

# Contact Tracing in the Context of COVID-19

DR. ANITA HARSOOR<sup>1</sup>, AKKANAGAMMA<sup>2</sup>, DIVYA<sup>3</sup>, K CHAITRA<sup>4</sup>

<sup>1, 2, 3, 4</sup> Dept of Computer Science and Engineering, Poojya Doddappa Appa College of Engineering, Kalaburagi

**Abstract—** *The COVID-19 pandemic has spread with increased fatalities around the world and has become an international public health crisis. Public health authorities in many countries have introduced contact tracing apps to track and trace infected persons as part of measures to contain the spread of the Severe Acute Respiratory Syndrome Coronavirus. However, there are major concerns about its efficacy and privacy which affects mass acceptance amongst a population. Even with the vaccination campaigns being carried out largely, the Covid cases are still increasing & the death toll is rising every day. It is very difficult to detect & identify a Covid infected person initially as the person will not show any symptoms and by the time it gets detected, the carrier would have already made contact with many people. It is very important to detect & identify the contacts made by the virus carrier at the very beginning to break this chain.*

**Indexed Terms—** *Registration phase, Registering Encounters, Contacts Information, Upload.*

## I. INTRODUCTION

Coronavirus is a large group of viruses causing human respiratory infections that might lead to severe diseases. COVID-19 virus, a type of coronavirus, was discovered in 2019 in Wuhan, China [1]. It is mainly transmitted through droplets generated when an infected person coughs, sneezes, or exhales. The outbreak of COVID-19 is affecting communities, businesses, organizations, and the global economy, resulting in shortages of many goods in markets around the world. According to World Health Organization (WHO) reports, this pandemic has triggered an unprecedented need for digital health technology solutions for population screening, tracking the infection, prioritizing the use and allocation of resources, and designing targeted responses [2,3]. COVID-19 had immense effects on society's health and everyday life. Tasks like attending the workplace or meeting friends somewhere were once unremarkable, but suddenly became difficult without applying precautions advised by WHO, such

as social distancing, frequent hand washing, and wearing masks regularly [4]. Contact tracing emerged as a public health tool to battle and control the spread of infectious disease by identifying and monitoring people who were in close contact with an infected person. Contact means to be within 1 m of a confirmed COVID-19 case for more than 15 min, to have physical contact with an infected person, or to provide care for COVID-19 patients without protective equipment within 2 days before the onset of disease and 14 days afterward [5]. In the case of COVID-19, confirmed contacts are required to quarantine for 14 days from the last point of exposure and to be monitored by health officials [6]. Contact tracing requires the collection and storing of contacts' personal and private data, including name, address, date of birth, relationship with the source case, and contact frequency and duration. Data protection is an essential part of this process. People's information must be protected during data collection, storage, and management. As life has gone on, people have needed to communicate and engage with other people in different areas for various reasons throughout their day. In those circumstances, preventing the spread of COVID-19 by only applying manual contact tracing and protection measures was not enough to mitigate the virus.

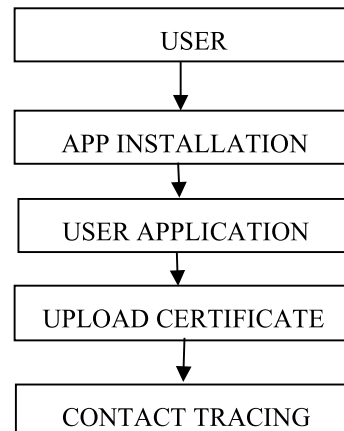


Figure 1: Block Diagram

Bluetooth-based solutions Currently, many applications, such as Tabaud, Alhosn UAE, and BeAware, use Bluetooth technologies. Bluetooth based contact-tracing apps use a wireless technique to detect the smartphones of nearby positive diagnosed cases that have Bluetooth activated in their app. The technology emits Bluetooth Low Energy (BLE) “chirps” and sustains a database exchange mechanism by recording a pseudorandom bit sequence emitted by the chirping smartphones, along with the estimated power of the chirp's delivery [7]. The BLE protocol allows the app to exchange a small amount of data with peers regularly, but communication with the server relies on traditional secure application protocols, e.g., Hypertext Transfer Protocols Secure (HTTPS). The impact on battery utilization for these protocols is related to the number of information exchanges [8].

