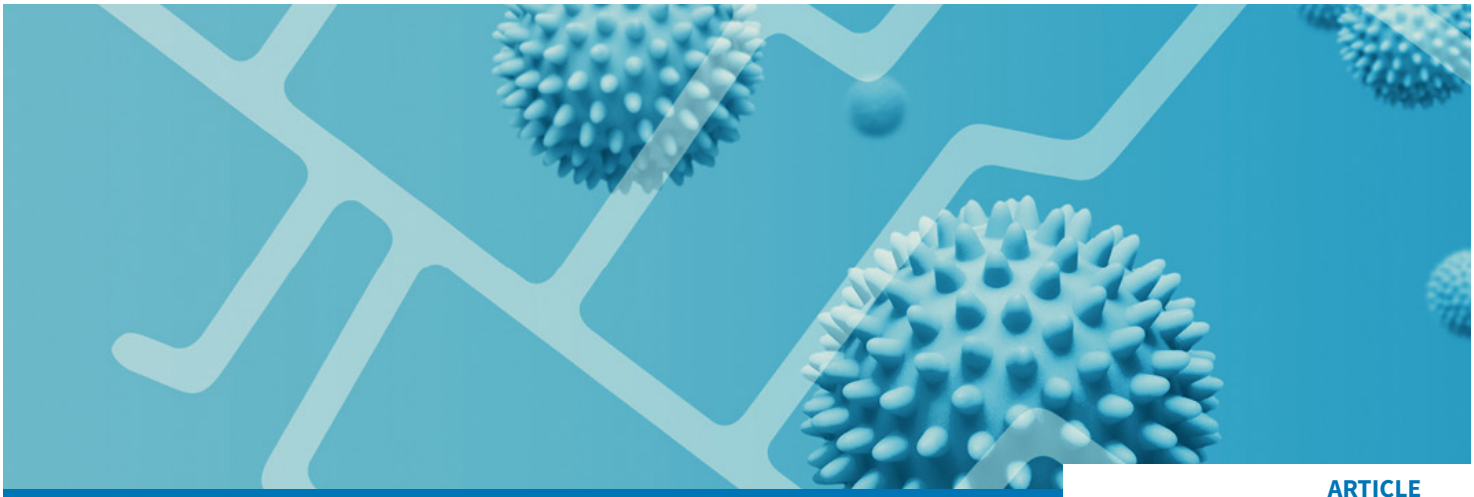

ARTICLE

A Review of India's Contact-tracing App, Aarogya Setu

The Government of India's Ministry of Electronics and Information Technology (MeitY) agency launched Aarogya Setu, a contact-tracing mobile application. Aarogya Setu has been created by the National Informatic Centre (NIC) in response to the COVID-19 crisis, as a way to collect and understand public health-related data.[1]

"On various online discussion forums, there is significant interest in the workings of this government- managed app and its use of personal and sensitive user data.."

The application uses mobile phones to perform a cross reference of individuals' data with the database held by Indian Council of Medical Research (ICMR), which was specially created as part of ongoing COVID-19 testing infrastructure. The purpose of Aarogya Setu is to notify users whether they have been exposed to COVID-19, by checking their proximity to known patients. In the event of a match, the application will warn other users in the area that an infected person is in their proximity. According to the press release dated May 26, 2020 available on mygov.in website, roughly 114 million users have adopted the app.[2]

Aarogya Setu also collects some sensitive personal information including gender and recent travel information. This has raised privacy and security questions. This whitepaper evaluates the functionality and data privacy aspects of the application.

About Aarogya Setu

Aarogya Setu app is a self-assessment disease monitoring app launched by the Indian government. The app is available in 11 languages, including Indian regional languages.[3] It is a digital service that is designed to augment the government's initiatives to generate awareness among the population about COVID-19. It provides best practices to stay healthy, medical advisories and guidelines related to COVID-19. The aim of this app is to enable early detection and prevention of potential risks caused by COVID-19 infection.

1 https://www.mygov.in/aarogya-setu-app/
2 https://static.mygov.in/rest/s3fs-public/mygov_159050700051307401.pdf
3 https://www.mygov.in/task/aarogya-setu-app-covid-19-tracker-launched-alert-you-and-keep-you-safe-download-now/

"As per new rules introduced, data of an individual cannot be stored beyond 180 days, and it also empowers a person to ask for deletion of his/her personal data from the government records related to Aarogya Setu within 30 days of raising the request."

