

Overview of Aarogya Setu Application

Shweta Devidas Kedare¹

¹Shweta Devidas Kedare, Department of Master of Computer Application, ASM IMCOST, Maharashtra, India

Abstract - The app - Aarogya Setu, which means "bridge to health" in Sanskrit -It is an Indian app which was launched on April 2nd 2020, by Indian government. It is designed as a Coronavirus, or COVID-19 contact tracing app that uses the Bluetooth and location technology in phones to note when you are near another user who also uses the Aarogya Setu app. In case someone you have come in close proximity to is confirmed infected, you are alerted.

The app alerts are produced by instructions on how to self-isolate and what to do in case you develop symptoms.

Basically this app gives basic information about Covid-19, including hygiene and social distancing protocols. It also has details of how one could donate to the prime minister's coronavirus-specific relief fund, PM-Cares.

India has made it mandatory for government and private sector employees to download it But users and experts in India and around the world say the app raises huge data security concerns.

KeyWords: security, data, private, information, COVID-19, technology, location, bluetooth, proximity, etc.

1. INTRODUCTION

Since the risk of COVID-19 started increasing in India so, The government of India decided to launch the application, name Aarogya Setu, which was intended to monitor the ratio of COVID-19 patients in India .This app is an updated version of an earlier app called Corona Kavach (now discontinued) which was released earlier by the Government of India.

Aarogya Setu App is an India's main contact tracing technology, was launched on April 2nd 2020. The app was developed by the National Informatics Centre under the Ministry of Electronics & Information Technology.

According to NITI Aayog CEO Amitabh Kant, it has become the world's fastest app to reach 50 million downloads in just 13 days.

The app is there on both Google Play (for Android phones) and Apple App Store (for iOS). It is available in 11 languages — 10 Indian languages (Marathi, Hindi, Tamil, Telugu, Kannada, Malayalam, Panjabi, Bengali, Odia, Gujrati) and English. The size of Aarogya Setu app is 4.0MB(Android App)

The purpose of this app is to spread awareness of COVID-19 and to connect important COVID-19 related health services to the people of India. Basically an Aarogya Setu app is an Indian open-source, which is written in Kotlin and Java language. It's a COVID-19 "Contact tracing, Self-assessment and syndromic mapping", primarily a digital service mobile app.

Once you download the app, it will insist you to provide some important, personal and sensitive information which is related to you such as:

1)Mobile Number

(Initially, user has to enter their mobile phone number, verified with a one-time password.)

2)Full name

3)Age

4)Gender

5)Travel history

6)Known contact with a coronavirus patient

7)Smoking habits.etc.

After installing the app, you have to switch on Bluetooth (you are recommended to keep it on at all times) and Location. Then, set 'location sharing' to 'Always' (you can change this anytime later).

1.1 How does it work?

Basically it is a tracking app which uses the smartphone's GPS and Bluetooth features to track the coronavirus infection.

With Bluetooth, it tries to determine the risk if one has been near (within six feet of) a COVID-19 - infected person, by scanning through a database of known cases across India. Using location information, it determines whether the location one is in belongs to one of the infected areas based on the data available.

"If you have met someone in the last two weeks who has tested positive, the app calculates your risk of infection based on how recent it was and proximity, and recommends measures.

After accepting all this information, the data is then shared with the government.

1.2 Features

Aarogya Setu app helps user by providing information related to following aspects:

- 1) Tells the risk of getting COVID-19 for the user
- 2) Helps the users identify COVID-19 symptoms and their risk profile
- 3) Gives updates on local and national COVID-19 cases
- 4) If applied for E-pass, it will be available
- 5) It also gives information about how many COVID-19 positive cases are there in a radius of 500 m, 1 km, 2 km, 5 km and 10 km from the user.
- 6) The app is built on a platform that can provide an Application Programming Interface (API) so that other computer programs, mobile applications, and web services can make use of the features and data available in Aarogya Setu.

2. Problem Statement:

- 1) The Narendra Modi government launched the Aarogya Setu. The app is meant to alert users if they have come in contact with a Covid-19 positive patient, and what measures they need to take in case that happens. But cybersecurity experts worry that Aarogya Setu could violate its users' privacy and be a surveillance tool in the hands of the government.
- 2) Despite glaring flaws, prime minister Modi recommended that citizens should download this app, also India has made it mandatory for government and private sector employees to download it. where as several government agencies have also been spreading awareness about Aarogya Setu through different social media and other channels. But users and experts in India and around the world say the app raises huge data security concerns.
- 3) The data collected by Aarogya Setu is stored both on the device and on central servers. And while the terms of service say that digital records of time of user contact will be deleted in 30 days, but not to anonymised and aggregated data sets. This means that encrypted user data on its own servers could last beyond the purposes of tracing coronavirus. reports states that user data can be held longer for purposes for which the information may lawfully be used. As a result there is a risk the personal information of users may be held for the duration of this public health crisis and beyond
- 4) Data collected through the app it suppose to be used by the country's health ministry, but the committee that designed India's app lacks any representation from the ministry of health and family welfare, or any independent involvement of persons with a medical or epidemiological background, according to the Internet Freedom Foundation paper.
- 5) As Aarogya Setu's privacy agreement leaves it open for the government to repurpose this data for its other agencies, which is extremely risky in terms of privacy and security purpose.

We have to understand that, to protect people's right to privacy, countries, including Singapore, that contact tracing will be used strictly for disease control and cannot be used to enforce lockdowns or quarantines.

