bluetooth connections (∼30 m range). However, in some cases, global navigation satellite systems (GNSS), cellular towers, and Wi-Fi data, which are mostly self-supplied by the user are inevitable for localization analysis [14]. Apart from other alternatives, GNSS has the potential to provide accurate positioning information, that, in return, can be used in multiple ways in the context of this ongoing pandemic, such as tracing and tracking close contacts, mapping and tagging, resource planning, and delivery of medical and emergency materials (https://gnss.asia/blog/gnss-joins-the-fight-against-the-global-pandemic/) (accessed on 2 October 2022). The utilization of Galileo signal fetched or to harness even the potential of GNSS depending on the phone type in use can assist in making the vulnerability maps which can be used to alert people to stay away from the contaminated places [15]. An overview of the Galileo signal frequencies is shown in Figure 11. Many commercial services have been developed based on Galileo signal and GPS systems for location tracking and positioning.

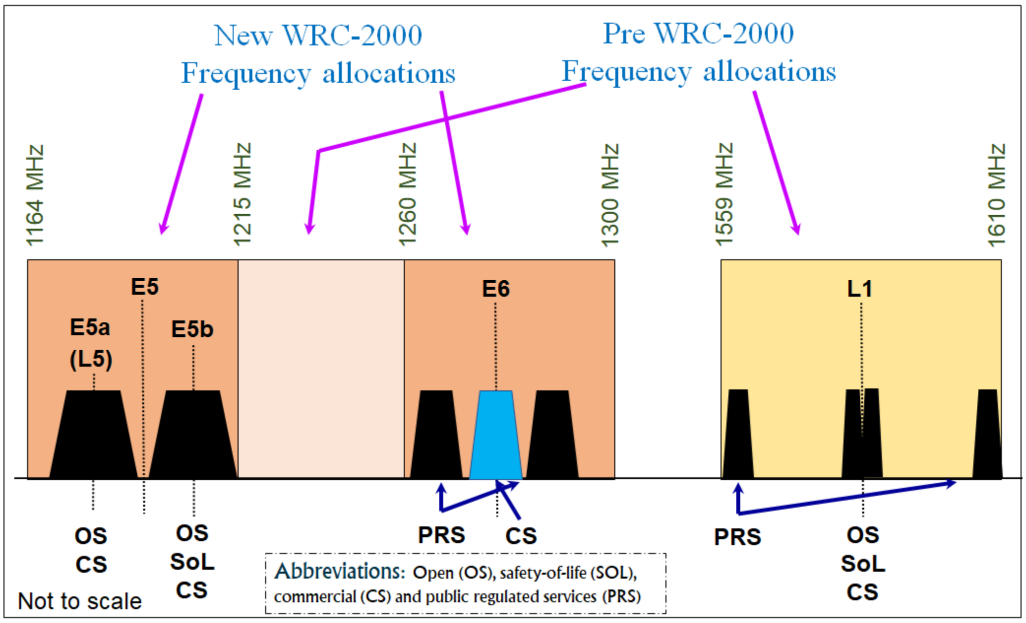


Figure 11. Overview of the Galileo signal frequencies used in commercial GNSS-based services.

GNSS data have been widely used in tracing the contacts of infected people [16]. GNSS-based systems consist of multiple satellites which provide signals from space by transmitting positioning and timing information to the receivers. The receivers then use these data to define their locations via the time signals obtained along a line of sight by the radio from satellites. Hence, it is vital to incorporate heterogeneous sources of data to extend the applicability of the framework to old phones, as well as to capture the hidden routes of COVID-19 transmission (e.g., visit the contaminated places) [17]. Furthermore, GNSS-based contact tracing platforms are most suitable for outdoor environments, and GNSS can enhance the localization performance in contact tracing applications [18,19]. To preserve location privacy, advanced technologies, such as blockchain, can be used [20]. Depending upon the system design, more sources can be integrated to seamlessly capture location information, and enhance the adoption of the system by the general public.

3.15. Lack of Compression Techniques to Seamlessly Reduce Computing Overheads

As mentioned in the previous sections, PPCT developed by Apple and Google generates and stores a substantially large number of keys, and some of them may not be needed in identifying the contacts of an exposed person. The storage and processing of such a substantial number of keys bring many overheads, especially in terms of memory. To overcome such issues, compression techniques can be integrated with the PPCT to reduce the storage consumption in the platform [21,22]. Apart from employing compression techniques, parallel architectures can be employed rather than serial architectures to match the keys of infected individuals to find the potentially exposed contacts [23]. The integration of compression techniques and parallel architectures can reduce the computing overheads, and can enhance the scalability of this platform.

