

OVERVIEW OF TECHNOLOGIES AND APPLICATIONS FOR PHYSICAL DISTANCING DURING THE COVID-19 PANDEMIC

Marko Peric, Dino Zupanovic

University of Zadar, Croatia

Abstract

Paper presents existing technologies and applications and proposes an upgraded application model in prevention of COVID-19 as well as other airborne diseases. By analysing existing applications, their advantages and disadvantages were considered as a baseline for upgraded conceptual application model proposal with special consideration towards users' security and privacy.

Keywords: COVID-19, prevention, application, distancing, review

1. INTRODUCTION

The aim of the whole world is to control COVID-19 pandemic, to slow down the virus transmission, to prevent the disease spread as well as many deaths. Therefore, every country should adopt and carry out measures appropriate for everyone. The role of personal protective measures is to prevent COVID-19 spread from person to person, i.e. to protect a person and their contacts, to lower contamination of surfaces frequently touched. Personal protective measures include frequent hand hygiene, physical distancing, mask using, cleaning and disinfection of one's environments and houses. Measures referring to physical distancing in public prevent virus transmission between infected and non-infected persons. They also protect people with compromised health, i.e. people who are at greater risk of more serious illness if they are infected with coronavirus. These measures include physical distancing, limitations or cancellation of mass gatherings etc. As for physical distancing, World Health Organisation (WHO) recommends a minimal distance of at least one meter between people in order to reduce the risk of interpersonal disease transmission. According to sociologists, the term that should be used as far as distancing is concerned is physical distancing, not social distancing. A distance is measured in metres or centimetres, i.e. it refers to geographical distance from person A to person B. On the other hand, social distancing refers to distance between individuals or groups in society. Modern technologies, especially mobile applications are used to facilitate keeping physical distance. Such a type of mobile applications serves to inform people about new circumstances on physical distancing. In order to avoid the manual contact tracing, the goal was to create a scalable and automated solution of the physical distancing apps. The role of information science, in this context, is to recognize challenges the society is facing with and to respond to them by making suitable software solutions. This paper presents existing methods and concepts of making mobile applications for keeping physical distance, their comparison and, finally, a suggestion for their improvement. It describes centralised and decentralised models of applications, their advantages, flaws, security and anonymity of users.

2. BASIC CONCEPTS OF PHYSICAL DISTANCING APPS

There are two major approaches to the development of this type of applications, centralised and decentralised one. Furthermore, a public debate on the applications' data collecting should be organised. However, there are also concepts of hybrid applications that could be centralized-decentralised. Technologies and their usage in such apps should be described and explained.

2.1. Centralised (non - application) approach

Centralised (non – application) approach uses mobile phone's location and communication between devices to inform the user via, e.g., SMS that they could be infected. Centralised approach gives the epidemiologists a better insight into how the disease spreads. However, as far as GDPR is concerned, the insight into the disease spread and informing the people they could be infected represents a challenge

not only because of the possible privacy breach, but also because of the unauthorised usage of personal data. Some of the countries that have adopted such an approach are Israel, South Korea and Germany which combines both, centralised and decentralised approaches [1, 2].

2.2. Decentralised application approach

Decentralised application approach is more popular than centralised one because of better security solutions. The beginnings of decentralised approach date back to 2013. However, a more active approach to the development of this technology has started with COVID-19 break out. The organisation that has developed an open source application is Covid Watch at Stanford and Waterloo Universities [3]. In the middle of 2020, a group of European researchers from Fraunhofer Heinrich Hertz Institute and École Polytechnique Fédérale de Lausanne under the aegis of Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) started developing a decentralised approach solution. However, due to transparency and privacy issues, the researchers withdrew from the project. At the moment, there are several decentralised approach solutions to apps accepted by many countries.

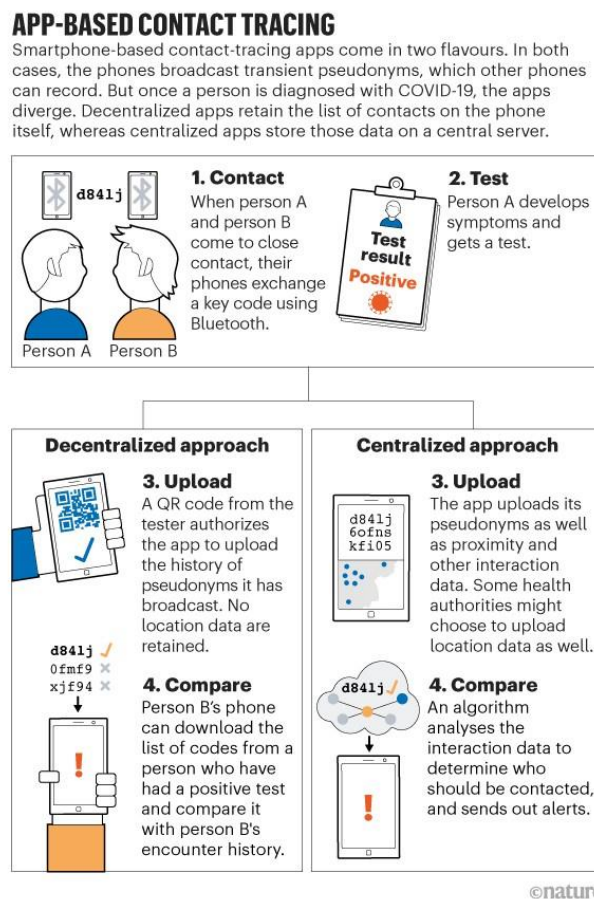


Fig. 1. Illustration of differences between centralised and decentralised systems [1]

