Int. J. Advance Soft Compu. Appl, Vol. 12, No. 3, November 2020
ISSN 2074-8523; Copyright © ICSRS Publication, 2020
www.i-csrs.org

Covid-19 Tracing Contacts Apps: Technical and Privacy Issues

Salaheddin J. Juneidi

Computer Engineering Department,
Palestine Technical University Khadoorei[1],
Hebron, West Bank Palestine.
e-mail: Salaheddin.juneidi@ptuk.edu.ps

Received 20 July 2020; Accepted 5 October 2020

Abstract

Since the start of the year 2020 the world is facing an outbreak of Covid-19 pandemic, technical specialists all over the universe have been scrambling to develop services, apps, and system's protocols for contactors tracing, with the objective to identify and to notify everyone that gets close with an individual carrier. Some of these apps are lightweight and temporary, while others are diffuse and aggressive. Some of tracing services are developed locally by small interested programmers, while others are large-scale international operations. To date, we have recognized more than 25 large automated contact tracing efforts around the globe, included with details about what they were, how they worked, and the procedures and conditions that were put in place around them. This paper will deal with general data of the most prominent applications in terms of technical approaches used in the world and compare them with regard to the efficiency of tracking covid-19 and compare them with concerning of the people's privacy who use these apps.

Keywords: *Covid-19, GPS location, Blue trace, Google/Apple, DP-3T, Apps, Privacy.*

1. Introduction

Many applications, services and systems have been proposed and launched [1] with an aim to track and identify infected people with objective to reduce or even to prevent physical contact with other people, some of these tracking

[1] Special thanks to Palestine Technical University -Khadoorei for continuous support of research efforts

technologies are lightweight and temporary, while others are widespread and invasive: the Chinese system, for example, absorbs data including very personal data such as *identity*, *location* and even online *payment history* so local police can monitor those who break quarantine rules.

Modern technology is based on big data manipulation in all aspects of life [2]. Smart mobile devices include many sensors and functions that are capable of gathering an enormous amount of sensitive information. As a result, any vulnerability in the host platform can have a significant impact on end user privacy and security. Android platform and OSI can be manipulated and exploited by a malicious application to gain access to users' private data. So we need to worry about the users privacy too. Some services are produced locally by small groups of programmers, while others are large-scale global operations. Apple and Google are mobilizing huge teams to build their next systems that notify people of potential exposure, which hundreds of millions of people can use almost instantly. Despite the flow of services, we know very little about them or how they might affect society. How many people will download and use it, and how widely will it be used to make it work? What data will they collect, and with whom is it shared? Are there policies in place to prevent abuse? We started asking these questions and finding that there aren't always clear answers. Then we started comparing apps around the world, to understand how these apps work , with the purpose to identify their technical specifications and how much they preserving privacy of people.

We realized that there isn't a central repository of information; Raw and ever-changing piece of data is spread across a wide variety of sources. There was no single standardized approach for developers and policymakers. Citizens of different countries saw radically different levels of oversight and transparency. With a purpose for helping in monitoring this rapidly evolving unusual situation, most important job is gathering information in one place for the first time with the Covid Tracing Tracker - a database for capturing details of every major effort to track automated contacts around the world. This article is structured as the following, the first section is an introduction and related work, the second section will go through main approaches and protocols to track covid-19, and the third section will evaluate these approaches regarding efficiency and privacy, and finally will conclude this article.

Table 1: Apps of tracing contacts in 45 country and the technology used [1]

No	**Country**	**Name**	**Technology**
1	Australia	COVIDSafe	Bluetooth
2	Austria	Stopp Corona	Bluetooth, Google/Apple
3	Bahrain	BeAware	Bluetooth, Location
4	Belgium	Belgium's app	Bluetooth, Google/Apple, DP3T
5	Bulgaria	ViruSafe	Location
6	Canada	COVID Alert*	Bluetooth, Google/Apple
7	China	Chinese health code system	Location, Data mining
8	Cyprus	CovTracer	Location, GPS
9	Czech	eRouska	Bluetooth
10	Denmark	Smittestopp	Bluetooth, Google/Apple
11	Estonia	Estonia's App*	Bluetooth, DP-3T, Google/Apple
12	Fiji	CareFiji	Bluetooth
13	Finland	Ketju	Bluetooth, DP-3T
14	France	StopCovid	Bluetooth
15	Germany	Corona-Warn-App	Bluetooth, Google/Apple
16	Ghana	GH COVID-19 Tracker	Location
17	Gibraltar	Beat Covid Gibraltar	Bluetooth
18	Hungary	VirusRadar	Bluetooth
19	Iceland	Rakning C-19	Location
20	India	Aarogya Setu	Bluetooth, Location
21	Indonesia	PeduliLindungi	Bluetooth, Location
22	Iran	AC19	Location
23	Ireland	Covid Tracker	Bluetooth, Google/Apple
24	Israel	HaMagen	Location
25	Italy	Immuni	Bluetooth, Google/Apple
26	Japan	COCOA	Google/Apple
27	Kuwait	Shlonik	Location
28	Malaysia	MyTrace	Bluetooth, Google/Apple
29	Mexico	CovidRadar	Bluetooth
30	New Zealand	NZ COVID Tracer	Bluetooth, QR codes
31	Northern Ireland	StopCOVID NI	Bluetooth, Google/Apple
32	Norway	Smittestopp	Bluetooth, Location
33	Philippines	StaySafe	Bluetooth
34	Poland	ProteGO	Bluetooth
35	Qatar	Ehteraz	Bluetooth, Location
36	Saudi Arabia	Tawakkalna	Location
37	Saudi Arabia	Tabaud	Bluetooth, Google/Apple
38	Singapore	Trace Together	Bluetooth, BlueTrace
39	Switzerland	SwissCovid	Bluetooth, DP-3T, Google/Apple
40	Thailand	MorChana	Bluetooth, Location
41	Tunisia	E7mi	Bluetooth
42	Turkey	Hayat Eve Sığar	Bluetooth, Location
43	UAE	TraceCovid	Bluetooth
44	UK	NHS COVID-19 App	Bluetooth, Google/Apple
45	Vietnam	BlueZone	Bluetooth

1.2 Covid-19 trackers main approaches

Primarily, first step is compiling a list of automated contact tracing apps which provided by various national governments. These apps are designed to automatically notify users or public health officials whether someone has been exposed to covid-19; It is what is commonly known as an *'exposure notice'*. Additionally, we say something about the underlying technology that the app is based on. The basic terms are explained below, and in the following categories:

- *Location*: Some applications identify a person's contacts by tracking phone movements (for example, using the Global Positioning System (GPS) or triangulating from cell towers).
- *Bluetooth*: Convergence tracking, as it exchanges encrypted feature phones with other nearby phones via Bluetooth. Better ID tracking in target capture area.
- *Google / Apple*: It depends on the common API developed by Apple and Google. It allows iOS and Android phones to communicate with each other via Bluetooth, making it a connection that allows contacts to connect to both. Later on the two companies plan to build this feature directly into their operating systems.
- *DP-3T:* This means decentralized tracking to maintain privacy. It is an open source protocol for Bluetooth-based tracking where individual phone contact records are only stored locally, so no central authority can know who has been exposed.