Apart from the key issues cited above, in some cases, exchanging keys can be meaningless. For example, people living close to each other (e.g., separated by walls) or working at the same place, etc. Therefore, intelligent strategies are needed to decide when to record a contact, and to optimize the key searching process. Finally, generating keys only when needed and deleting them based on intervals (e.g., 14 days) can assist in overcoming storage issues that remained unexplored in the design of the Apple–Google contact tracing platform. Further information regarding the exemption of the same household from the social distancing rules can be obtained from prior studies [24]. Furthermore, incorporating strategies to overcome the energy issues in Bluetooth-based contact tracing platforms needs further exploration from the research community [25]. Lastly, devising an optimized strategy to record contacts based on social distance violations ($\leq$2 m) rather than the range of Bluetooth (20/30 m) needs further exploration. Although the Apple–Google contact tracing platform is a major advance, the above extensions are believed to enhance the technicality of the system that can help to better fight infectious diseases.

4. Integration of AI-Powered and Privacy-Preserved Techniques with the Apple–Google Contact Tracing Platform: New Synergies and Applications

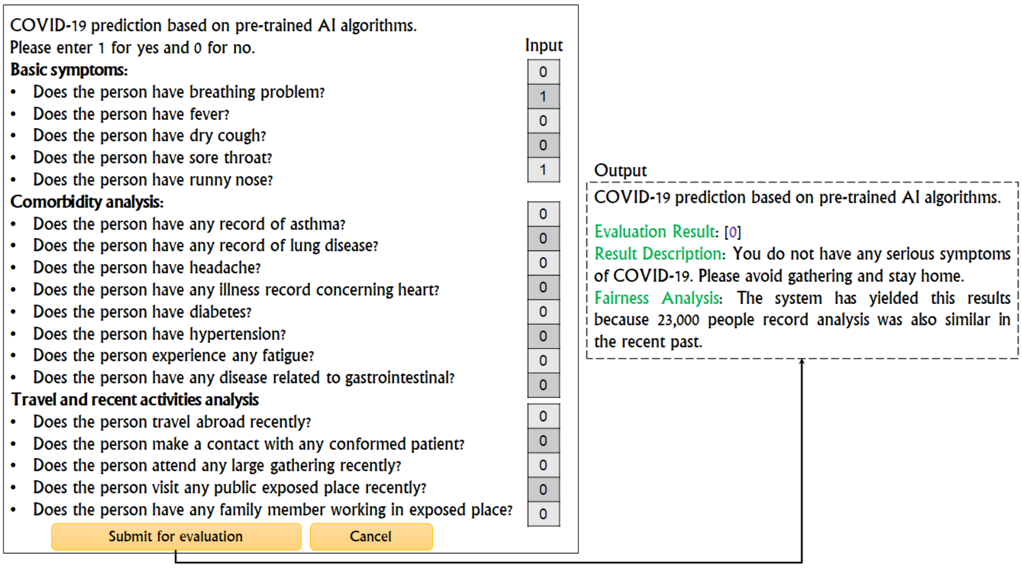
Since the platform proposed by Apple and Google does not use spatial and temporal information in the contact tracing process, many hidden routes of infection can be left out. Furthermore, in most cases, the virus can spread without physical contact via contaminated surfaces, and, therefore, new synergies are imperative in enhancing the application horizon of the Apple and Google platform. In line with these needs, we suggest two AI-powered and privacy-preserved services that can valuable addition to the contact tracing platform.

4.1. Self-Checking the Possibility of COVID-19 Infection Using AI Techniques

Recently, pre-trained AI models have been widely used in the medical domain for multiple purposes, such as the identification and detection of diseases [26,27]. These systems take images/voice data as input and determine the desired output by analyzing the data with already analyzed data. To this end, we suggest the addition of self-checking the possibility of COVID-19 infection service using a pre-trained AI model in the Apple–Google contact tracing platform. This service is based on AI algorithms and non-private data, and these kinds of services have already shown great promise in recent times [28]. The IPO (input, processing, and output) of the services is given below.

- Input: symptoms data, activities data, travel records, and underlying disease(s) data.
- Processing: ML/DL models, such as SVM, regression, KNN, RF, CNN, RNN, etc.
- Output: Possibility of infection, recommendation, and /or health tips.

Recently, the demand for explainable AI in healthcare applications is becoming a defacto standard [29,30]. Hence, some justification or analysis of results can also be provided along with the output. In Figure 12, we demonstrate an overview of such a service that can be beneficial to the community for checking any possibility of infection proactively. In this service, 0 means that no possibility of infection. In contrast, 1 indicates the possibility of infection. In this service, most of the data are non-private, and, therefore, privacy is significantly preserved. In this service, if values for most critical questions, such as 1, 2, 3, 5, 10, 11, 12, 16, and 17, are 1, the results can be 1 (100%). The integration of such services can enhance the persuasiveness of the platform which, in return, can be helpful to constrain the spread of the virus.