3. TECHNOLOGIES AND THEIR USAGE

This chapter presents the usage of various technologies; methods and protocols physical distancing apps are based on. The most significant technology, without a doubt, is Bluetooth, which is the basis of most applications. Bluetooth supports Bluetooth Low Energy (BLE) technology without which mobile phones autonomy would be significantly shorter. Received Signal Strength Indicator (RSSI) helps to determine the approximate distance between the devices.

3.1. Bluetooth

Bluetooth is a wireless technology whose development started in 1989 under the name Short-Link, later renamed to Bluetooth. Ericsson Mobile started its development with the goal to develop wireless headphones. Bluetooth technology is very popular today and is applied in everyday life, in various devices – mobile phones, cars, computer peripherals etc. Institute of Electrical and Electronics Engineers (IEEE) is an organisation in charge of Bluetooth technology's standardisation. Over the years, Bluetooth has had many versions with performance upgrades and improvements [4]:

1. Bluetooth 1.0 and 1.0B (1999) – The first Bluetooth versions had device anonymity problems which made Bluetooth usage impossible.
2. Bluetooth 1.1 (2001) – Device compatibility increased to 100%.
3. Bluetooth 1.2 (2003) – It was the first widely used technology. Pairing speed was improved. Interference with other technologies working in the same frequency was reduced.
4. Bluetooth 2 (2004) - The exchange data rate was improved from 1 to 3 Mbps.
5. Bluetooth 2.1 (2007) – Less power was used. The encryption became mandatory.
6. Bluetooth 3 + HS (2009) - The connection was started via Bluetooth but data was transmitted over Wi-Fi.
7. Bluetooth 4 (2010) - BLE (Bluetooth Low Energy) was introduced with considerably reduced power consumption.
8. Bluetooth 4.1 (2013) – It had more efficient data exchange and better co-existence with LTE frequencies.
9. Bluetooth 4.2 (2014) – It was designed for the Internet of Things (IoT). The size of the packet increased by 10x, making it possible to exchange 2.5 times more data.
10. Bluetooth 5 – It is a version that increases energy utilisation needed for data transfer. It increased the transmission range from 50 to 200 meters.

3.1.1. Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE) is a wireless technology used to connect low energy devices. Therefore, BLE is oriented towards applications that spend less energy and have longer battery autonomy. BLE was introduced in 2010 as a part of Bluetooth 4, not as the upgrade but as a technology focused on Internet of Things applications (IoT) that transmit less data on lower frequencies. Therefore, BLE is not intended for the exchange of large amounts of data or listening to high quality music or streaming. BLE technology makes it possible to calculate distance between two devices from RSSI value of the BLE beacon. Every manufacturer that uses Bluetooth has its own Special Interest Group (SIG) identifier that makes it possible to isolate specific categories of Bluetooth devices like cars, personal computers, headphones etc.

3.1.2. Received Signal Strength Indicator (RSSI)

Received Signal Strength Indicator (RSSI) is the strength of the beacon's signal. The signal strength depends on distance, broadcasting power and obstacles like walls and/ or trees. At maximum broadcasting power, (4 dBm) RSSI radius stretches from -26 dBm (approximately 10 cm) to -100 dBm (40 to 50 m). The shorter the data-refreshing interval is (between 100 to 2000 ms), the more stable the signal is. It increases power consumption, i.e. battery life decreases [5, 6]. Formula for calculating distance (D = distance, M = measured power, N constant that depends on the environmental factor, range 2-4):

$$D=10^{\frac{(M - \text{RSSI})}{(10 \cdot N)}} \quad (1)$$

Based on the formula, if RSSI value is -69 dBm, a distance between two devices is one metre.

$$D = 10^{\frac{((-69\text{dBm}) - (-69\text{dBm}))}{(10 \cdot 2)}} = 1 \quad (2)$$

3.2. Geofencing

The term geofencing refers to services based on user location, i.e. when applications use data gathered via Global Positioning System (GPS), Radio Frequency Identification (RFID) or WiFi. Based on the data collected, it is possible to determine one's area of moving. Therefore, geofencing can be used as a way of preventing COVID-19. As far as safety is concerned when using geofencing, a special attention has to be given to user protection, i.e., to their privacy protection. In 2017, the state of Massachusetts made a consumer protection law that objected to the use of location-based advertising [7].

