Suraksha Setu: Private Distance Manager

Anirudhdhsinh Jadeja[1], Sandeep Jangir[2], Vishwas Kumar[3]

Department of Computer Science & Engineering

Parul University, Vadodara

Email: *160303105108@paruluniversity.ac.in[1], sandeep.jangir270054@paruluniversity.ac.in[2], vishwas.kumar270209@paruluniversity.ac.in[3]*

DOI:- https://doi.org/10.47531/SC.2022.26

Abstract

This article mainly focuses on the necessary privacy concerns of users and updating features of current techniques by adopting robust features and securing weak points. This article suggests working with two platforms, web-based and app-based, to share data more efficiently. Focusing on current requirements, only a single source protocol is used. Data about positive persons should be uploaded by authorised laboratories only and accessed from a single source only. This will help to get more accurate data about positive cases. Instead of focusing on each user's data, it focuses on data of different areas, which helps decide which area is sensitive. Secure location service is added to help people maintain social distance, ensuring that the user's destination is safe. All processes are done locally, and data is kept secure in local storage, enhancing users' privacy. This way, user's privacy and efficiency both are preserved.

Keywords: - *Privacy, Public Safety, Tracing, Transportation*

INTRODUCTION

To fight corona, many countries have developed apps with the objective of contact tracing, and many have declared lockdown periods. The main problem is that containment is an effective means to slow the spread, allowing health care systems the capacity to treat those infected. However, 'lockdown' like containment can also disrupt the population's productivity, distort the markets (limiting transportation and exchange of goods), and introduce fear and social isolation for those not yet infected or who have recovered from an infection. The current situation also has cases of persons who don't have symptoms of the virus and still tested positive. This considerably invokes concern about data shown by apps which are just predictions.

In most cases, all apps fail to get correct information about locations spreading the virus rapidly. And they are unable to provide exact information from where the spread started and from which part this chain can be cut. So, to overcome this, this article suggests that only authorised laboratories should update data on a server, and only that data will be displayed. Predictions of apps will be used to get info about who needs more concern about testing. So, people with higher chances will be tested first and then will be updated in the database. To protect privacy,

data will be updated based on areas of concern that can be identified. It also shows the sensitivity of location at a particular destination which helps users make decisions about their destination.

Using chain of infection, identify origins of infection and cut down the chain before it spreads more widely. The idea is to mainly use local storage for processes and data, which builds trust in users about their privacy.

PRIOR RESEARCH

Trace Together:

Trace Together works by exchanging short-distance Bluetooth signals between phones to detect other participating users in close proximity. Records of such encounters are stored locally on each user's phone. If MOH interviews a user as part of the contact tracing efforts, they can consent to send their TraceTogether data to MOH.[1]

Phone numbers are the only personally identifiable information required from the user. The phone numbers are used to contact users if they have had prolonged exposure to an infected person.

BlueTrace devices log encounters with each other by exchanging messages over Bluetooth using a BLE handshake. In BLE parlance, devices can take on Peripheral or Central roles.

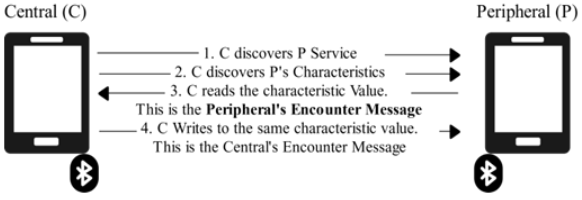

Fig. 1 BLE Handshake Flow [2]

BlueTrace addresses this by having users exchange temporary IDs (TempIDs). Each TempID comprises a UserID, created time, and expiry time encrypted symmetrically with AES-256-GCM, and then Base64 encoded. Blue Trace works with Scanning and Advertising cycles in which scanning allows devices to scan other BlueTrace devices as Central. BlueTrace devices should implement a blacklist of recently seen devices and not attempt to connect to them for the duration of the blacklist period. When patients have been confirmed to be infected, health authorities ask them if they have the app installed. If they do, they are asked to upload their encounter history to the health authority. To protect users and the system from fraudulent uploads, an authorisation code is provided.