These categories may expand over time, but these are at which point this article is written. There are many factors that affect this type of applications, we need to agree on criteria to know how effective these applications are, and we also need to balance this effectiveness factor with the privacy of people. We know that culture and laws are the main effect on protecting people's privacy. Privacy from religious and atheist societies differs from a free and dictatorial democratic state. The technology can be with a double edge that can intrude privacy and the other can protect privacy, so it is not the technology that is responsible but how it will be used. From Table 1, we see that several applications are being used to track Covid 19 vectors. In the next section, we will describe these applications technically and ethically according to the above categories.

2. Categories of Covid-19 Tracking and Apps

Many apps have been proposed to make accurate trace of contacts of Covid-19 [1] , each country has its tracking apps , and some time more than one apps are used in a catenin country and people can select which apps like to use , we have mentioned categories to distinguish between these more than 200 various contact tracing apps. In this section we will define the technical and ethical issues related to each category , so we will go through in each method without judging which is more effective, because that needs a period time for carrying out testing regarding efficiency.

2.1 Location GPS

Many applications for tracing contacts have been produced and adopted, mostly with governmental support in some regions and authorities. Several frameworks have been developed for creating apps for contact tracing. Privacy concerns have been raised, particularly around systems that rely on tracking the geolocation of app users.

Less intrusive alternatives include the use of Bluetooth signals to record the user's proximity to other cell phones. The result of cooperation of Google and Apple resulted that they announced that they would integrate functionality On April 10, 2020, with purpose to make the Android and iOS operating systems to support blue tooth-based applications directly. The Indian Covid-19 tracking app Aarogya Setu has become the fastest growing app in the world, outperforming Pokemon Go with 50 million users in the first 13 days of its release.

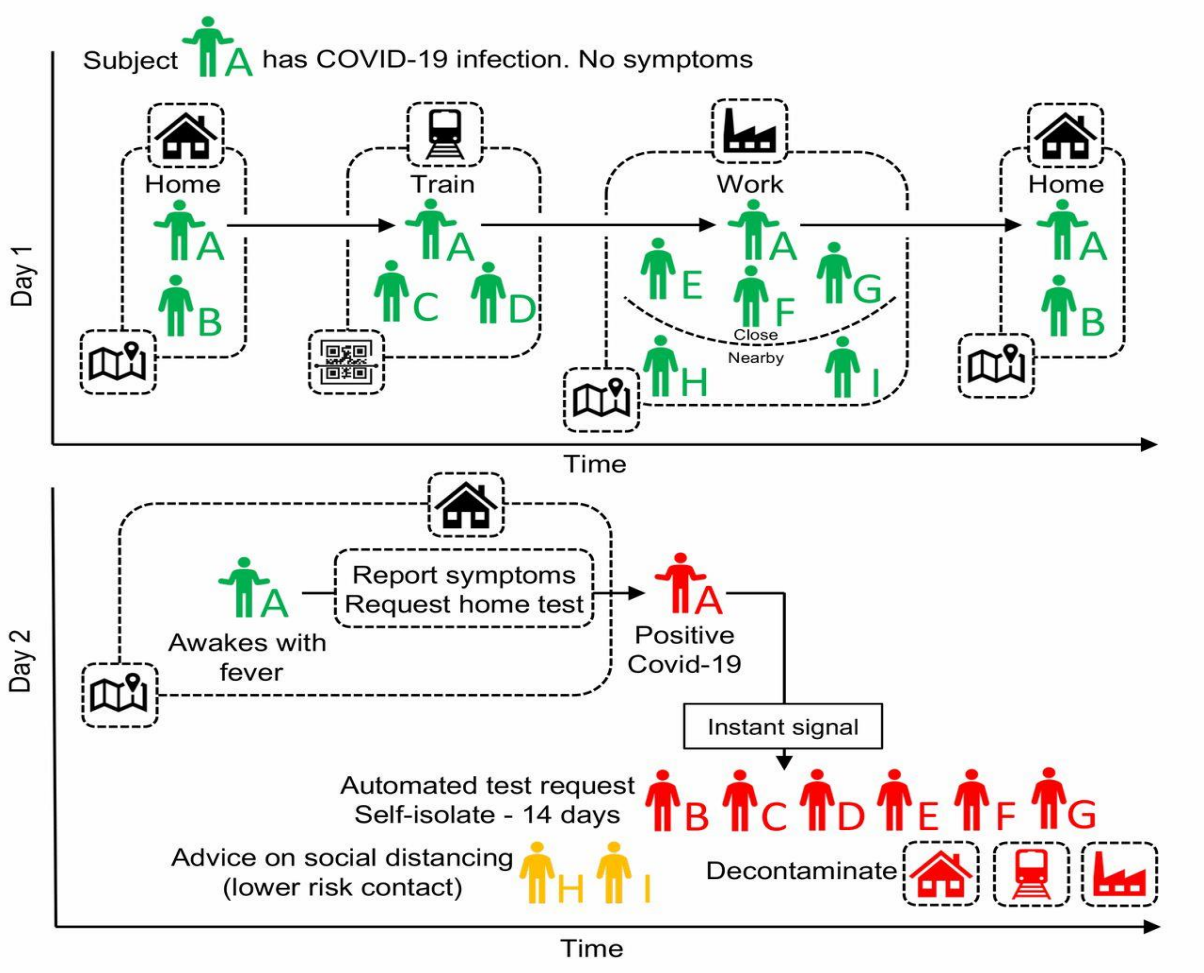

Figure 1: COVID-19 GPS &-localizations protocol of tracing contacts and tracking apps

Figure 1 is an example of proposal for aCOVID-19 based on location-based contact tracking apps. For example an individual A's contacts (and also

individuals who using the app) can be tracked using GPS shared localization of each others with app users, complete with scanning of QR codes shown on the facilities in general is highly mobile as the GPS is very rough. For each user requests a SARS-COV-2 test (using some apps) and for any positive test result initiates an instant message notification to users who have been in close contact. The application recommends isolating the case (Individual A) and quarantining their contacts. Some countries are using network-based location tracking instead of apps, which eliminates the need for an app download / install and the ability to avoid being tracked. The Israeli entity that occupied Palestine, for example, which defined as police and a military state, network-based tracking has been approved. [3] Network-based solutions that have access to raw location data have potentially significant privacy issues without users permission, or how much data is transferred to the surveillance tracking system. However, not all systems with central servers need access to personal location data; A number of privacy systems have been established that use only centralized servers for interconnection (see the section below). [4]

Another example of location GPS, In South Korea, without apps based system was used to perform contact tracing. Instead of using a “dedicated app”, the system collected tracking information from a variety of sources including mobile device tracking data and card transaction data and combined them to create text message notifications for potentially infected individuals. [5] In addition to using this information to alert potential contacts, the government has also made location information available to the public, which is permitted due to far-reaching changes in information privacy laws following the outbreak of MERS in that country. [6] This information is available to the public through a number of apps and websites.