3.3. Exposure Notifications System (ENS) framework

Exposure Notifications System (ENS) is a service developed by Google and Apple in order to exchange anonymous keys. ENS offers two user levels/ statuses – infected user and potentially infected user. ENS marks infected users with positive COVID-19 diagnosis as “affected” and notifies users who are potentially at risk of being infected. Users, potentially at risk of being infected, receive an information on date and time of the contact, as well as on duration of the exposure to the virus. Android devices have to meet certain preconditions in order to use NES, i.e. they should run Android 6.0 or above and have Bluetooth turned on. Older Android OS versions should have location settings turned on, whereas on devices running Android 11 OS, location settings do not need to be on [8, 9, 10].

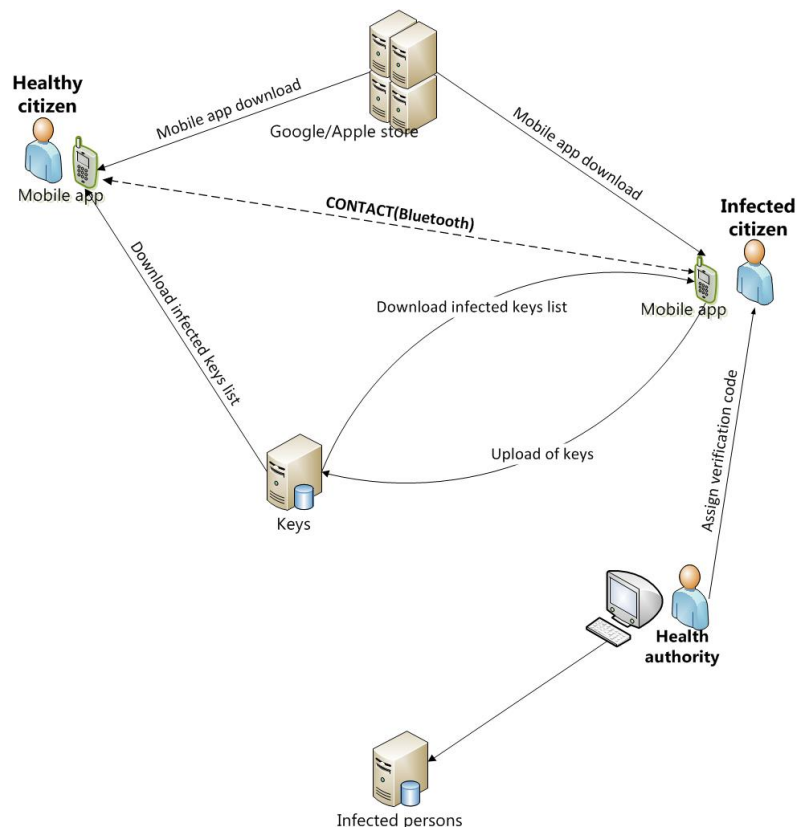


Fig. 2. ENS and “Stop COVID” application [11]

3.4. Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT/PEPP)

Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT/PEPP) is a centralised protocol designed to facilitate infected users' tracing. It was developed in cooperation between several European countries. PEPP-PT is based on Bluetooth BLE technology. After the user installs and turns on the application for a country with an integrated PEPP-PT solution, the application works in the background even when the phone is locked/ not active, and it sometimes sends temporary identifiers to the devices nearby via BLE.

signal. The server collects and processes data by calculating a distance and duration of exposure to the virus. It notifies the user about the possible exposure risk [12].

As far as privacy is concerned, PEPP-PT protocol has caused many controversies. Therefore, a petition for its removal was created. Over 300 hundred academics from 26 countries have signed it [13].



Fig. 3. German implementation of PEPP-PT model [12]

3.5. Decentralised Privacy-Preserving Proximity Tracing (DP-3T)

Decentralised Privacy-Preserving Proximity Tracing (DP-3T) is an open protocol created as an answer to PEPP-PT protocol. What they both have in common is the BLE technology usage. The only difference between them is that DP-3T prevents third parties from tracking users. Since data on users are not shared with third parties, DP-3T has many advantages as far as privacy is concerned than PEPP-PT protocol. On the other hand, DP-3T requires greater computer resources from the clients/users for processing data on the infection [14]. Apple and Google's protocol, ENS, is based on the similar principles as DP-3T protocol.

3.6. Temporary Contact Number (TCN) Strawman Protocol

Temporary Contact Number (TCN) Strawman Protocol is the first open source decentralised solution to tracing contacts with emphasis on the users' privacy. All devices running the protocol generate a random TCN, store it and broadcast it to devices nearby over Bluetooth. At the same time, the application receives and stores TCNs from nearby devices or health authorities acting on their behalf [22]. All users' applications, occasionally download a list of reported TCNs. Afterwards, they compare it with collected TCNs.

3.7. BlueTrace

BlueTrace is an open-source protocol for contact tracing via Bluetooth. It protects personal data and users' privacy. When two devices "meet" and fulfil certain parameters, they exchange messages containing temporary identifiers in case that one of the device owners has been potentially exposed to the virus. These identifiers rotate/ change very frequently to avoid user tracking. The user's encounter

history is stored locally on the user's device. None of the users can access a part referring to health authorities. If a user is infected or a subject to contact tracing, they will be asked to share their contact history with health authorities in charge. Only health authorities can see the encrypted contact history and use it for contact tracing. BlueTrace is designed to upgrade manual contact tracing by solving its key limitation – an infected person can report only the contacts they have met. In that way, a possible abuse, i.e. intentional, false contact reporting could be avoided. BlueTrace also enables scalable contact tracing, i.e. it needs less resources [14].