The app is available for iOS, android and KaiOS platforms. Similar apps have been released in other countries—Australia (COVIDSafe), Singapore (TraceTogether), Israel (HaMagen), Switzerland (SwissCovid), Saudi Arabia (Corona Map) among others. There are few other countries such as UK and France that are still evaluating apps pertaining to the pandemic.

How the application works

When a user installs the application on any Android or iOS mobile device, at the time of registration, the user must accept the Terms of Use and Privacy Policy, and the use of the application signifies user's continued acceptance thereof. The application collects the following information: name, age, sex, profession, phone number, international travel within last 28-45 days and whether the user is a smoker.

This information is stored on a server controlled by the Government of India. It is hashed with a unique digital ID(DID) that is pushed to the user's mobile application. The DID is used to identify the user. The user must enable the mobile phone's Bluetooth and GPS services so that when the phone comes within range of another device with the app, it can engage in an information exchange.

When two users come in close contact, their unique IDs are stored on the two phones along with the time stamp and GPS location. This information is stored in an encrypted format. It is uploaded to the app's servers (controlled by the government) only if a user tests positive.

There is a feature in the application called, 'self-assessment test,' which prompts the user to answer a health questionnaire. Whenever a self-assessment test is completed, the application will collect device location and upload it to the server along with the user's DID, unless the result is 'Green'. The application continuously collects the user's location data every 15 minutes and stores it securely on the mobile device. Information from the application is uploaded to the server in following cases[4]:

- If the user self-declares positive for COVID-19 or
- If self-declared symptoms indicate that the user is likely to be infected with COVID-19 or
- If the result of their self-assessment test is either 'Yellow' or 'Orange'.

Security aspects

A French researcher recently raised an alarm over security aspects of the app.[5] The Indian Computer Emergency Response Team (CERT-In) and the National Informatics Centre (NIC) have stated that the features that prompted his concerns were not security flaws, but design aspects of the app. On various online discussion forums, there is significant interest in the workings of this government- managed app and its use of personal and sensitive user data.

We did some fact-finding

To deliver its functionality, the application constantly accesses the phone's Bluetooth and stores the user's location data. While this may appear as a red flag to some, accessing a phone's location is a very common access right that most applications require. In some cases, location access is also needed to let the application run in the background.

Protection of personal/confidential data of application users

As per the section-2 of privacy policy of this application, "persons carrying out medical and administrative interventions necessary in relation to COVID-19" will have access to the data collected by this app.[6] On May 11, the government issued a set of guidelines for data processing of app users and added clauses that may lead to imprisonment of persons found guilty of violating certain data protection measures.

As per new rules introduced, data of an individual cannot be stored beyond 180 days, and it also empowers a person to ask for deletion of his/her personal data from the government records related to Aarogya Setu within 30 days of raising the request.[7]

4 https://web.swaraksha.gov.in/ncv19/privacy/
5 https://www.hindustantimes.com/india-news/french-researcher-flags-aarogya-flaws-govt-denies/story-Ea0mGXS3NWRvlfYSBJJYaK.html
6 https://web.swaraksha.gov.in/ncv19/privacy/
7 https://indianexpress.com/article/india/govt-issues-data-processing-rules-for-aarogya-setu-adds-jail-term-on-breach-6405205/

Source code is now public

Recently the government announced opening the source code of the Android app, for scrutiny by the developer community to address privacy concerns and launched a bug bounty programme for finding security flaws.[8] The developer community can now review the source code of the app, understand how the entire process works and examine to what extent personal information is processed. Source code for the iOS version is forthcoming, along with the server code. This demonstrates the government's good faith efforts towards transparency.

Limitations on liabilities

Section 6 of the Terms of Use of the app states that, along with limiting the liabilities of the government for certain aspects such as accuracy of the information provided by app, the government will not be liable for accurately identify persons in your proximity who have tested positive to COVID-19.[9]

Fake Aarogya Setu App

Some external malicious actors have developed a malicious application called ArogyaSetu.apk that they allegedly sent to Indian defense personnel through WhatsApp from the United Kingdom (UK).[10] When this malicious software is installed on a user's device, it extracts sensitive information about defense forces and sends it to the originator without the knowledge of the device owner. Eventually, defense personnel were informed about this attack, and have now been instructed to download the app only from trusted sites like mygov.in or from Google Play for Android and App Store for iOS.