Gulf Arabic countries and states, for example Saudi Arabia, the Emirates, Bahrain ... etc [1], the official mobile application for Android and iOS, developed by Information Government Authority (iGA), The app to alleviate the spreading of COVID-19 by the implementation of contact tracing efforts for identifying and tracking the whole of active cases and also their contacts. It also uses citizens' location data to alert individuals in case they approach an active state or a visited site an active case, as well as track the movement for cases that are in quarantine with a time period of 14 days (then lately reduced to only 10 days by WHO) ; The app arranges a affect-resistant GPS tracking contacts for sharing a real-time tracking information with health workers. Health workers are notified when quarantine cases exit the 15-meter pre-defined area, and in this case the team will respond by reminding individuals of the importance of following procedures to preserve the welfare of citizens and residents.

2.2 Blue Trace

This protocol focuses on two areas, first registering locally registered users in the zone around of the device, second sending the record to the Operational Health Authority, taking in consideration of maintaining privacy. We can do this,

by protocol that can be divided into Device – to - Reporting Server Communication (DRSC), and Device-to-Device Communication (DDC) areas.

The DDC component runs over the existing Bluetooth Low Energy protocol, and determines how two devices recognize each other's existence [7]. The DRSC component uses HTTPS to report a schedule of visits to a central server owned by a health authority once the user has tested positive for the infection. The health authority can then, using the registry, notify users who have come into contact with the infected patient [8].

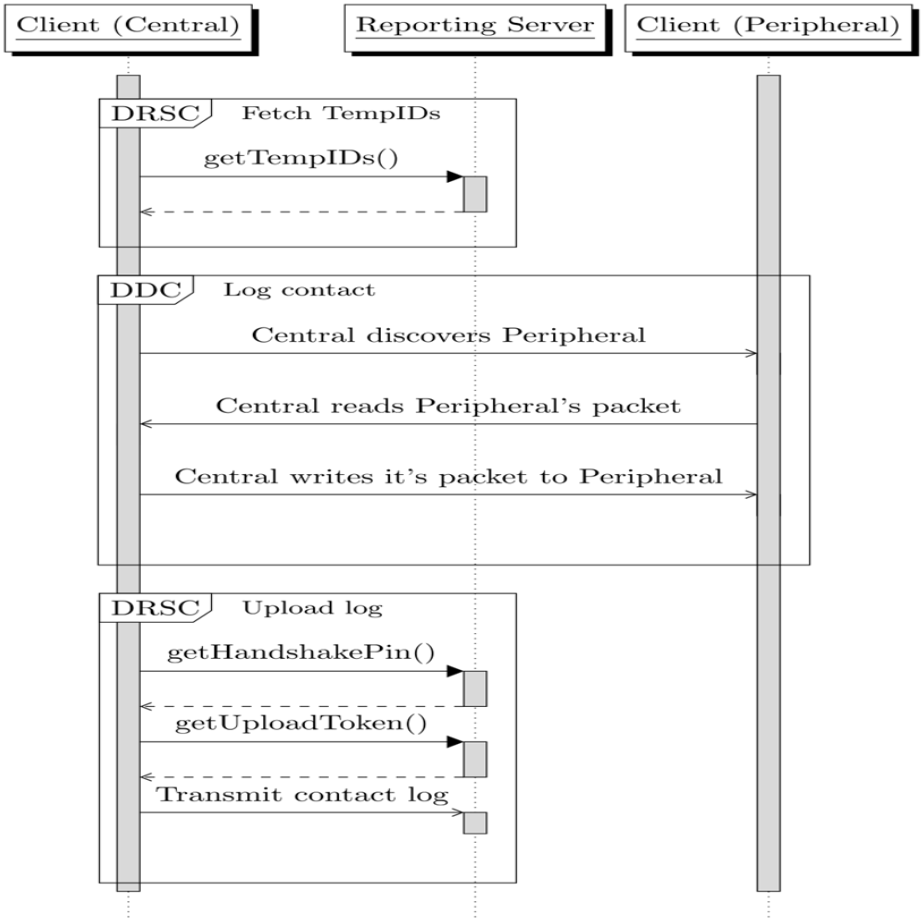

Figure 2: DRSC And DDC communication protocols of blue trace

Every application that implements the "*BlueTrace protocol"* has a matching central reporting server managed by a health authority. We must notice that the report server is the one which responsible of processing for initial registration, then it provides a unique user IDs, and then it collects the contact records that are generated by the DDC portion of the protocol. When a user launches the BlueTrace app for the first time, they will be asked for their internationally formatted phone number and assigned a fixed ***user ID***. [8]. This phone number is used later if the user records an encounter in an infected patient's call log. Once registered, users are provided temporary identifiers ***(TempIDs***) to

uniquely identify them on other devices. Each ***TempID*** has a life of 15 minutes to prevent malicious parties from carrying out reboot attacks or tracking users over time with persistent unique IDs. ***TempIDs*** are generated from the User's ***UserID, TempID*** start time, and ***TempID*** expiration time, which is encrypted and converted to the *Base 64* chain by the server using a secret symmetric encryption key. For making sure that the devices have steady supply of TempIDs, also even with unbalanced network environment, ***TempIDs*** are sent to devices in dated batches. The ***TempID*** configuration is shown below [9].