COVID-19 prediction based on pre-trained AI algorithms.
Please enter 1 for yes and 0 for no.

	Input
Basic symptoms:	
• Does the person have breathing problem?	0
• Does the person have fever?	1
• Does the person have dry cough?	0
• Does the person have sore throat?	0
• Does the person have runny nose?	1
Comorbidity analysis:	
• Does the person have any record of asthma?	0
• Does the person have any record of lung disease?	0
• Does the person have headache?	0
• Does the person have any illness record concerning heart?	0
• Does the person have diabetes?	0
• Does the person have hypertension?	0
• Does the person experience any fatigue?	0
• Does the person have any disease related to gastrointestinal?	0
Travel and recent activities analysis	
• Does the person travel abroad recently?	0
• Does the person make a contact with any conformed patient?	0
• Does the person attend any large gathering recently?	0
• Does the person visit any public exposed place recently?	0
• Does the person have any family member working in exposed place?	0

Output

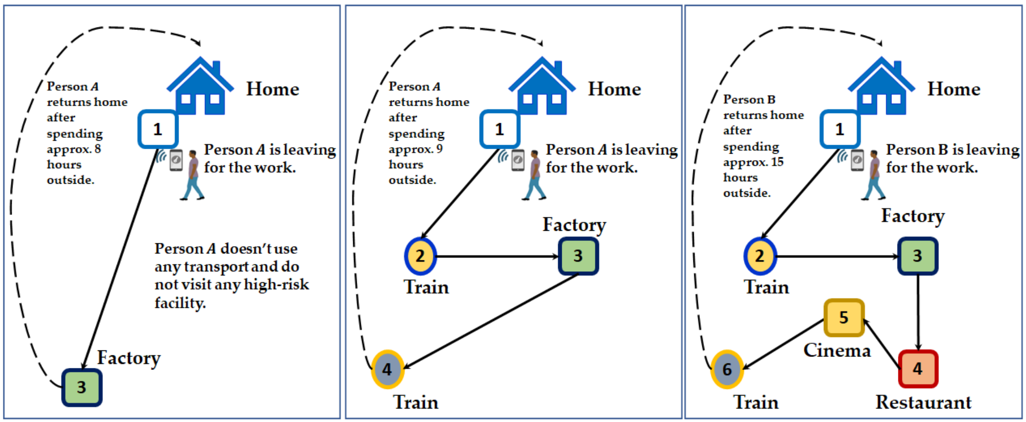
COVID-19 prediction based on pre-trained AI algorithms.

Evaluation Result: [0]
Result Description: You do not have any serious symptoms of COVID-19. Please avoid gathering and stay home.
Fairness Analysis: The system has yielded this results because 23,000 people record analysis was also similar in the recent past.

Figure 12. Overview of service that can be used to self-check the possibility of COVID-19 infection.

4.2. Estimating the Vulnerability/Risk to COVID-19 Infection Using Mobility Information

Since the vulnerability/risk of being infected with COVID-19 highly depends on mobility, and, therefore, we suggest a vulnerability/risk estimation service to be integrated with the Apple–Google contact tracing platform. Many risk estimation methods have been developed in the literature for accomplishing multiple tasks concerning COVID-19 [31,32]. Researchers at JOHNS HOPKINS University developed a multi-criteria-based method for separating vulnerable groups (https://www.ahealthierworld.jhu.edu/tracking-vulnerable-populations-covid) (accessed on 15 August 2022). Similarly, in our proposed service, a risk/vulnerability score can be estimated based on the location/facilities a person visits, and many other factors such as the size of the facility, time a person spent at some facility, etc. Concisely, if a person just goes to work and comes back daily, then his/her infection risk is lower compared to the person who visits multiple locations each day (e.g., delivery services). In Figure 13, we demonstrate low-, medium-, and high-risk scenarios based on the mobility information.


Person *A* returns home after spending approx. 8 hours outside.
Home
1
Person *A* is leaving for the work.
Person *A* doesn't use any transport and do not visit any high-risk facility.
Factory
3
Person *A* returns home after spending approx. 9 hours outside.
Home
1
Person *A* is leaving for the work.
Factory
2
Train
3
4
Train
Person B returns home after spending approx. 15 hours outside.
Home
1
Person B is leaving for the work.
Factory
2
Train
3
5
Cinema
6
4
Train
Restaurant

(a) Less vulnerability/risk scenario. (a) Medium vulnerability/risk scenario. (c) High vulnerability/risk scenario.