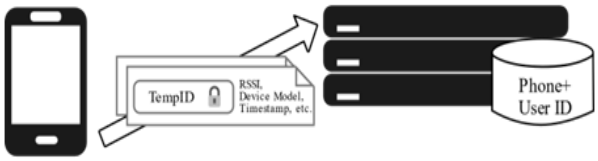

Fig. 2 Upload of encounter history.[2]

The collection and logging of encounters between devices are done in a decentralised P2P manner. The application has been built on an open-source protocol called BlueTrace protocol, developed by Singapore's Health Ministry and its Government technology Agency. The source code for the android and iOS applications and its cloud function is available on GitHub [3].

Conclusion of Blue Trace: It notifies users within a proximity range. It makes sure that only authentic cases are shown to the user. Most data are stored locally. Maintaining privacy is the main goal. But, On the other hand, there is no location-based update and no mechanism to stop people from gathering. It also fails to detect the chain of infection.

Private Kit: Safe Path is an MIT-led, free, open-source technology that enables jurisdictions and individuals to maximise privacy while also

maximising the effectiveness of contact tracing in the case of a positive diagnosis. The Safe Paths platform comprises a smartphone application, PrivateKit, and a web application, Safe Places.[4] The PrivateKit App will enable users to match the personal diary of location data on their smartphones with anonymised, redacted, and blurred location history of infected patients.

The digital contact tracing uses overlapped GPS and Bluetooth trails that allow an individual to check if they have crossed paths with someone who was later diagnosed positive for the virus. Through Safe Places, public health officials are equipped to redact location trails of diagnosed carriers and thus broadcast location information with privacy protection for both diagnosed patients and local businesses. [5]

The Private Kit: Safe Paths solution, in its first iteration, enables individuals to log their location. With consent, they can provide health officials with an accurate location trail once they are diagnosed positive. Additionally, governments are equipped with a tool to redact location trails and thus broadcast location information with privacy protection for diagnosed carriers and local businesses.

Safe Paths provides users with information on whether they have crossed paths with a diagnosed carrier in its second iteration. Safe Paths' ability to do so without collecting information on the user in an external cloud prevents government surveillance. Safe Paths fosters public trust and utilises experts to audit its security and privacy features as an open-source tool.

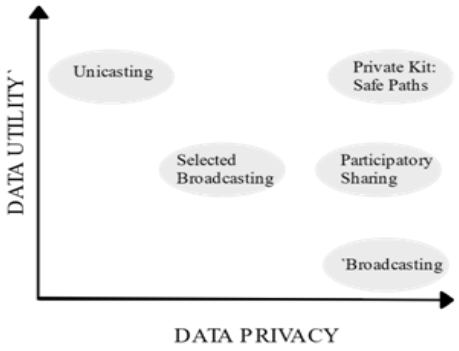

Fig. 3 Data Utility vs Data Privacy by Private Kit [6]

In this third iteration, Safe Paths enables privacy protected participatory sharing of location trails by diagnosed carriers and direct notification of users who have been close to a diagnosed carrier without allowing a third party, particularly a government, to access individual location trails. For public audibility, the application is built on an open-source protocol that is accessible on Github.[7]

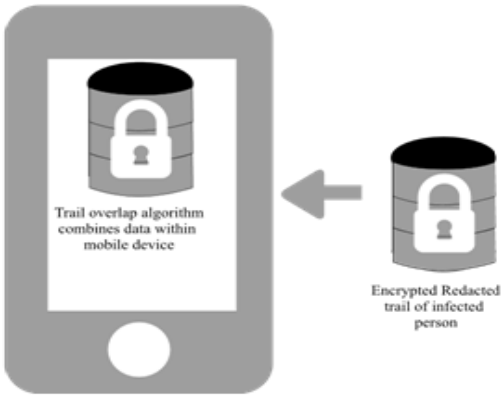

Fig. 4 Location Trail by Private Kit: Safe Paths [8]

Conclusion of Private Kit: This App supports location-based tracing and also provides privacy protection. It can generate a location trail and also gives authentic information. But, on the other hand, a policy is not clear if user consent will conflict with Government interests or requests. It also fails to stop people from gathering.

Aarogya Setu:

Aarogya Setu is one of the most downloaded and appreciated app in the Google play store recently. It is built by s India's National Informatics Centre

(NIC), which is under MeitY. Aarogya Setu comprises both IOS and Android platforms but lacks a web-based portal. Aarogya Setu notifies users as soon as they come in proximity of other users who may have chances of infection. It uses GPS and Bluetooth BLE handshake protocol to determine whether the users are close to another user. It is now widely accepted in India. The Prime Minister of India also pushed the app.