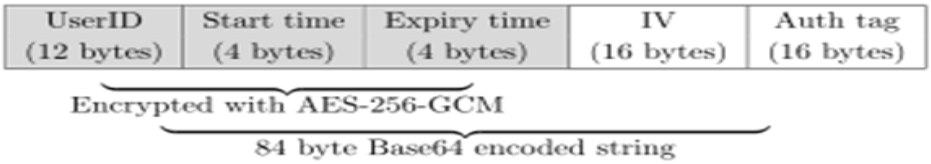

Figure 3: Base 64 registered user logged record


```
            "id":
"FmFISm9nq3PgpLdxxYpTx5tF3ML3Va1wqqgY9DGDz1utPbw+Iz8tqAdpbxR1
nSvr+ILXPG==", // TempID
            "md": "iPhone X", // Device model
            "rc": -60, // Signal strength
            "o": "IJ_HAI", // Health authority identifier
            "v": 2 // Protocol version
}
```


Figure 4: Example of Register user logged record

These properties are then added to a local database on the device where they are stored for 21 days and can be sent to the report server later. The connected device is also added to a local blacklist for two work cycles in order to stop two devices from repeatedly communicating with each other, saving power and storage. The a key component of the BlueTrace protocol is based on the collaboration between separate health authorities [10]. As in Figure 5 it is designed so that multiple authorities can work together without disclosing personal information to foreign authorities with which the user is not registered. Because different authorities preserve their own encryption keys and also their own format of user records, health authority from other country cannot decrypt and see a foreign user data.

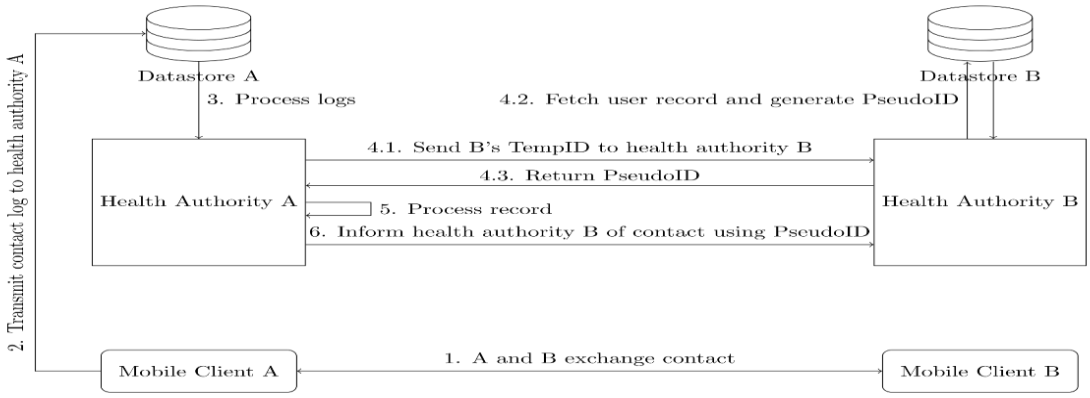

Figure 5: Multiple authorities exchange data about contacts

To ensure that registry of the entries are sent to the correct reference [11], part of the DDC handshake process will contains a health authority identifier (HAI), which is a unique string assigned to registered health authorities. As soon as the registry entry for a foreign health authority is identified, the receiving health authority transfers the log entry to the foreign authority's reporting server where it is verified, and a fixed PseudoID is returned.

The ***PseudoID*** is represented a user ID cryptographic function hash, designed to enable foreign health authorities to make statistical analysis on contact records about a specific user without revealing unnecessary personal information [12]. Once PseudoID is evaluated in close contact with the infected patient, the foreign health authority that issued the PseudoID is informed and can follow up as necessary.

2.3 Google/Apple

Digital contact tracing protocols typically have two main responsibilities, summarized as recording confrontation and reporting infection. [13] Exposure notification only defines encounter logging and is a decentralized architecture, with the majority of infection reports being centralized, delegated to individual application applications.

To handle confrontation recording, the system uses Bluetooth Low Energy to send tracking messages to nearby devices running the protocol to discover encounters with other people. Tracking messages contain unique identifiers that are encrypted with a secret daily key kept by the sending device. These IDs change every 15-20 minutes as well as the Bluetooth MAC address in order to prevent customers from being tracked by malicious third parties by monitoring the static IDs over time.

The daily encryption keys for the sender are generated with a random number generator. [14] The devices record received messages and keep them locally for 14 days. In the case of some of the users have tested positive that

means infected, the latest 14 days of daily encryption keys are uploaded to a central server, from where they are transmitted to all devices on the network. The manner in which the daily encryption keys are transmitted to the central server and broadcast is determined by the individual application developers. The conventional received keys are then accessible established in the protocol, where every client individually can search for matches in the local to meet some logs. If a match is found that meets certain risk criteria, the app notifies the user of potential infection. Google and Apple is using Received Signal Strength (RSSI) of some beacon messages as soon as some a source of proximity inference. RSSI and other signal metadata will also be encrypted to resist de-identification attacks.

This protocol does not use a persistent *tracing* ***key,*** rather every day a new random 16-byte *Temporary Exposure Key* ***(tek$_i$)*** is generated. Here ***i*** denotes the time is discretized in 10 minute intervals starting from Unix Epoch Time. From this two 128-bit keys are calculated, the *Rolling Proximity Identifier Key* **(RPI_X)** and the *Associated Encrypted Metadata Key* ***($AEMK_i$). RPI_X*** is calculated with the algorithm , ***$RPIX_I$= HKDF(tek$_i$,NULL, 'EN-RPI_X' , 16) and $AEMK_I$*** *using* the algorithm ***$AEMK_I$* = HKDF(*teki ,NULL, 'EN-AEMK' , 16)*** **.**