Figure 13. Overview of three vulnerability/risk scenarios based on mobility information.

Based on the three scenarios shown in Figure 13, we suggest a vulnerability/risk estimation function that considers multiple factors, such as the number of facilities a person visits per day, the number of contacts a person makes daily, masks status, transport use status (e.g., public/personal), spatial-temporal activities, demographics, etc. By computing the vulnerability/risk score, recommendations can be made to relevant people for limiting daily activities that otherwise can lead to infection. Furthermore, super spreaders can be identified in this way. Computing vulnerability/risk value using a trace of facilities a person visits on a cell phone enables people to take preventive measures. Furthermore, determining vulnerability/risk value by considering multiple factors can help identify the focus group for frequent tests. Furthermore, we suggest storing facility visits' information and other activities on a local device to alleviate privacy concerns.

4.3. Generating Vulnerability Map of Facilities by Utilizing and Tagging Ge–QR Codes

In the proposed implementation of the Apple–Google contact tracing platform, Bluetooth data are mainly used, and, therefore, there is no mechanism to recommend a group of people to undergo a COVID-19 test based on facilities visited by them. By not generating a vulnerability map based on the facilities' information, the virus can quickly and discretely spread across the regions. To cover this gap, we suggest constructing a map of the facilities and store locally using other location tools such as GNSS data. Since Galileo signals are privacy-preserved, and, therefore, they can be integrated with the platform. Some web applications like Corona Map (see Figure 14) in South Korea are being employed for tagging the contaminated/dangerous areas and hotspots of COVID-19.

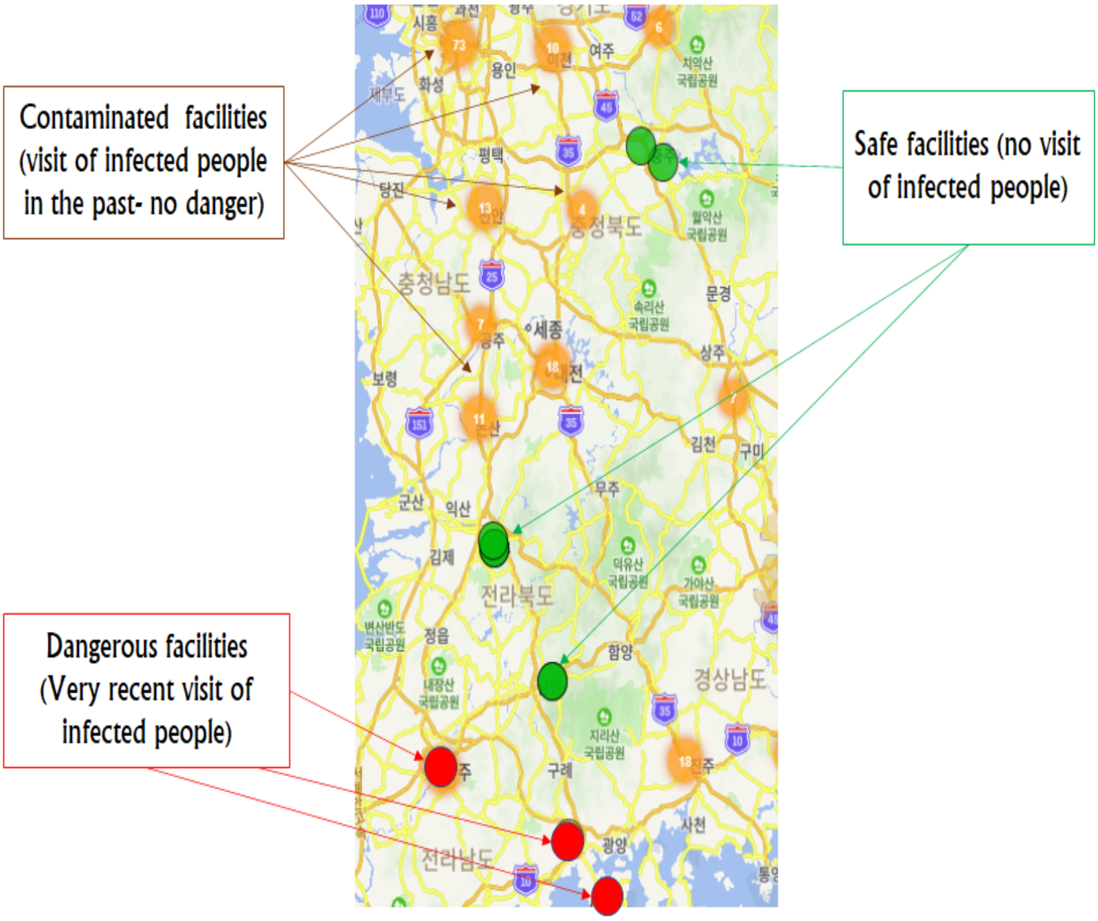

Contaminated facilities (visit of infected people in the past- no danger)
Safe facilities (no visit of infected people)
Dangerous facilities (Very recent visit of infected people)
시흥
용인
여주
화성
평택
당진
충청북도
충청남도
세종
보령
문경
상주
김천
구미
군산
익산
김제
전라북도
정읍
함양
경상남도
구례
광양
사천
전라남도