GPS is a location-passed tracing tool. This tool is used to locate or trace people to identify individuals who have been exposed to or infected with COVID-19. Using GPS signals, an application will collect and record user movements as coordinates with a timestamp. The application looks for matches in a multidimensional grid of longitude, latitude, and time [09]. The system is composed of a user device that sends the location and a server that stores and encrypts the data. GPS is mostly used to enforce a quarantine on COVID-19 patients with an application that would highlight areas where a high number of COVID-19 cases are located. GPS location tracking requires the users to always have their phone charged and working, with location tracking enabled [10].

#### How Contact Tracing Apps Work

While contact tracing apps take the guesswork out of identifying where people were and when, they still rely on people manually entering information about their condition and the onset of any COVID-19 symptoms. Here's a basic idea of how contact tracing apps work:

1. Users download the app. Bluetooth must be turned on and left on.
2. Phones with the app can exchange anonymous keycodes when they're within a close range.
3. If a user develops COVID-19like symptoms, they'll log them in the app and answer any related questions. They will also log when and if they are diagnosed with COVID-19.

4. Anyone who came into close contact with this person within the last two weeks will be alerted of potential COVID-19 exposure.

## II. METHODOLOGY

This system is used for contact tracing and notifying people with users around them. This application built in the android studio platform and for the data storage Firebase is used.

It's an Android focused IDE, designed specially for Android development. It was launched on 16th May 2013, during Google's I/O 2013 event. Android studio contains all the Android SDK tools to design, test, debug and profile your app. By looking at the development tools and environment, we can see its similar to Eclipse with the ADT plug-in, but as I have mentioned above, it's an Android focused IDE, and there are many cool features available in Android Studio that can foster and increase your development productivity.

One great thing is that it depends on the IntelliJ Idea IDE, which has proved itself to be a great IDE and has been in use by many Android engineers.

Firebase: The Firebase Realtime Database is a cloudhosted database. Data is stored as JSON and synchronized in realtime to every connected client, with cross-platform support for iOS, Android, Web and more.

### ALGORITHM

This app is divided into modules where the user will interact with all the modules.

1. REGISTRATION PHASE
2. REGISTERING ENCOUNTERS/
3. CONTACTS INFORMATION
4. UPLOADING ENCOUNTERS DATA

#### 1. REGISTRATION PHASE

The steps required to register a user in a centralised architecture. A user downloads the app (steps 1 and 2) and registers details such as name, mobile phone number, age, and postcode with the server (step 3).

The server verifies the mobile number by sending a One Time Password (OTP) by SMS (steps 4 and 5).

Upon verification, the server computes a TempID

(step 6), which is only valid for a short time (Bluetrace recommended expiry time is 15 min). The TempID and the expiry time are then transmitted to the user's app.

For the age we are using the datepicker method the dependency is implementation 'com.google.android.material:material:1.5.0'.

For the firebase authentication means for the otp generation and checking the otp dependencies will be

implementation 'com.google.firebase:firebaseauth:19.3.2'

## 2. REGISTERING ENCOUNTERS/CONTACTS INFORMATION

Once a user comes in contact with another app user, they exchange an "Encounter Message" using Bluetooth, as presented in Figure . An encounter message comprises the exchange of TempID, Phone Model, and Transmit Power (TxPower) (steps 1 and 3). Each device also records the Received Signal Strength Indicator (RSSI) and the timestamp of the message delivery (steps 2 and 4). Note that phone numbers are not included in these messages. Since the TempIDs are generated and encrypted by the server they do not reveal any of the app user's personal information. Thus, both app users have a symmetric record of the encounter that is stored on their respective phones' local storage. The protocol uses a temporary blacklist to avoid a user registering duplicated contacts. Thus, once a user receives an Encounter Message, the app automatically blacklists the sender for a short time.