The app starts with asking Preferred Language. After that, some tips on why to use this app are shown to the user. Furthermore, some permissions about Location, Bluetooth, and Data sharing asked. It also shows privacy policy to the user and when permissions and policy are accepted. It moves further, asking for basic info like mobile number, Gender, Full Name, Age, and profession. It generates a Unique Digital id and pushes it into the server.

It consults users by asking questions about health and symptoms. If the user meets symptoms user will be marked as having a high chance of infection. And when that user comes in proximity of another user, that another user will be notified. It is noted that the information collected from the app will be securely stored on the mobile device of the other registered user and will not be accessible by such other users.[9]

When two devices come in proximity, they share the following data,

1. Media Access Control (MAC) Address
2. Distance between the Devices
3. Device ID (A static random ID computed from the personal information and the phone number of the users)
4. GPS latitude and longitude
5. Signal strength as seen by the devices
6. Time at which the contact device was seen
7. Bluetooth model name and number[10]

As per the updated privacy policy in version 1.0.6, it is mentioned that "Nothing set out herein shall apply to medical reports, diagnoses, or other medical information generated by medical professionals in the course of treatment." Each time the user completes a self-assessment test, the app will collect location data and upload it along with DiD to the server.

The policy mentions that the app continuously collects location data and stores it securely on the mobile device, maintaining a record of all the places you have been at 15-minute intervals. This information will only be uploaded to the server along with DiD if a user has a chance to be infected with corona. So, it is noticed that every user who may have a chance to be infected with the virus will be highlighted on other user's devices. This type of strategy can lead to privacy concerns of users who may have chances. So even if they don't have a virus infection, other people won't treat him the same. The current release of the app also shows a number of positive cases. Aarogya setu has only one platform to show this data. This app lacks a web-based platform that can provide data to the public more reliably.

Conclusion of Aarogya Setu: It can give location-based updates of each user and notify the user if another user has a chance of infection. But, uploading each user's data is not the best way to trace. If any user has a chance of infection, they might be falsely marked as positive by other people. There is still exist a concern about data security. It also fails to generate area reports. It also fails to detect a chain of infection. The app fails when a user turns off Bluetooth.

Considerable Points

- Location data are essential for making crucial decisions for areas that may require more attention.
- Knowing the number of positive cases is an excellent approach to take further steps.
- Each user should be aware of the situation around them.
- The privacy of a user is a great concern that should be preserved.
- Information spreading through the nation should be static, reliable, and authentic.
- Users who require more attention should be considered first.
- Users outside the home still need to be secured from each other.
- Users should be free to choose whether they want to show their status publicly or not.

Points need to be secured:

- Tracing and transmitting user's personal information to servers results in privacy flaws.

PROPOSED MODEL

The system proposed here is intended to be used as part of a broader campaign to combat COVID-19. These methods focus on gathering and disseminating the information needed to perform targeted interventions. This system has three components that work almost independently but can be bundled into a single mobile app. Depending on privacy requirements and the needs of specific public health authorities, a subset of these capabilities could be utilised.

Three parts:

1. Publishing authentic information about COVID-19 positive cases from a single source only.
2. Breaking Chain of Infection
3. Securing Routes

A. Publishing Information

To preserve the authenticity of the information, a single source protocol is used, and data should be updated by only laboratories used to test cases. One platform of the website should be constructed to update and display data about cases of positive people. It is essential to not making the private information of users' public. Only the number of cases will be made public. Furthermore, a user who tested positive will be notified by app, and regional doctors will be informed about that for further steps. The user will be free to willingly publish their information about the current status of the test. And users will be notified to be in quarantine as much as possible. Private data will be collected by laboratories that are needed to perform tests. Hospitals and laboratories will be working in sync to provide accurate information. Hospitals will be updating case details whether the infected person is under treatment, recovered or dead. The website will be public, so anyone can easily access the data about corona cases. In addition to this, this website can contain all the necessary steps and cautions. All official news published by the government will be accessed from here. Even after lockdown opens, news should be steady and authentic, so this solution works best to control fake news and non-static data among different social sites. For the security and authenticity of data, blockchain technology can work best. Blockchain works by adding the transactions, and altering or deleting transactions is not allowed in blockchain technology. Blockchain has its security mechanism, which

works by hash code. So, to make data static, non-alterable and secure, blockchain is the best choice.