3.8. Whisper Tracing Protocol

Whisper Tracing Protocol (WTP) and Coalition App were presented on April 16th, 2020. They enable a centralised or decentralised model of working. The protocol is based on Bluetooth and BLE technologies. The interaction between the users is stored locally (decentralised), and/ or on a third party's server (centralised) if the user has allowed it. All data is encrypted no matter the place of storage, which increases users' privacy protection.

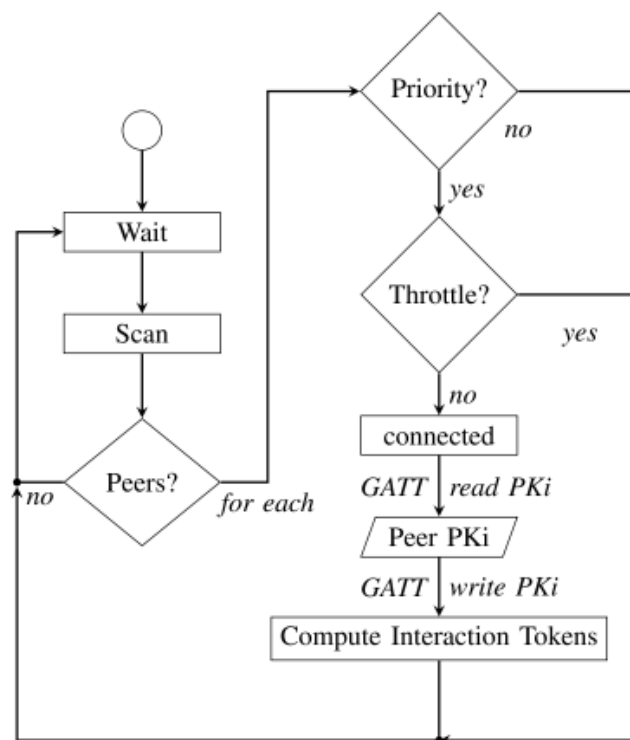


Fig. 4. Interaction, scanning and connecting via Bluetooth Whisper Tracing Protocol [24]

When scanning its surroundings via Bluetooth technology, Whisper Tracing Protocol has periodic scan set on two timers. The first one shows a duration of one scan whereas the other shows time between two cycles of scanning. If the second timer is set on shorter time of scanning, contact tracing will be more frequent. However, it will affect battery life. After the scanning, the protocol will compare device identities and reject the unnecessary ones, like cars. It accepts other devices and gives them a priority in order to avoid double connections. When the protocol encounters a priority device, it checks whether public keys were exchanged with other devices. Afterwards, it fills in data base with Tokens, Ping, Connect, UserKeyPair and Whisper Events Tables. When the tables are filled in, the timer of waiting between scans is activated and new scan is initiated (Figure 4):

- Tokens Table: Contains all unique interactions together with time. It erases all interactions older than three weeks.
- Ping Table: Contains all device addresses. It hashes them to provide privacy.

- Connect Table: Contains all the public keys received as well as time.
- UserPairKey Table: Records the user's own keys.
- WhisperEventTable: Tracks all scans and the number of users encountered at every scan.

4. APPS' SECURITY ASPECT

Possible security flaws will be discussed in this chapter in order to give an insight into problems of the existing solutions to apps and technologies. Limitations to (malevolent) users who create more (fake) accounts, their fake impersonations (as COVID-19 positive or negative users) pose a security risk that should be given more attention to. As far as user privacy is concerned, data the applications collect can be divided into the following categories:

- User's location history,
- User's contacts (when and where),
- If the user was infected,
- If the user received a notification on a contact with an infected person.

A possible problem with BLE technology could be repetition of identifiers the users share with other users. This situation could lead to false positive or negative reports on user's condition and it could "contaminate" the whole network of contacts. If such a malevolent action is automated, Sybil Attack is created. In order to prevent Sybil Attack, it is advisable to use Proof of Work (PoW) algorithm that is used in Bitcoin network [15].

As far as user privacy is concerned, it was advised to use decentralised application model to fight COVID-19. With decentralised model, every user saves and processes data on their device. Therefore, a possibility of data manipulation and collecting users' data is reduced. Most of the applications use Bluetooth BLE technology, which, when using Media Access Control (MAC) address makes it possible to find out user's identity. Furthermore, although it is possible to change it, this creates more security problems and questions the efficiency of the application based on such approach. Centralised approach collects data that can be processed without the user's knowledge and based on users actions it can create a model to show ads, predict actions etc. Some Asian countries have collected data on their users' activities via mobile telecommunication networks, under the COVID-19 excuse, in cooperation with the teleoperators and without users' consent. Based on data collected they send SMS messages to users informing them that they should be quarantined with police supervision. Upon receiving such a message, users get a defined area of movement (geofencing), i.e., they cannot leave the area without the authorities' consent.