Permissions will be enabled by using these modules in the AndroidManifest.xml.

```
<uses-permission
android:name="android.permission.
ACCESS_FINE_LOCATION" />
<uses-permission
android:name="android.permission.
ACCESS_COARSE_LOCATION" />
<uses-permission
android:name="android.permission.
BLUETOOTH" />
<uses-permission
android:name="android.permission. INTERNET" />
```

```
<uses-permission
android:name="android.permission.
READ_EXTERNAL_STORAGE" />
```

## 3. UPLOADING ENCOUNTERS DATA

All encounter records are stored locally and are not automatically uploaded to the server. Figure shows the application flow when a user tests positive for COVID-19 (step 1). The health official confirms whether the user has the tracing app installed, and flags the user as infected (step 2). The encounter data upload is voluntary. If the user agrees to upload the data, the health official sets this up in the back-end server, and the server generates an OTP for verification (step 3). Once verified, the encounter data is uploaded to the server(step4).

For uploading the data and saving the files in firebase we use

implementation 'com.google.firebase:firebasedatabase:20.0.4'

implementation 'com.google.firebase:firebasestorage:20.0.1'

## III. RESULTS

Android app permissions can give apps control of your phone and access to your camera, microphone, private messages, conversations, photos, and more. App permission requests pop up the first time an app needs access to sensitive hardware or data on your phone or tablet and are usually privacy-related.

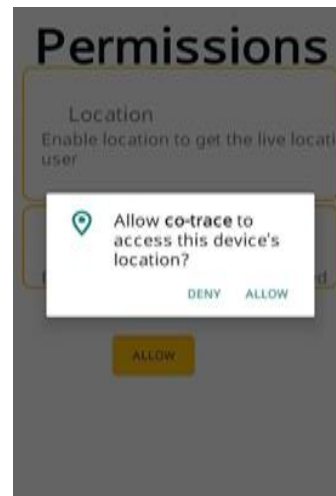


Figure 2: Permissions

User Verification ensures that users provide accurate information. When enabled, users will have to provide a valid email address, otherwise they won't be able to list items. Admins can also set up a one-time or recurring verification fee that can be credited, at a later date, to the user's account. User Identity Verification is a security measure that verifies that all requests made from within your app or Web Chat widget are coming from authentic end users.

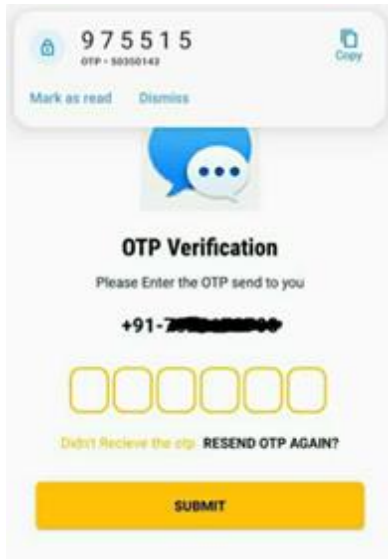


Figure 3: OTP Verification

A home page is generally the primary web page which a visitor navigating to a website from a search engine will see, and it may also serve as a landing page to attract visitors. Home page contains all the areas of the application. This application contains mainly of four areas – health status, upload certificates, news updates, tracing of covid patients. Health status includes the status of your health and it asks for the updates of your health and advise on the same for user. Upload certificates includes, if the user is tested positive, they can upload their certificates in the given file location upload. News updates includes the updates of the daily news of covid-19 In the world. Tracing is nothing but the tracing of the covid positive patients in the surrounding place