Figure 14. Overview of the safe and risky facilities based on patients' temporal visit information.

In simple words, a map marks facilities that were recently visited by confirmed COVID-19 patients. Different color codes are used to show the vulnerability level in terms of how long ago those visits took place. Due to this precise information, people can avoid riskier areas. These applications provide a much better understanding/awareness of which areas are risky and relatively safe, respectively. By integrating such services, riskier locations can be better avoided to contain the spread of the virus. Furthermore, a vulnerability map can be generated to provide fine-level details of risky facilities.

The integration of the above-mentioned services in the platform can enhance its functionalities, which, in return, can help constrain the virus. Lastly, some of the previous studies have suggested that the contact tracing platform proposed by Apple and Google can be subject to function creep [33]. Hence, the technical analysis of the main functionalities of the platform is imperative. The technical analysis presented in this paper can contribute to responsible data science (https://redasci.org/) (accessed on 25 August 2022). Furthermore, the complete/partial implementation of the suggested contents can enhance the popularity of the platform and can lead to the development of community-beneficial technologies.

5. Proof of Concept Experiments and Comparisons

In this section, we compare the performance of the PPCT proposed by Apple and Google, and the modified PPCT (M-PPCT) proposed in this study based on proof of concept experiments. Specifically, we compare the performance of both platforms in terms of number of keys, computing time, storage complexity, etc. We examined the platform and identified various issues concerning its performance of the platform. The PPCT platform generates keys based on the windowing concept which may increase the storage consumption in resource-constrained cell phones. In Figure 15, we present the performance comparison between PPCT (Apple Google) and M-PPCT (Ours) from the perspective of number of keys and corresponding storage consumption. From the results, it can be seen that the M-PPCT has a lower number of keys than PPCT, which can significantly reduce storage consumption. In M-PPCT, we suggest key generation only when two mobiles are close for a reasonable amount of time rather than time windowing. These concepts can contribute to reducing the overheads of PPCT developed by Apple and Google.

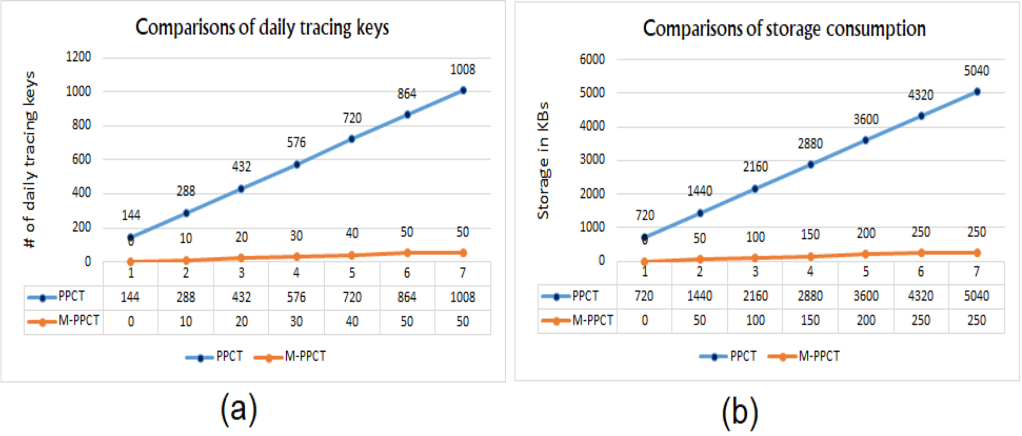


Figure 15. PPCT versus M-PPCT: comparisons of number of keys (**a**) and storage consumption (**b**).