5. EXISTING APPLICATIONS

The existing applications can be divided in two groups, official (supported by authorities) and unofficial (private persons or companies' applications). Official applications have more downloads than unofficial ones, although even they are not well accepted by users. All the applications that use Apple and Google services (ENS API), exchange anonymous keys. European Commission and members of the European Union have still not agreed on the interoperability rules. Therefore, it is impossible to get a notification that a user of some other, similar application has been infected.

5.1. Stop COVID-19

Stop COVID-19 is an application developed by the Government of Croatia and Ministry of Health. The purpose of the application is to slow down COVID-19 spread. The application itself is based on decentralised approach to data processing. ENS API created in the Google-Apple cooperation gives anonymous keys. ENS API is based on Bluetooth BLE technology [11].

5.2. Hamagen

Hamagen is a centralised application solution created for the Israeli Ministry of Health. This application is very popular with users, it has two millions of downloads which makes one-fifth of the total population of Israel. As far as privacy is concerned, the application has created many controversies, i.e. there is a possibility to track users for military purposes in the Gaza Strip [17].

5.3. Google Sodar

Google Sodar is a tool that uses augmented reality to help following physical distancing rules when leaving home. It is an experimental project which creates a two-meter radius ring (six feet) around user, shown on the mobile monitor. The scope of the tool is to visualise the distance so that the user could adapt to keeping physical distance [18].

5.4. Check your mask

Check your mask is an application made in France. It uses camera to check if a mask is worn correctly. Such a technology could be applied at the entrances of shopping centres, underground and other open or closed spaces with many people in it. It could help people wearing the mask for the first time or the children and the elderly.

5.5. Queue Saver

Queue Saver is an application intended to prevent queues and crowds in banks, hospitals, shops etc. The user scans QR code and receives the number so that they can withdraw from the potential crowd. When their turn is to enter, they receive a notification. Such a principle could be applied to fight against COVID-19 [19].

5.6. Corona DataSpende

Corona DataSpende is a smartwatch application created in Germany to track COVID-19. The application uses a smartwatch or fitness bracelet to collect data like pulse, body temperature or sleeping habits. All data collected are processed and released online. Such an approach gives insight into general conditions and possible focus of infection.

5.7. Symptom Tracking App

Symptom Tracking App is a sort of a questionnaire the user uses to check their health if they suspect they could be infected. Majority of these applications share their data with health authorities in order to give their contribution to the fight against COVID-19 [20].

5.8. COVID-19 Quarantine Monitor

COVID-19 Quarantine Monitor is Indian response to fight against COVID-19. The application is centralised solution that collects data via Bluetooth and GPS. It processes data on server and notifies users if they were exposed to infection. India has more than 10 applications of this type and, altogether, they have more than 100 million downloads.

5.9. World Health Organization COVID-19 App and Coalition App

WHO COVID-19 App is an attempt of the World Health Organisation to create a global app to track COVID-19. As far as contact tracing is concerned, the application was not that accepted, so it was given up. WHO COVID-19 App is not the only app intended to work on global level. Coalition App was also intended for the global usage; however, it is not well accepted. It uses WTP that enables privacy and user security.

5.10. Usage overview of applications used to track COVID-19

The application has no purpose if it is not used. It is supposed that an application is successful if the number of users in a country is 40 to 60% of the population. In most of the countries, the usage of such applications is voluntary. However, there are countries, like Qatar, where one can be punished with three years in prison or 55 000-dollar fine for not using the application. At the moment, the numbers showing the app's adoption in the population are rough estimate. They are based on the number of people living

in a country and the number of downloads within a population older than 14. Furthermore, most of the statistic data do not include China since it does not have a standalone contact tracing application. In China, contact-tracing features are a part of the existing applications like AliPay and WeChat which are widely used there [25].