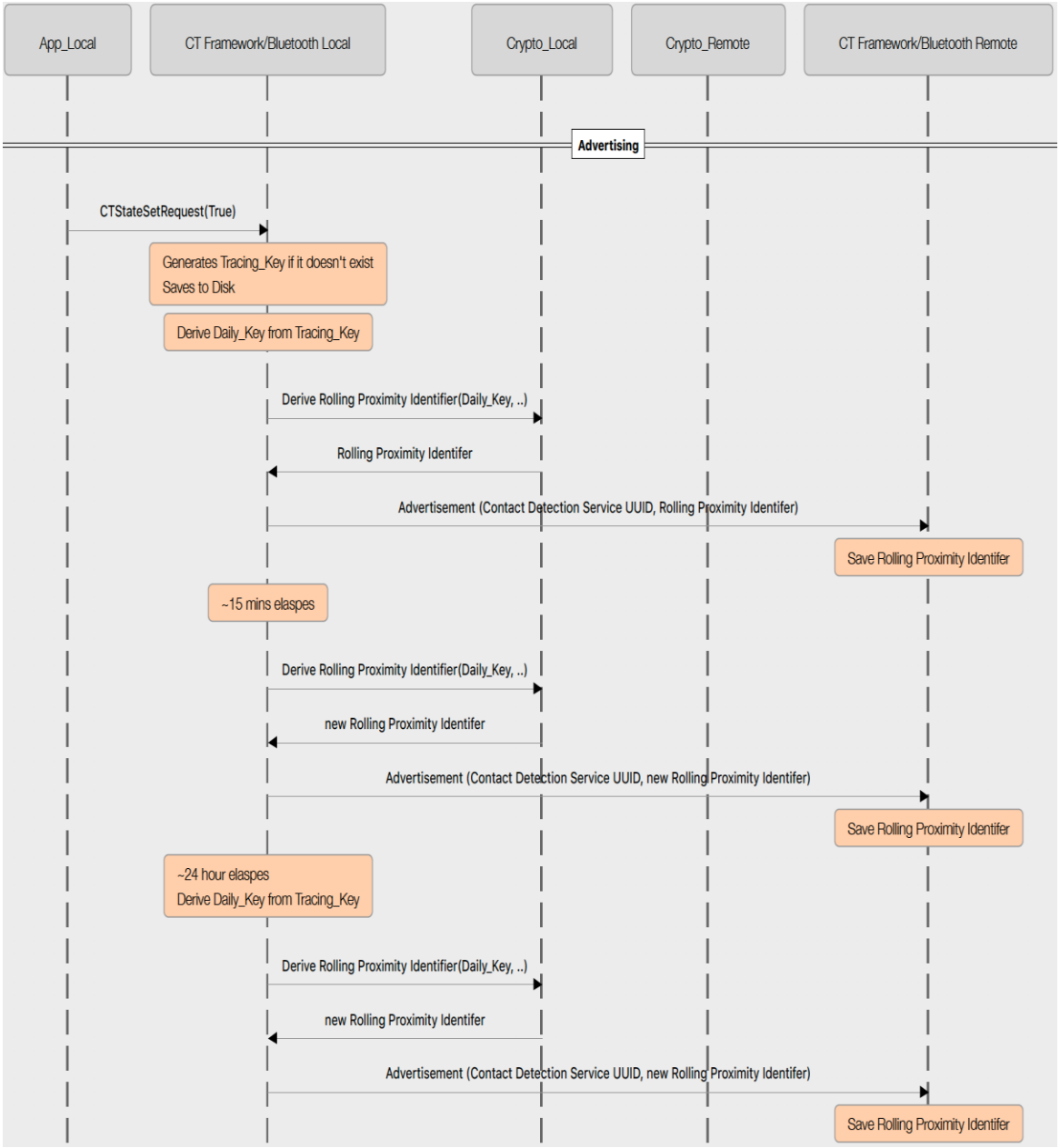

Figure 6: Apple/ Google Crypto Schema

From these values a temporary Rolling Proximity Identifier ***(RPII,J***) is generated every time the BLE MAC address changes, roughly every 15-20 minutes. Using the following algorithm ***RPII,J = AES128 (RPIXI , 'EN-RPI||0x00000000000 || ENIN),*** where ***AES128 (Key, Data)*** is an ***AES*** cryptography function with a 128-bit key, the data is one 16-byte block, j denotes the Unix Epoch Time at the moment the roll occurs, and ***ENIN*** is the corresponding 10-minute interval number. Next, additional Associated Encrypted Metadata is encrypted. Notice if the metadata represents is not specified, we need

to allow for later expansion of the protocol. The following algorithm is used which is defined as Associated Encrypted ***Metadatais i,j = AES128_CTR (AEMK,RPII,J , MetaData),*** where ***AES128_CTR (Key,IV, Data)*** denotes AES encryption with a 128-bit key in CTR mode. We must notice that the Rolling Proximity Identifier RPI and its Associated Encrypted Metadata AEM are normally then combined and broadcast using BLE. On the behalf of Clients exchange and l their logs of these payloads. [15]

Figure 6 depicts Apple / Google Phone Encryption Scheme creates a secret "tracking key" for your device at once. Then this secret key is used to generate a Daily Tracking Key every day, thus generating a Rolling Affinity ID from the Daily Key every 15 minutes. Each key is generated more frequently than the original by hashing with a *timestamp*, which makes it nearly impossible to move up the chain, and infer your daily key from the affinity identifiers being sent, for example, but everything can be easily verified downstream [16]. The 32-byte trace key is large enough that collisions are not very likely, and everyone's tracking key does not need to be disclosed. If the test result is positive, your daily keys for the time window you were infectious will be uploaded to a Diagnostic Server, which then sends these daily keys to all participating phones, allowing each device to check the signals it received against the list of infectious people - that you get. From the server. None of your exposure data needs to be left behind at all.

Diagnostic server uses daily keys for infected individuals so that your phone is able to distinguish between one short contact, where only one ID was seen from a given daily key, and a longer and more dangerous contact, where it is multiple for 15 minutes IDs were seen from the same affected daily key , Although your phone cannot link the rolling proximity IDs together over time. And since the everyday keys are derived from your covert key in a one-way fashion, the server doesn't need to know anything about your identity if you are infected.

The ACLU has produced a white paper that precedes the proposed plan, but covers what they would like to see on the privacy and security fronts, and presents it in light of this. The current proposal scores well. Being in line with other "contact tracing" recommendations to maintain privacy is also reassuring. Once a registered health authority confirms that a user has been infected, the user's temporary exposure switches $\boldsymbol{tek_i}$ and their respective interval numbers ***i*** for the past 14 days are uploaded to the central reporting server. Clients then download this report and individually recalculate every Rolling Proximity Identifier starting from interval number ***i,*** Match it with the local user's meeting record. If a matching entry is found, a contact is created and the app provides a notification to the user warning them of a potential infection. [17]

2.4 Decentralized Privacy-Preserving Proximity Tracing (DP-3T)

DP-3T, stylized as $\boldsymbol{dp^3t}$, It is an open protocol developed in response to the COVID-19 pandemic to facilitate digital contact tracing of infected participants.

[18] The protocol, like the competing protocol, uses Pan-European Privacy Preservation Convergence Tracking (PEPP-PT), Bluetooth Low Energy technology to track and record encounters with other users. [19] The protocols are different in terms of their reporting algorithm, as ***PEPP-PT*** is requesting from clients to upload their contacts records to a central reporting servers. While with DP-3T.the central reporting server never has access to contact records nor is it responsible for processing clients and informing them of the connection. [20] Because of contact records will never transferred for third parties, so it will has significant privacy advantages over the ***PEPP-PT*** approach, but this comes at the expense of requiring more computing power from the client side to process infection reports

The DP-3T uses 16-byte ephemeral identifiers (***EphID***s) to uniquely identify devices in the vicinity of the customer. These ***EphID***s are recorded locally on the receiving customer's device and are never transferred to third parties.

As we decide to coexist the pandemic, whether we are in lockdown or still at work, there is a chance for all of us that we can still catch the virus from a stray contact. [21] Planning these infections and tracking people close to sick can be a big problem for infection control authorities, and there have been a variety of proposals for smartphone apps designed to track users' contacts via the bluetooth identities that their phones encounter. This is the most concern to privacy concerning people because there is a chance that governments could use this as an excuse to dig into people's data and personal surveillance by these means. Given in Figure 7 ;some universities academics around Europe have join their efforts with a proposal for decentralization to get proximity checking and to tracing systems which will allow spotting candidate infection risk without compromising the privacy of those using it.