In the next experiments, we compare the performance of PPCT and M-PPCT in terms of number of contacts and corresponding computing time for matching keys. In M-PPCT, contacts are recorded when two users are relatively close and spend a reasonable time together. In contrast, PPCT records the contacts based on Bluetooth range, and, thereby, many contacts are not risky in terms of infection (or possibly of spreading infection). In Figure 16, we present the performance comparison between PPCT (Apple Google) and M-PPCT (Ours) from the perspective of number of contacts and corresponding computing time. From the results, it can be seen that the M-PPCT has a lower number of contacts than PPCT, which can significantly reduce computing time in matching diagnostic keys. In M-PPCT, we suggest key exchange only when two mobiles are very close for a reasonable amount of time rather than within Bluetooth range (∼30 m). These concepts can contribute to significantly reducing the overheads of PPCT developed by Apple and Google, and slowing the spread of COVID-19.

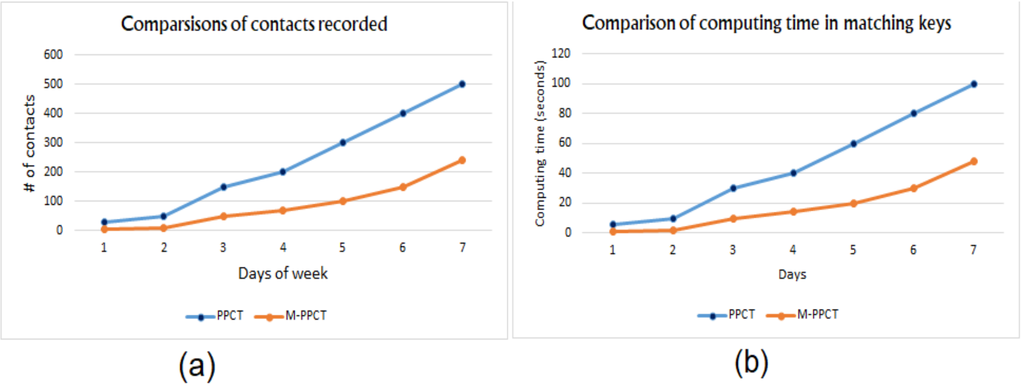


Figure 16. PPCT versus M-PPCT: comparisons of number of contacts (**a**) and computing speed (**b**).

Apart from the comparisons given above, PPCT cannot distinguish between the zero mobility cases (a person has installed the app, but stays at home), working together (meeting same persons frequently), living together (husband and wife), traveling together, and driving together. In these cases, there is a possibility of recording repetitive contexts of the same person which can lead to extensive performance bottlenecks. To further enhance the technical significance of the proposed work, we provide an in-depth analysis of proposed functionalities for PPCT and corresponding technical significance in Table 2.

Table 2. In-depth analysis of proposed functionalities for the PPCT.

Sr. Number	Proposed Functionality	Technical Significance
1.	Transparency of key generation	Preventing tracking of individuals
2.	Need-based production of *rpi*	Reduction in memory consumption
3.	Filter unneeded keys/contacts	Reduction in computing overheads
4.	Optimization strategies in storing keys	Storage of necessary contacts
5.	Parallel search for keys matching	Reduction in latency
6.	Outdated keys' deletion	Reduction in memory consumption
7.	Partial keys storage	Controlling hidden routes of transmission
8.	Seamless contact utilization	Effective privacy preservation
9.	Spatial-temporal information use	Blocking hidden routes of virus spread
10.	Use of timing information	Identifying the contaminated facilities
11.	Key management and control	Restricting virus transmission/spread
12.	Spatial and temporal information use	Significantly reduced keyspace
13.	Efficient key matching	Offloading and parallel searching techniques
14.	GNNS functionalities	Precise capture of localization information
15.	Compression techniques	Reduction in memory storage (or size)

As shown in Table 2, the suggested functionalities can reduce various performance bottlenecks in PPCT, and can augment the robustness and scalability of this platform. Furthermore, the technical suggestions can improve the performance of PPCT in constraining the spread of COVID-19. In Table 2, we present the efficient solutions for various bottlenecks of the PPCT. To the best of our knowledge, these functionalities and their likely impact on the performance of the PPCT platform remained unexplored in the recent literature. The suggested analysis can enhance the service scenario (s) of PPCT and can improve the service standard of PPCT.