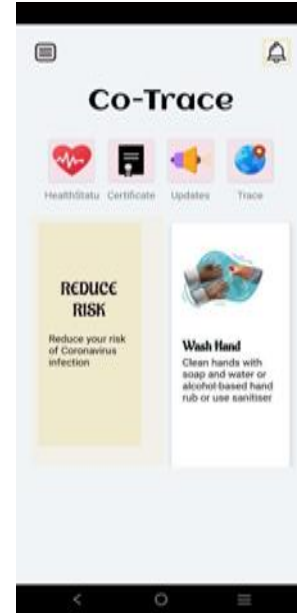


Figure 4: Home Page

Uploading certificate is the process of uploading or providing the information about the status of your health to the remaining users of the application. Once the user is tested positive, there is an option to upload their certificates and let the other users know about the present situation of the person. It will be very useful to the users to safeguard themselves. Using the uploaded certificates, users can prevent themselves from being covid positive.



Figure 5: Upload Certificate

#### IV. CONCLUSION

This system can be used by any User who wants to be aware of Covid 19 Situation & wants an app to alert him. Finally, in the analysis of this systematic literature review, recommendations to address these challenges, future directions, and considerations in the use of digital contact tracing apps and related technologies to contain the spread of future pandemic outbreaks are presented. We highlight recommendations to improve the willingness to use such digital technologies and could facilitate mass acceptance amongst users. With support from national governments, these technology applications serve as an alert system for enabling rapid contact tracing and notification as well as mass reach to the population.

#### REFERENCES

- [1] Nadeem Ahmed, Regio A. Michelin, Robert Malaney, Salil S. Kanhere, Aruna Seneviratne, Wen Hu, Helge Janicke, Sanjay K. Jha, Sushmita Ruj, Wanli Xue , “A survey of covid19 contact tracing app” , Volume: 8 , IEEE ,20 July 2020 , 134577 – 134601.
- [2] Burki T.K. Coronavirus in China. *Lancet Respir. Med.* 2020;8(3):238. doi: 10.1016/S2213-2600(20)30056-4.
- [3] Tania Martin, Georgios Karopoulos, José L. Hernández-Ramos, Georgios Kambourakis, Igor Nai Fovino, “Demystifying covid-19 digital contact tracing”, Hindawi, European Commission, Joint Research Centre, Ispra 21027, Italy, Volume 2020, 27 Oct 2020.
- [4] Nasro Min-Allah, Bashayer Abdullah Alahmed , Elaf Mohammed Albreek , Lina Shabab Alghamdi , Doaa Abdullah Alawad , Abeer Salem Alharbi , Noor Al-Akkas , Dhiaa Musleh , Saleh Alrashed , “ A survey of COVID19 contact-tracing apps”, pumed, 21 Aug 2020.
- [5] Jonatan Almagor, Stefano Picascia , “Exploring the effectiveness of a COVID-19 contact tracing app using an agent-based model”, pubmed, 2020 Dec 17.
- [6] Simon Munzert, Peter Selb, Anita Gohdes, Lukas F.stoetzer, “Tracking and promoting the usage of a COVID19 contact tracing app”, *Nature Human Behaviour*, 21 January 2021.
- [7] Lai C.-C., Shih T.-P., Ko W.-C., Tang H.-J., Hsueh P.-R. Severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) and coronavirus disease-2019 (COVID-19): the epidemic and the challenges. *Int. J. Antimicrob. Agents.* 2020;55(3):105924. doi: 10.1016/j.ijantimicag.2020.105924
- [8] Hatke G.F. 2020. Using Bluetooth Low Energy (BLE) Signal Strength Estimation to Facilitate Contact Tracing for COVID-19; pp. 1–12. arXiv. 1.
- [9] Ahmed N. A survey of COVID-19 contact tracing apps. *IEEE Access.* 2020; 8:134577–134601.doi: 10.1109/ACCESS.2020.3010226.
- [10] Dar A., Lone A.H., Zahoor S., Khan A.A., Naaz R. Applicability of mobile contact tracing in fighting pandemic (COVID-19): issues. challenges and solutions. 2020.
- [11] Wen H., Zhao Q., Lin Z., Xuan D., Shroff N. vol. 335. *LNICST*; 2020. A study of the privacy of COVID-19 contact tracing apps.