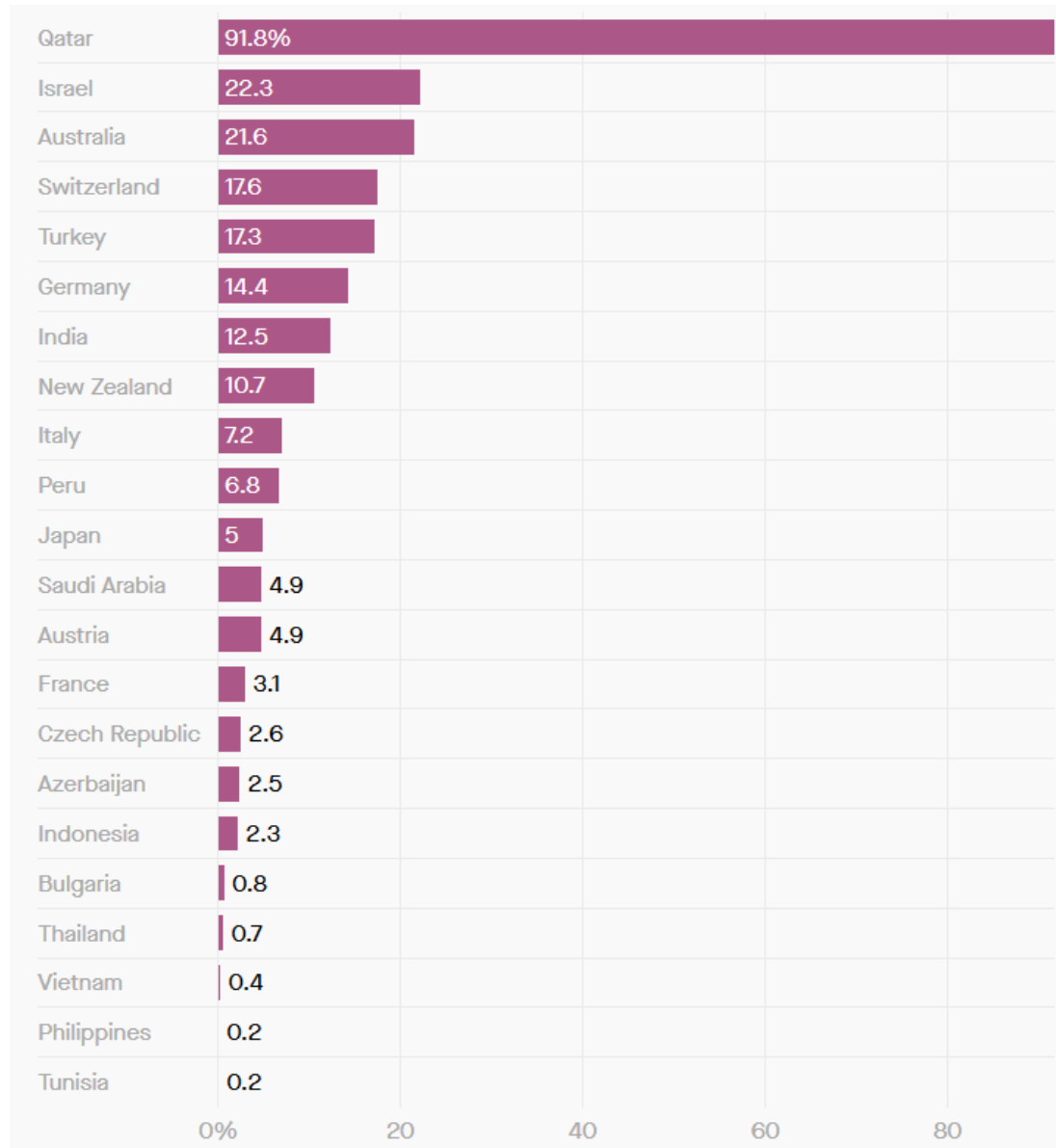


Fig. 5. Distribution of app users in countries [25]

6. CONCEPTUAL MODEL OF APPS USED TO FIGHT COVID-19

On the basis of the existing apps' characteristics and in order to increase safety and privacy, it is possible to propose an advanced app concept. Such a concept should facilitate physical distancing without saving and sharing data with third parties. Bluetooth and BLE technology (it should work on at least Bluetooth v4.0) make it possible to search for nearby devices every 250ms. After eliminating unwanted categories via SIG identifier (computers, cars, headphones etc.), a distance could be determined by determining the RSSI signal's strength. If a device was identified in the user's surroundings, the user would be notified of it via sound notification, vibration, and sign on the screen.