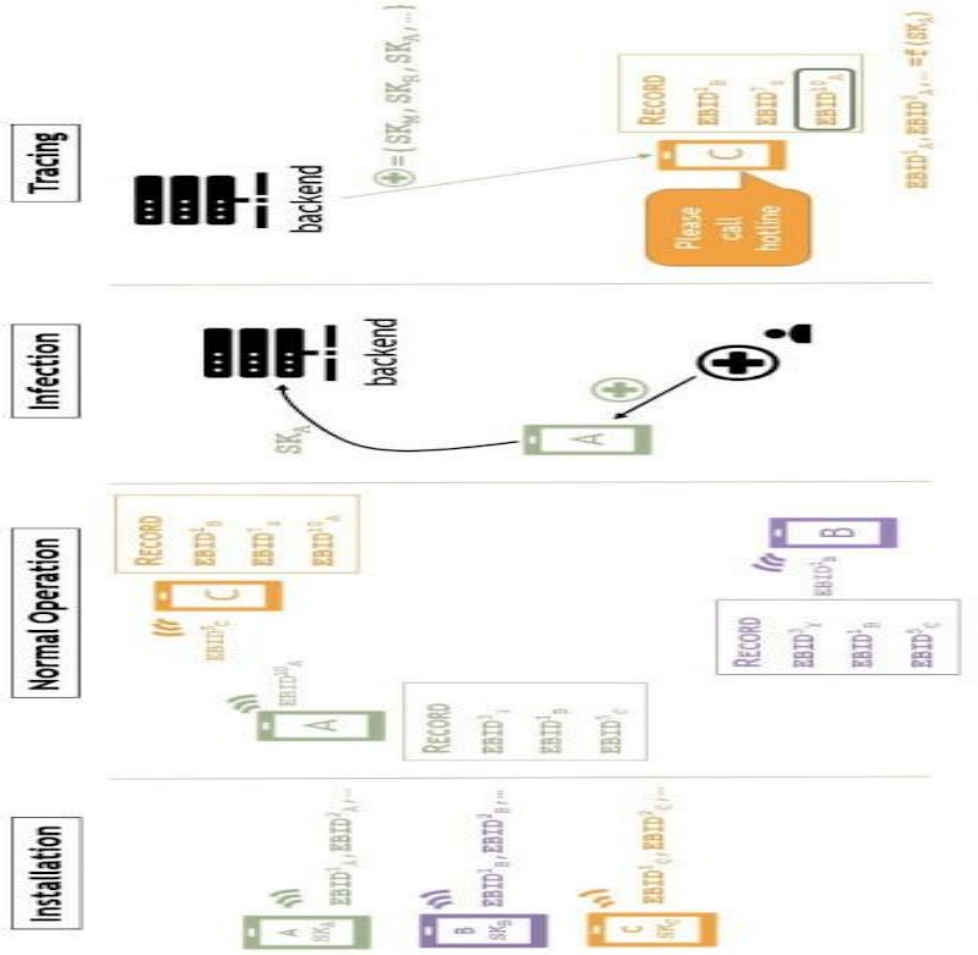

Figure 7: Protocol of decentralization of proximity and tracing systems that allow identification of infection risk

As a privacy snooping system may use a backend database to track all users and record their locations and interactions, this system uses anonymous codes stored on the local level instead of the central server[19]. When a user is infected, it is entered at the application level rather than at the server level, and the central portion of the system only distributes anonymous tokens to clients. Thus, the calculation of whether an infected person has been contacted is made on the customer, which means that the operator has no opportunity to collect monitoring data. When the time the pandemic is gone away, the system will disappear as people will abandon itTo generate an **EphID,** first, a client generates a secret key that rotates daily **(SKt)** by computing, ***SKt = H (SKt-1*)** where ***H()*** is a cryptographic hash function such as ***SHA-256.*** SK_0 is calculated by a standard secret key algorithm such as ***Ed25519***. The client will use SKt during the day t to generate a list of *EphIDs.* At the beginning of the day, a client generates a local list of size $n = (24 * 60) / l$ new ***EphID***s to broadcast throughout the day, where *l* is the lifetime of an *EphID* in minutes. To keep way abusive third parties from

launching patterns of movements by defining tracing static identifiers over a wide area, ***EphID*s** are rotated frequently. As shown in Figure 8Given the secret day key SKt, each device computes ***S_Epf.ID (BK) = PRG (PRF (SKt, BK)),*** where *BK* is a global fixed string***, PRF ()*** is a pseudo-random function like *HMAC-SHA256*, and *PRG()* is a stream cipher producing *n*16* bytes. This stream is then divided into 16-byte chunks and arbitrarily sorted to get the ***EphIDs*** of the day.[20]

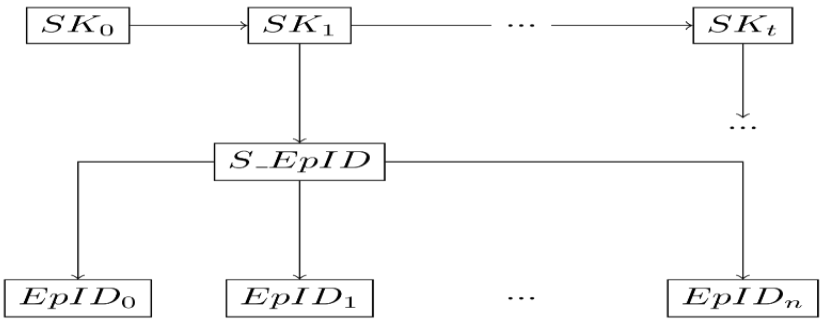

Figure 8: diagram of different components of the Ephemeral ID algorithm used input of each other

2.4.1 Dp-3T has two main components

1-Device handshake: In order to find and communicate with clients in close proximity to a device, the protocol uses both the server and client modes of Bluetooth LE, switching between them frequently. In server mode, the device announces its EphID to be read by clients, with clients searching for servers. In case some client meets server, clients read their EphID and afterward writes their EphID to the server. The two devices then store the meeting in their contact records along with an approximate timestamp and signal strength. Signal strength is used later as part of the infection reporting process to estimate the distance between an infected patient and a user. [21].

2-Infection report: When reporting an infection, there is a central reporting server that is controlled by the local health authority. Before a user can send a report, the health authority must first confirm the infection and create a code that authorizes the customer to download the report. In addition, the health authority instructs the patient on the day on which their report should begin (denoted by the symbol **t**). The client then uploads the SK and t pair to the central reporting server, which other clients in the network download at a later time. Using the same algorithm used to generate the original ***EphIDs***, customers can reproduce every ***EphID*** that has been used for the past period including ***EphID,*** and then check their local call log to determine if the user is in close proximity to an infected patient.