Further analysis

FTI experts performed static and behavioral analysis on the application (apk), in adherence to the laws and rules of the application and the government. Below is the summary of the findings:

Application permission

Aarogya Setu application requires access to some specific permissions on your Android or iOS device such as location, mobile data, location, local storage and Bluetooth configuration. FTI has not observed this application access other information sources such as contacts, SMS, internet history, social media profiles/ posts etc. We have not seen any malicious behaviour of the Aarogya Setu App during our analysis which would contradict its publicised functionality.

Manifest analysis

Every application has a Manifest file that presents essential information about the application to the mobile operating system. While analysing this apk file [11], we found that the Broadcast receiver which responds to broadcast messages from the application and system, is shared with other applications. On occurrence of the events, it either creates a status bar notification or performs a task. We observed that Broadcast receiver is accessible to other applications in the device. This vulnerability can get exploited by any other application or emulator in the mobile system and can be further hardened.

Strings analysis

Strings are sequences of printable characters which can reveal some information about what the programme does, or what it can do. For example, if a programme accesses a URL while it executes, then you will see the URL accessed stored as a string in the programme. We checked certain strings found during the analysis and did not observe any suspicious or malicious communications. Also, no evidence of any malware was found while analysing the strings.

Domain malware analysis

A domain is a substitute that replaces the Internet Protocol (IP) address. For example, IP address 172.217.8.14 can be replaced with a domain name such www.google.com. We listed out a bunch of domains that are being communicated by this application but did not see any bad or suspicious communication going on. All the communicated domains are whitelisted and safe.

URL Analysis

A URL incorporates the domain name, along with other detailed information, to create a complete web address. Many times, this URL can be tampered or obfuscated to redirect a web browser to some malicious web page. We analysed the communicated URLs and found no malicious or suspicious communication. All the communicated URLs are whitelisted and safe.

8 https://innovate.mygov.in/aarogyasetu-bug-bounty/#tab1
9 https://aarogyasetu.gov.in/terms-conditions/
10 https://theprint.in/defence/fears-rise-that-pakistan-based-intel-operatives-could-misuse-aarogya-setu-app/409798/
11 https://apkpure.com/aarogya-setu/nic.goi.aarogyasetu

Recommendations to protect personal data

1. Keep your application updated all the time by installing the latest available updates
2. Do not install any app from an unidentified location or links shared on SMS/WhatsApp. Only install the app from authorised App Store/Google Play
3. Do not share screenshots or results of your app with anybody other than authorised medical representatives or government authorities
4. Keep your mobile device operating system updated to the latest version
5. If your phone is changed/exchanged, uninstall the app from the old phone
6. Keep the mobile device password protected.

Conclusion

The government has been trying to address concerns about Aarogya Setu application and is trying to be as transparent as possible. In absence of data protection and privacy laws, users of the app may continue to raise concerns regarding privacy and security. Key points to remember include:

1. An old version of the Aarogya Setu application (v1.0.1 released in Apr 2020) had a bug that could allow other applications to read files inside the application using an exposed Activity and its intent filter. This issue is fixed in newer version v1.1.1.
2. We did not observe any names, or personal information being leaked or shared with any unidentified location.
3. This application has jailbreak and root detection capabilities enabled that allows it to detect mobile phones that are hacked and have SSL pinning implemented. But both may be bypassed by custom scripts as claimed by some security researchers. However, this is subjective to advanced technical manipulation and behaviour of the variant of the mobile operating system it is applied on.
4. There is no vulnerability of any major consequence observed in this application during our testing. However, security and privacy of the data should be maintained on the application server, which was not included in our testing.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals. We did not have access to the source code of the app to do a deep dive analysis and have relied on black box testing to understand the app behaviour.

AMIT JAJU
Senior Managing Director & Head of Technology Segment
+91 (0) 98200 73695 M
amit.jaju@fticonsulting.com

AMOL PITALE
Senior Director
+91 (0) 9833996432 M
amol.pitale@fticonsulting.com