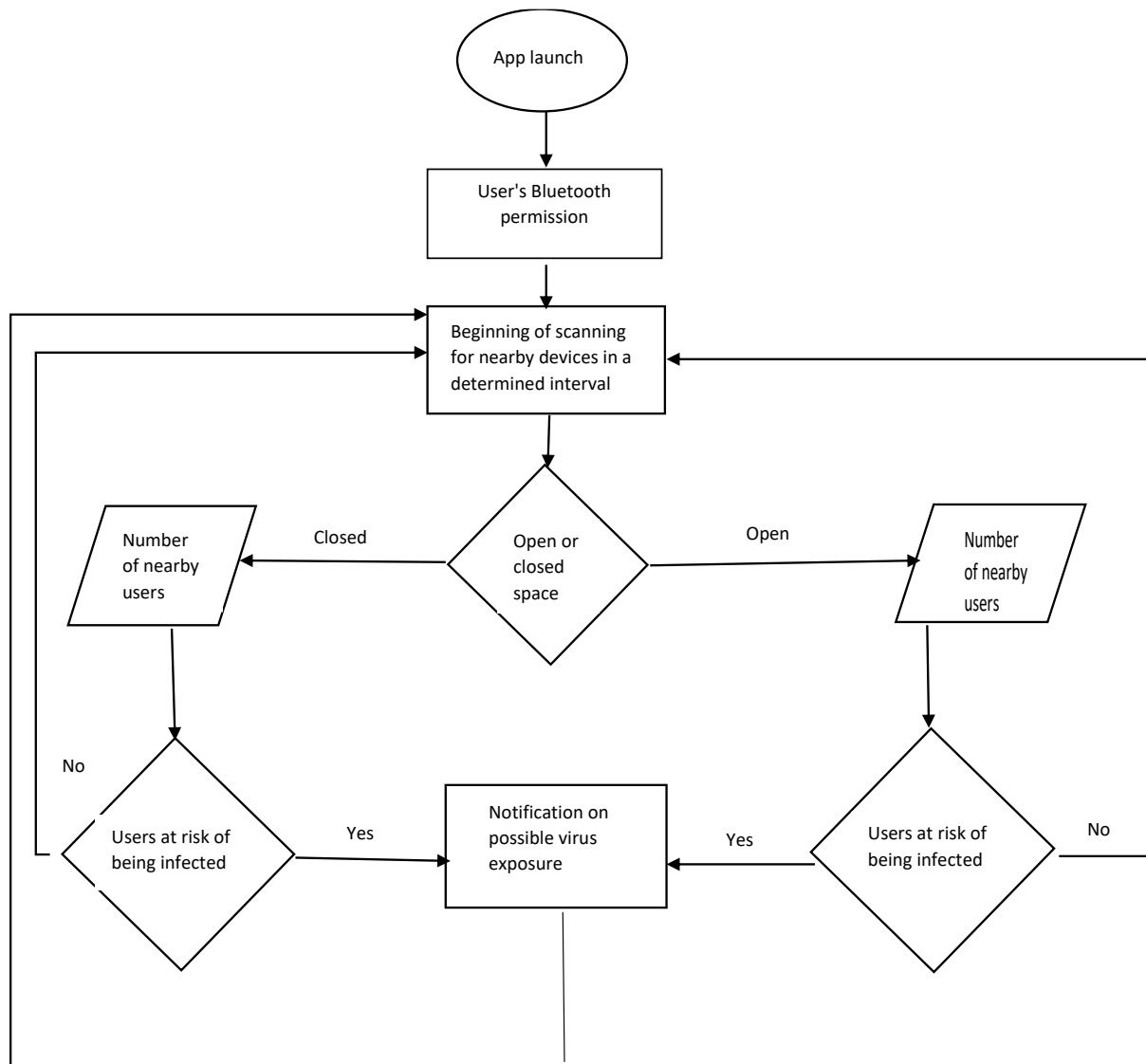


Fig. 6. Bluetooth part of the application

It would be possible to integrate the news on COVID-19 into the app. The news would be refreshed when opening them or automatically (e.g. every five minutes). The app would download the statistics on the number of infected people as well as the interactive chart based on the statistics. Statistics and news are downloaded from third parties app called RestApi. If a person suspects to be infected, they could use Symptom-Tracker in the form of a questionnaire to check what to do next. If a user has symptoms, they could get phone numbers of health authorities that do COVID-19 tests or of a family doctor. According to the symptoms shown in the Table 1, the application could also contain the questionnaire.

Symptoms and signs	COVID-19 (disease caused by SARS-CoV-2)
Beginning	First week – mild, second week - serious
High temperature	>38 °C (45,4 %)
Headache	70,3 %
Loss of smell	70,2 %
Muscle pain	62,5 %
Fatigue	63,3 %
Cough	Dry (63,2 %)
Runny nose	60,1 %
Stuffy nose	67,8 %
Sore throat	52,9 %
Breathing	Shortness of breath (19 %)
Diarrhoea	4 % (older persons)
Nausea	5 % (older persons)

Table 1. Symptoms of COVID-19

It would be possible to choose, in settings, an option keeping physical distance in open or closed spaces. The option “Open space” implies keeping 2 m physical distance with a maximum of 7 persons in radius of 5 metres (Geofencing). The option “Closed space” implies keeping 1 m physical distance with a maximum of 5 persons in radius of 3 metres. The application should run in the background, and if some of the physical distancing rules were broken, the application would send sound notifications. As far as security is concerned, the application should enable user’s privacy. When using Bluetooth to scan the surroundings, it is possible to reveal user’s true identity. In that case, MAC Bluetooth randomizer should be used.

7. CONCLUSION

Current COVID-19 situation would definitely, be better controlled by using technology in order to stop its spread. The optional solution to that problem is a mobile app used in cooperation with health authorities. Since technological solutions are not well adopted by majority of the population, it is necessary to educate people to see the advantages of the contemporary technological solutions. Furthermore, a special attention has to be given to collecting personal data, especially to data whose collecting is not entirely regulated by law. In countries, members of the European Union, data collecting has to be in accordance with The General Data Protection Regulation (GDPR) no matter the scope of data collecting. Developing a global, well-accepted application could facilitate the fight against COVID-19 and could be used as the basis for some, similar future situations.