In the entire protocol, the health authority never had access to contact records, only testing patients and allowing reporting. The DP-3T protocol consists of two separate responsibilities, tracking and recording close encounters with other users

(handshaking), and reporting those encounters so that other clients can determine if they have been in contact with an infected patient (report an injury). Likewise most of the networking contact tracing protocols, devices do handshake using Bluetooth with Low Energy to search and find and then to share details with some local nearby clients, then the infection reporting stage uses HTTPS to upload a report to a central reporting server. In addition, like other decentralized reporting protocols, the central reporting server cannot access the contact records of any client; Instead, the report is designed so that customers can individually derive the connection from the report

3. Covid-19 trackers evaluation

From the previous discussions on various categories of apps and technical protocols on tracking Covid-19 and tracing contacts , we found that two main issues must be taken in consideration which are *efficacy and privacy,* these two issues must be balanced to have most efficient in tracing contactors and also to keep the minimum privacy rules that applied in most free countries. In this section we will go through some criteria of the up mentioned categories to define and compare between them, to determine the most appropriate technology to be adopted according each country regulations

1. Technical issues

Technology is getting smarter with more advanced programming and engineering techniques [21]. Technical issues is describing merely the backbone equipment, servers, cloud, edge computing and communication media to trace contacts of Covid-19, the following are characteristics that we are concerning with regarding technical issues:

1. Centralized vs, Decentralized: in the most basic form centralized is collecting and processing in one level in a hub of infrastructure could be a cloud or central server. D centralized data is collected in distribute servers or edge data centers and data is processed in each location solely.
2. Communication media Secured: is defined how much data carriers are secured from intruders to / from data repository such as server, cloud, data center and edge computing
3. Data and user authorization: is concerning to who can see these data? permissions and right for users to access data stored on repositories.

2. Privacy issues

Privacy is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively. nevertheless, Privacy may be lessened by surveillance, for Covid-19 tracing of contacts we need to look after the following points concerning privacy [22].

1. Voluntary: the users have an option to download the apps. Or it’s not the decision of citizens to decide and they must comply for country policy.

2. Data limited : collected data is limited to check the Covid-19 tracing contacts and not use for track citizens behaviour and interests
3. Data destruction: data is not lasting for ever and useless data is deleted once it runs out of time. And will not processed later for other usage of tracing of Covid-19 contacts.
4. Transparency: the ability to users to see his/her own data and ability to communicate data admin for changing false data that collected in uncertain procedures

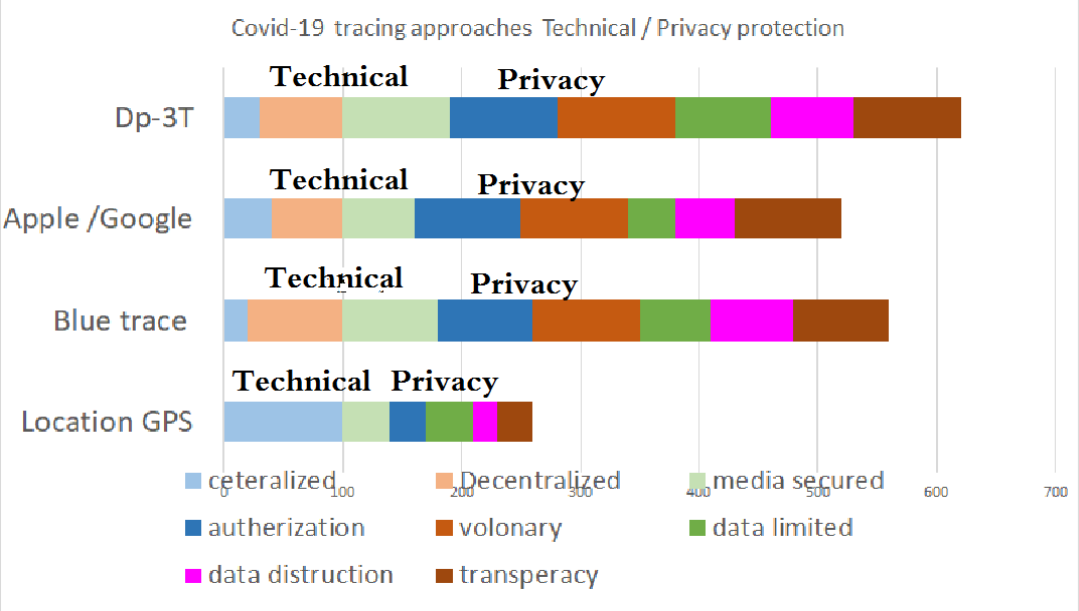

Figure 9: Percentage of main tracing methods for technical and privacy issues

In total we have seven related points and issues (technical + privacy) must be considered to give an evaluation of the main approached of tracing contacts. Each point will be given a value out of 100% , this value is given based on the amount of how much each category/ approach is considering this certain point of issue .For example the issue *centralized* is given 100% in Loction GPS , but is given 30% , 40%, 15% in Dp-3T, Apple/ Google , Blue trace respectively , From the elaborated details that are given in the previous section we can determine the amount of the evaluation criteria for technical and privacy issues Figure 9 is summarizing the combination of technical and privacy issues. This combination is based on giving to each criteria a value of 100% to be added for each tracing approach, with error margin about + or – 10%, we notice from Figure 9 that technical issues is not vary between these approaches. But privacy issues are much different depending to the privacy criteria that given above.

4 Conclusion and Remarks

We have seen in this article that the world has faced a new epidemic with high rate of infection, this infection is based on social contacting , this article is

not going through the medical reasons and medical prescriptions and also is not about to define the main actors for infection whether it's the mouth , nose , eye and handshaking. The contribution of this article is to categorize and to compare main approaches for tracing Covid-19. In General, we notice that as much as we have fewer social contacts the less this epidemic will spread. From the fact that every person is carrying cellular phone, we can track the movement for a person from his/her cellular, and then take an action on infected people according to their situation that can be alert messages to all people close to him / her , or even the action quarantine of this person amount of time. Technology is offering a wide range of data availability about people not only location , but every daily action can be detected by technology which may *jeopardize* people privacy .This research is presented for researchers and practitioners to understand the main methods to trace contacts of Covid-19, accordingly the amount of data is exposed people depending on the selected approach. We have presented four approaches that summarize more than 45 various apps for tracking people used in the world , then we established criteria to judge each approach, this criteria is composing two main part ,first part is technology efficiency , and the second part is privacy preserving, We relate technical and privacy issues to ensure as much as we could to keep the balance between technology from one side and privacy from the other side . Then keep choices to each country regime depending the scale level of privacy protection of each country depending on its law and its culture.