6. Conclusions and Future Work

In this concise paper, we have explained the working of the contact tracing platform proposed by Apple and Google for constraining the spread of COVID-19. Specifically, we have provided a technical analysis (i.e., systematic details of how the platform works) of the platform and discussed unexplored additional functionalities that can be vital to further enhance the capabilities of the platform in terms of robustness and privacy. Furthermore, we have suggested some additional services that can be valuable addition to the platform. The enclosed finding can improve the technical level of the platform, which, in return, can be used to fight future infectious diseases effectively. Due to the urgency of the situation, most digital tools developed in the pandemic arena have overlooked the important designs (or legal measures) that have led to poor adoption of most systems in real-life scenarios. The rectification of most apps and the data life cycle used in them is essential in the "new normal". To this end, this study examined the Apple–Google contact tracing platform developed to find the contacts of infected people to highlight its failures in handling the diverse privacy, as well as computing challenges stemming from the COVID-19 era. Any prototype/system developed based on the concepts proposed in this technical note will be released as open source for the well-being of the general public and community feedback. In the future, it is imperative to integrate the latest technologies, such as AI, blockchain, and high-performance computing (HPC) applications with epidemic handling platforms that, in return, can be beneficial to fighting infectious diseases in a privacy-preserved way. Further, we intend to devise a proof of concept framework that can be used for accomplishing multiple goals in the context of an epidemic/pandemic, unlike the Apple–Google contact tracing platform that only assists in contact tracing. Furthermore, we intend to devise a comprehensive platform to check quarantine violations, ranking the most influential individuals based on mobility, spread prediction, forecasting trends, vulnerability estimation and map generation, super spreader identification, vaccine status, etc. Lastly, we intend to explore the promising applications of federated learning in the context of COVID-19. Finally, developing simulation/development tools to assess the performance (in terms of computing resources versus virus containment) of the PPCT in realistic scenarios is an exciting area for future research.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data and studies that were used to support the findings of this technical note are included within this article.

Acknowledgments: The authors would like to thank the editor and reviewers for their insightful comments and valuable suggestions, which helped improve the quality of the paper significantly. The authors would like to thank the researchers and tech giants for their efforts in proposing/developing community-beneficial technologies to address the global COVID-19 crisis.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Akat, M.; Karataş, K. Psychological effects of COVID-19 pandemic on society and its reflections on education. *Electron. Turk. Stud.* **2020**, *15*, 4.
2. Cao, Y.; Li, Q.; Chen, J.; Guo, X.; Miao, C.; Yang, H.; Chen, Z.; Li, C.; Li, L. Hospital emergency management plan during the COVID-19 epidemic. *Acad. Emerg. Med.* **2020**, *27*, 309–311. [CrossRef] [PubMed]
3. Mbunge, E. Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls. *Diabetes Metab. Syndr. Clin. Res. Rev.* **2020**, *14*, 1631–1636. [CrossRef] [PubMed]
4. Wang, Y.; Ngien, A.; Ahmed, S. Nationwide Adoption of a Digital Contact Tracing App: Examining the Role of Privacy Concern, Political Trust, and Technology Literacy. *Commun. Stud.* **2022**, *73*, 364–379. [CrossRef]
5. Longbing, C. AI in Combating the COVID-19 Pandemic. *IEEE Intell. Syst.* **2022**, *37*, 3–13.
6. Hassandoust, F.; Akhlaghpour, S.; Johnston, A.C. Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. *J. Am. Med. Inform. Assoc.* **2021**, *28*, 463–471. [CrossRef]
7. Michael, K.; Abbas, R. Behind COVID-19 contact trace apps: The Google–Apple partnership. *IEEE Consum. Electron. Mag.* **2020**, *9*, 71–76. [CrossRef]
8. Majeed, A. Effective Handling of COVID-19 Pandemic: Experiences and Lessons from the Perspective of South Korea. *COVID 1* **2021**, *1*, 325–334. [CrossRef]
9. Park, S.; Choi, G.J.; Ko, H. Privacy in the time of COVID-19: Divergent paths for contact tracing and route-disclosure mechanisms in South Korea. *IEEE Secur. Priv.* **2021**, *19*, 51–56. [CrossRef]
10. Kouliaridis, V.; Kambourakis, G.; Chatzoglou, E.; Geneiatakis, D.; Wang, H. Dissecting contact tracing apps in the Android platform. *PLoS ONE* **2021**, *16*, e0251867.