6) The Indian government has not released any information about the source code of the app. "The only information we have of the app is its frontend and its rather lacking terms of service and privacy policy. Other projects release as much information as possible intended to obtain transparency."

This, in effect, prevents ethical hackers from identifying security threats in the app, and makes it potentially more vulnerable to malicious attacks. where as other tracing app has its own frequently asked questions section and detailed videos on how data is collected and used. Aarogya Setu has neither.

7)Aarogya Setu application appears to clearly be inconsistent with privacy.The paper evaluates Aarogya Setu on various privacy and safety parameters against two similar apps specific to Covid-19—the TraceTogether app from the Singapore government, and Massachusetts Institute of Technology's Private Kit: Safe Paths project.

Major differences between Aarogya setu(Indian government app)versus TraceTogether(Singapore government app)

a)TraceTogether states that the data collected through the App can only be used by the country's Health ministry where as in Aarogya Setu App there are already reports which confirm that this server is being linked with other government datasets. Such linking increases risk of permanent system of mass surveillance

b)In TraceTogether App the source code is visible where as in Aarogya Setu App source code is hidde.(because of which people are unaware about the terms and services which is used to protect data, and there is no as such guarantee about the security of data.)

c)TraceTogether App releases as much information as possible to obtain the transparency where as The only information we have about Aarogys Setu App is it's frontend and it's rather lacking terms of service and privacy policy.(which mean Aarogya Setu App has no means of transparently auditing what the app is doing in the backend)

d)Singapore monitors people's interactions through Bluetooth beacons, MIT does it through GPS, and then there's India which uses both.

e)Other apps just collect one data point which is subsequently replaced with a scrubbed device identifier. India's Aarogya Setu collects multiple data points for personal and sensitive personal information which increases privacy risks.

f)In its current form, the app does not allow its users to de-register or delete their accounts. To prevent movement tracking, the app deletes a user's location data from their phone in 30 days from its date of collection, in 45 days from the server if the user tested negative and 60 days from government servers in case of those who have been cured of COVID-19. The app's privacy policy states that upon cancellation of registration by a user, their information will be deleted after 30 days. But since the app does not provide an option to cancel registration or de-register, it's unclear whether uninstalling the app means deregistration.

Government has failed to provide any defined period by when it intends to review, delete and ultimately destroy its systems and data which is collected under the Aarogya Setu project.

After consideration of all problematic issues of Aarogya Setu App here are some logical doubts about this app, apart from privacy and security:

Basically Aarogya Setu App is a contact tracing app which uses bluetooth and GPS technology for expected result i.e genuine result.

Q) So what if user didn't allowed access to GPS (location) and bluetooth technology ? could it lead to a false assessment of COVID-19 situation?

Aarogya Setu App asks users to have the device in their possession at all times, and that an exchange of devices could lead to the app reporting false positives.

Q)How will switching devices lead to a conclusion that someone is falsely identified as Covid-19 positive?

Q) Does this mean that people are categorised as Covid-19 positive based on the data collected by the application itself, instead of a formal test result to confirm a positive diagnosis?

Aarogya setu application claims that,"The app only provides data for a radius of 10 kilometres only for phones in India.", which was later proved completely false by the French ethical hacker **Robert Baptiste**.

On 5 May, Robert Baptiste who goes by the name Elliot Alderson on Twitter, pointed at vulnerabilities on the Aarogya Setu app by showing that details of millions of Indians using it could be accessed within a 100-km radius.

On 6 May, Robert Baptiste tweeted that security vulnerabilities in Aarogya Setu allowed hackers to "know who is infected, unwell, [or] made a self assessment in the area of his choice". He also gave details of how many people were unwell and infected at the Prime Minister's Office, the Indian Parliament and the Home Office.

If this is indeed the case, there is a need to strongly commence dialogue to roll back the application and fine tune the entire process."

3. CONCLUSIONS

How to prevent these risks?

- 1)The usage of these applications should be voluntary
- 2)All data should always be stored locally on people's devices
- 3)This data must be encrypted
- 4)No Government can access it at a later point, so must ensure nothing is centralised in a server
- 5)Governments must appreciate that any data from location information, to proximity confirmations, to health status, to whether they have been placed in isolation is sensitive personal information.
- 6)Privacy by design is more than just assurances that phone numbers are not recorded, all data is encrypted, pseudonymisation is deployed or that the use of the app is "voluntary" and based on consent. Most of these protections have known techniques of circumvention.

Therefore, we need to follow to two principles:

- 1)Strict limits (in terms of collection and duration) every step of the way; and
- 2)Comprehensive evidence-based justifications every step of the

REFERENCES

- [1] <https://qz.com/india/1838063/modis-aarogya-setu-coronavirus-app-for-india-a-privacy-disaster/>
- [2] <https://internetfreedom.in/is-aarogya-setu-privacy-first-nope-but-it-could-be-if-the-government-wanted/>
- [3] <https://www.google.com/amp/s/www.thehindu.com/news/national/how-does-the-aarogya-setu-app-work/article31532073.ece/amp/>
- [4] <https://www.google.com/amp/s/www.bbc.com/news/amp/world-asia-india-52659520>
- [5] https://en.m.wikipedia.org/wiki/Aarogya_Setu
- [6] <https://www.google.com/amp/s/www.bbc.com/news/amp/world-asia-india-52659520>