References

[1] MIT community about COVID-19, (2020) medical.mit.edu/covid-19-updates MIT 2020, *https://medical.mit.edu/covid-19-update*

[2] Salaheddin J. Juneidi, (2019) Machines' Fault Detection and Tolerance Using Big Data Management, *International Journal of Engineering Research and Technology*. ISSN 0974-3154, Volume 12, Number 10 (2019), pp. 1739-1750

[3] Awang Hendrianto Pratomo, Anggit Ferdita Nugraha, Joko Siswantoro and Mohammad Faidzul Nasruddin. (2019) Algorithm Border Tracing vs Scanline in Blob Detection for Robot Soccer Vision System. *International Journal of Advances in Soft Computing and its Application*, 11, 3(2019), 40-55.

[4] Jack K. Fitzsimons, Atul Mantri, Robert Pisarczyk, Tom Rainforth, Zhikuan Zhao, (2020) A note on blind contact tracing at scale with applications to the COVID-19 pandemic, *Cornell University Research April ,2020 , Cite as: arXiv*: 2004.05116

[5] Dhaval Dave Andrew. Friedson Kyutaro Matsuzawa Joseph J Sabia, (2020) When Do Shelter-in-Place Orders Fight COVID-19 Best? Policy

Heterogeneity Across States and Adoption Time, *Economic Inquiry Journal* , August 2020 ,

[6] Shaoxiong Wang, MD; Shuizi Ding, MD ; Li Xiong2,, MD, (2020)A New System for Surveillance and Digital Contact Tracing for COVID-19: Spatiotemporal Reporting Over Network and GPS JAMIR Publications *Adcvance digital Health Journal , Published* on 10.06.20 in Vol 8, No 6 (2020): June, JMIR Mhealth Uhealth 2020;8(6):e19457, doi:10.2196/19457

[7] Salaheddine Juma Juneidi , (2014) New Computing Paradigm: Agent Orientated Engineering and Programming , *International Review on Computers and Software (e-Journal IRECOS Vol 9, No 6* (2014)Copyright © 2014 Praise Worthy Prize -

[8] M. Toğaçar, B. Ergen, Z. Cömert (2020) COVID-19 detection using deep learning models to exploit social mimic optimization and structured chest *Comput Biol Med*, 121 (2020), *Article 103805, 10.1016/j.compbiomed.*2020.103805

[9] Robert A. Kleinman MD, Colin Merkel MASc, (2020) Digital contact tracing for COVID-19, Cite as: *CMAJ 2020. doi: 10.1503/cmaj.200922; early-released May 27, 2020*

[10] Luca Ferretti, Michelle Kendall, Lele Zhao1,Anel Nurtay, Lucie Abeler-Dörner,(2020) Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing, *Science Journal ,May 2020 , Vol. 368, Issue 6491, eabb6936*, DOI: 10.1126/science.abb6936

[11] Christou, Theodora and Sacco, Maria Pia and Bana, Anurag, (2020)Digital Contact Tracing for the COVID-19 Epidemic: A *Business and Human Rights Perspective* (June 4, 2020). Available at SSRN: *https://ssrn.com/abstract=3618958.*

[12] D. Zeinalipour-Yazti and C. Claramunt, (2020)"COVID-19 Mobile Contact Tracing Apps (MCTA): A Digital Vaccine or a Privacy Demolition?," 2020 21st IEEE *International Conference on Mobile Data Management (MDM),* Versailles, France, 2020, pp. 1-4, doi: 10.1109/MDM48529.2020.00020.

[13] Sagnick Biswas, Labhvam Kumar Sharma, Ravi Ranjan,Jyoti Sekhar Banerjee (2020) an Interactive Cross-Platform Based Dashboard for Real-Time Tracking of Covid-19 using Data Analytics , *Journal of Mechanics of Continual and Mathematical Sciences*, :

[14] K. Michael and R. Abbas, (2020) "Behind COVID-19 Contact Trace Apps: The Google–Apple Partnership," *in IEEE Consumer Electronics Magazine, vol. 9, no. 5, pp*. 71-76, 1 Sept. 2020, doi: 10.1109/MCE.2020.3002492.

[15] Audrey Guinchard (2020) Our digital footprint under Covid-19: should we fear the UK digital contact tracing app*?, International Review of Law, Computers & Technology*, DOI: 10.1080/13600869.2020.1794569

[16] Chettri, Sarat and Debnath, Dipankar and Devi, Pooja, Leveraging Digital Tools and Technologies to Alleviate COVID-19 Pandemic (June 11, 2020). Available at SSRN: *https://ssrn.com/abstract=3626092 or http://dx.doi.org/10.2139/ssrn.3626092*

[17] Douglas J. Leith, Stephen Farrell, Measurement-Based Evaluation of Google/Apple Exposure Notification API For Proximity Detection in a Commuter Bus, Cornel University research 15 Jun 2020, Cite as: arXiv:2006.08543 [cs.NI]

[18] Jason Bay, Joel Kek, Alvin Tan, Chai Sheng Hau, Lai Yongquan, Janice Tan, Tang Anh Quy. (2020) "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders". *Government Technology Agency*. Retrieved 2020-04

[19] Terence Eden (2020) Initial Release NHS Covid Apps Application and System Architecture May, *VM Ware Pivot Labs for British Government* 2020

[20]] *The DP-3T Project*, (2020)Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems, April 2020, Serge Vaudenay, "Analysis of DP3T", 2020, Cryptology ePrint Archive, *Report 2020/399 GITHUB.COM*

[21] *The DP-3T Project*, '(2020) Security and privacy analysis of the document 'PEPP-PT: Data Protection and Information Security Architecture' (*19 April 2020) GITHUB.COM*

[22] Salaheddin J. Juneidi. (2020). From Engineering to Programming: Smart Multi-Agent Application Using ARL. *International Journal of Advanced Science and Technology, 29(05), 2700 - 2716.*

[23] Adilah Sabtu, Nurulhuda Firdaus Mohd Azmi, and Siti Sophiayati Yuhaniz.(2015). Enhancing Security and Privacy Protection for MapReduce Processing: The Initial Simulation Work Flow. *International Journal of Advances in Soft Computing and its Application, 7,* 3(2015), 72-84.

Notes on contributor

Dr. Salaheddin J. Juneidi : Professor at Palestine Technical University – Khadoorei / Aroub , located in Hebron , Palestine. His main research interests are concerning Smart Systems , Big Data Theory , and Cloud – Edge Computing. Dr. Juneidi is the founder of Agent Role Locking ARL Theory , which considered as the basic view of modern agent oriented software engineering.