11. Saito, K.; Iwamura, M. Privacy-Preserving Infection Exposure Notification without Trust in Third Parties. *arXiv* **2021**, arXiv:2103.07669
12. Veale, M. Privacy is not the problem with the Apple-Google contact-tracing toolkit. *The Guardian*, 1 July 2020; pp. 1–3.
13. Ilves, I. Digital contact tracing: Privacy versus efficiency. *Cyber Secur. Peer-Rev. J.* **2021**, *5*, 102–112.
14. Xu, H.; Zhang, L.; Onireti, O.; Fang, Y.; Buchanan, W.J.; Imran, M.A. BeepTrace: Blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond. *IEEE Internet Things J.* **2020**, *8*, 3915–3929. [CrossRef]
15. Bošković, A.; Bijelić, S.; Sudžum, J.; Stojanović, R. *COVID-19 Related System for Real-Time Patients Monitoring and Tracking Technical Report*; University of Montenegro: Podgorica, Montenegro, 2022.
16. Shubina, V.; Holcer, S.; Gould, M.; Lohan, E.S. Survey of decentralized solutions with mobile devices for user location tracking, proximity detection, and contact tracing in the COVID-19 era. *Data* **2020**, *5*, 87. [CrossRef]
17. Grekousis, G.; Liu, Y. Digital contact tracing, community uptake, and proximity awareness technology to fight COVID-19: A systematic review. *Sustain. Cities Soc.* **2021**, *71*, 102995. [CrossRef]
18. Giustiniano, D.; Bianchi, G.; Conti, A.; Bartoletti, S.; Melazzi, N.B. 5G and beyond for contact tracing. *IEEE Commun. Mag.* **2021**, *59*, 36–41. [CrossRef]
19. Ojagh, S.; Saeedi, S.; Liang, S.H.L. A person-to-person and person-to-place COVID-19 contact tracing system based on OGC IndoorGML. *Int. J. Geo-Inf.* **2020**, *10*, 2. [CrossRef]
20. Wen, Z.; Yu, K.; Qi, X.; Sato, T.; Katsuyama, Y.; Sato, T.; Kameyama, W.; Kato, F.; Cao, Y.; Hashimoto, J.; et al. Blockchain-empowered contact tracing for COVID-19 using crypto-spatiotemporal information. In Proceedings of the 2020 IEEE International Conference on E-Health Networking, Application & Services (HEALTHCOM), Shenzhen, China, 1–2 March 2021.
21. Yi; Jirong; Mudumbai, R.; Xu, W. Low-cost and high-throughput testing of COVID-19 viruses and antibodies via compressed sensing: System concepts and computational experiments. *arXiv* **2020**, arXiv:2004.05759
22. Zhu, Z.; Xingming, Z.; Tao, G.; Dan, T.; Li, J.; Chen, X.; Li, Y.; Zhou, Z.; Zhang, X.; Zhou, J.; et al. Classification of COVID-19 by compressed chest CT image through deep learning on a large patients cohort. *Interdiscip. Sci. Comput. Life Sci.* **2021**, *13*, 73–82. [CrossRef]
23. Kaplan, M.; Kneifel, C.; Orlikowski, V.; Dorff, J.; Newton, M.; Howard, A.; Shinn, D.; Bishawi, M.; Randles, A.; Chidyagwai, S.; et al. Cloud computing for COVID-19: Lessons learned from massively parallel models of ventilator splitting. *Comput. Sci. Eng.* **2020**, *22*, 37–47. [CrossRef]
24. Bobowski; Adam; Cichoń, J.; Kutyłowski, M. Extensions for Apple-Google exposure notification mechanism. *Bull. Pol. Acad. Sci. Tech. Sci.* **2021**, *69*, e137126.
25. Sharon, T. Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics Inf. Technol.* **2021**, *23*, 45–57. [CrossRef] [PubMed]
26. Salman, F.M.; Abu-Naser, S.S.; Alajrami, E.; Abu-Nasser, B.S.; Alashqar, B.A.M. COVID-19 Detection using Artificial Intelligence. *Int. J. Acad. Eng. Res.* **2020**, *4*, 18–25.
27. Rangarajan, A.K.; Krishnaswamy, A.; Ramachandran, H.K. A preliminary analysis of AI based smartphone application for diagnosis of COVID-19 using chest X-ray images. *Expert Syst. Appl.* **2021**, *183*, 115401. [CrossRef]
28. Xue, H.; Liu, B.; Din, M.; Song, L.; Zhu, T. Hiding private information in images from AI. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
29. Pawar, U.; O'Shea, D.; Rea, S.; O'Reilly, R. Explainable ai in healthcare. In Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 15–19 June 2020; pp. 1–2.
30. Cinà, G.; Röber, T.; Goedhart, R.; Birbil, I. Why we do need Explainable AI for Healthcare. *arXiv* **2022**, arXiv:2206.15363
31. Caramelo, F.; Ferreira, N.; Oliveiros, B. Estimation of risk factors for COVID-19 mortality-preliminary results. *MedRxiv* **2020**. [CrossRef]
32. Lueger-Schuster, B.; Zrnić Novaković, I.; Lotzin, A. Two Years of COVID-19 in Austria—Exploratory Longitudinal Study of Mental Health Outcomes and Coping Behaviors in the General Population. *Int. J. Environ. Res. Public Health* **2022**, *19*, 8223. [CrossRef]
33. Hoepman, J.H. A critique of the google apple exposure notification (GAEN) framework. *arXiv* **2020**, arXiv:2012.05097.