REFERENCES

1. Zastrow M 2020, *Coronavirus Contact-Tracing Apps: can they slow the spread of COVID-19?*, Nature, accessed October 1st 2020, <<https://www.nature.com/articles/d41586-020-01514-2>>
2. Holmes O 2020, *Israel to track mobile phones of suspected coronavirus cases*, The Guardian, accessed October 1st 2020, <<https://www.theguardian.com/world/2020/mar/17/israel-to-track-mobile-phones-of-suspected-coronavirus-cases>>

3. Abate T 2020, *Stanford researchers help develop privacy-focused coronavirus alert app*, Stanford News, accessed October 1st 2020, <<https://news.stanford.edu/2020/04/09/stanford-researchers-help-develop-privacy-focused-coronavirus-alert-app>>
4. Google Developers – Android, *Bluetooth overview*, Google Inc., accessed October 1st 2020, <<https://developer.android.com/guide/topics/connectivity/bluetooth>>
5. Bluetooth SIG, Inc., *Enhancing Bluetooth Location Services with Direction Finding*, accessed October 1st 2020, <https://www.bluetooth.com/wp-content/uploads/2019/03/1901_Enhancing-Bluetooth-Location-Service_FINAL.pdf>
6. IoT and Electronics 2016, *How to Calculate Distance from the RSSI value of the BLE Beacon*, accessed October 1st 2020, <<https://iotandelectronics.wordpress.com/2016/10/07/how-to-calculate-distance-from-the-rssi-value-of-the-ble-beacon>>
7. White SK 2017, *What is geofencing? Putting location to work*, CIO, IDG Communications, Inc, accessed October 1st 2020, <<https://www.cio.com/article/2383123/geofencing-explained.html>>
8. Android Help, *Use the COVID-19 Exposure Notifications System on your Android phone*, Google Inc. accessed October 1st 2020, <<https://support.google.com/android/answer/9888358>>
9. *Privacy-Preserving Contact Tracing*, Apple Inc., Google Inc., accessed October 1st 2020, <<https://covid19.apple.com/contacttracing>>
10. *Exposure Notifications: Using technology to help public health authorities fight COVID-19*, Google Inc., accessed October 1st 2020, <https://www.google.com/intl/en_us/covid19/exposurenotifications/#exposure-notifications-and-privacy>
11. Government of Republic of Croatia, Ministry of Health, *Stop COVID-19 Hrvatska 2020*, accessed October 1st 2020, <<https://github.com/Stop-COVID-19-Croatia/stopcovid19-docs>>
12. Pan-European Privacy-Preserving Proximity Tracing 2020, viewed October 1st 2020, <<https://github.com/pepp-pt/pepp-pt-documentation/blob/master/PEPP-PT-high-level-overview.pdf>>
13. Der Spiegel 2020, *Den Tracing-App-Entwicklern laufen die Partner weg*, DER SPIEGEL GmbH & Co. KG, accessed October 1st 2020, <<https://www.spiegel.de/netzwelt/apps/pepp-pt-in-corona-krise-den-tracing-app-entwicklern-laufen-die-partner-weg-a-017f50eb-c1e2-4097-8182-53708ca6db59>>
14. Bay, J et al. 2020, *BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders*, Government Technology Agency Singapore accessed October 1st 2020, <https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf>
15. Sybil Attack 2019, GeeksforGeeks, accessed October 1st 2020, <<https://www.geeksforgeeks.org/sybil-attack>>
16. Mathieson, SA 2005, 'Mobile phone tracking threatens privacy', *Network Security*, vol.3, 2005., pp.19-20
17. Stub ST 2020, *Israeli Phone Apps Aim to Track Coronavirus, Guard Privacy*, U.S. News, accessed October 1st 2020, <<https://www.usnews.com/news/best-countries/articles/2020-04-20/new-tech-apps-in-israel-aim-to-track-coronavirus-guard-privacy>>
18. Shankar B, 2020, *Google's 'Sodar' AR tool helps you measure social distancing*, accessed October 1st 2020, <<https://mobilesyrup.com/2020/05/28/google-sodar-tool-social-distancing-covid-19-pandemic>>
19. Queue Saver, *Keep your customers safe while they wait in line*, Andromeda LLC, accessed October 1st 2020, <<https://queuesaver.com/how-it-works>>

20. Snaith, B & Tennison, J 2020, *Spot the difference – explaining the Covid-19 apps*, accessed October 1st 2020, <<https://theodi.org/article/spot-the-difference-explaining-the-covid-19-apps>>
21. *Blog zur wissenschaftlichen Auswertung der Corona-Datenspende-App*, Robert Koch Institut, accessed October 1st 2020, <https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Corona-Datenspende.html>
22. Ronacher, A 2020, *Temporary Contact Number based Contact Tracing*, Armin Ronacher's Thoughts and Writings, accessed October 1st 2020, <<https://lucumr.pocoo.org/2020/4/9/tcn-contact-tracing>>
23. Hammoudi, K, Cabani, A, Benhabiles H & Melkem M 2020, Validating the Correct Wearing of Protection Mask by Taking a Selfie: Design of a Mobile Application “CheckYourMask” to Limit the Spread of COVID-19, *Computer Modeling in Engineering & Sciences*, vol.124, no.3, pp. 1049-1059, <<https://www.techscience.com/CMES/v124n3/39927/pdf>>
24. Loiseau, L et al. 2020, *Whisper Tracing Version 3 - an open and privacy first protocol for contact tracing*, accessed October 1st 2020, <<https://docsend.com/view/nis3dac>>
25. Rivero, N 2020, *Global contact tracing app downloads lag behind effective levels*, accessed October 1st 2020, <<https://qz.com/1880457/global-contact-tracing-app-downloads-lag-behind-effective-levels>>