Advantages:

1. More accurate data.
2. The authenticity of data will be automatically proven.
3. There will be static numbers among all social sites.
4. Protection against fake news.

B. Breaking Chain of Infection:

In India, Aarogya Setu is working to collect data about users who may have chances to be infected with the coronavirus. But rather than showing to people who may have been infected, it should preserve privacy. The proposed model suggests that It shall update data on the server only. According to Robert Redfield, the director of the Centres for Disease Control and Prevention, USA government, 25 per cent of people infected with the new coronavirus don't present any symptoms or fall ill. However, they can still transmit the illness to others [11]. So, it is dangerous to show people that the person near them doesn't have a chance of corona. Here, it is noted that Aarogya Setu determines the chance of infection by some questions and symptoms of the person. So, this data can be used to determine whether the person needs care or not. If the person needs care, then regional doctors will be notified immediately to give them a priority.

Local doctors will collect a sample immediately and will send it to laboratories as a prime sample. If a person has higher chances and met someone else, then that user will be suggested to take a test instead of showing them that they are in contact with someone who has a chance to be infected. Data of this user won't be uploaded to the server until he gives consent. An alternate solution to track down sensitivity is tracing areas using the three-level tracing technique. In this technique, the user who has chances of the corona is in the centre. Let's call him User S. At the second stage, that user is there who came in contact of user s and may have chances to be infected and let's call him User A and at last that user who came in contact of USER A or may not be in contact of User A. Let's call him User B. And it will then create a chain of infection chances.

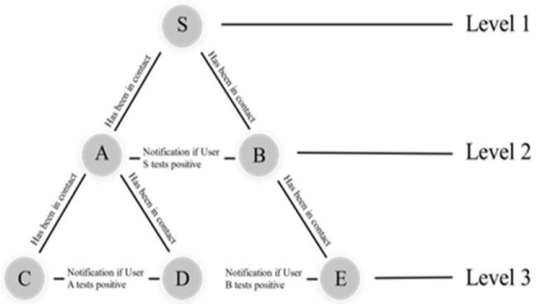

Fig. 5 Chain of Infection Chances

This way, we can determine how many users are in the area with a strong chance of being infected. This technique works using the parent-child relationship concept. If a parent has any illness, then it might affect the child too. So on, in this tree, if any parent gets their test result positive, the immediate child will be informed in real time. Let's assume a scenario.

- User S has been in contact with User A and User B.
- Now, User S will create a chain consisting of User A and User B.
- So on, User A and User B will create their own chain too.
- If User S tests positive, User A and User B will be notified at a level.

2. As per the parent-child relationship

- Level 3 users User C, D and E, won't be notified as their parent doesn't tested positive.

- But, As they are grandchildren of user S, there are still chances that Level 3 users have an infection. So, they will be suggested to maintain social distance strictly till User B's test result come.
- If User A tests positive, then there is a chance that user A got the infection from User S. So, considering that point, User B will also be notified to get tested.
- If User B tests positive, then there is a chance that user B got the infection from user S. So, considering that point, User A will also be notified to get tested.

The same chain goes for others. This way, we can stop infection by simply tracing the next person who has the most chances.

Users' records who took the test will be used to determine which area has started to spread the virus rapidly or will be used to determine which area needs more care.

If User S's test is positive.

Table 1 Infection via User S

Level	Users	Percentage
1	S	100%
2	A,B	50%
3	C,D,E	25%

- In this scenario, User S tested positive. Hence, users A and B have a strong possibility of being affected by a virus, so they will be notified and strongly suggested to give the virus infection test.
- Where User C, D, and E have a little chance, they will be informed to take precautions.

If User A's test is positive.

Table 2 Infection via User A

Level	Users	Percentage
2	A	100%
2	B	30%
3	C, D	50%

- In this scenario, User A tested positive, so there is a possibility that User A might get an infection from user S and because of that, User B will be notified to take precautions, and if possible, User B should give a test too.
- User C and D has a strong possibility to be infected so. They will be strongly suggested giving a test.

If User B's test is positive.

Table 3 Infection via User B

Level	Users	Percentage
2	B	100%
2	A	30%
3	E	50%

- In this scenario, User S tested positive, so users A and B have a strong possibility to be affected by a virus. So they will be notified and strongly suggested to give the test of virus infection.
- Where User C, D and E have minor chances where they will be informed to take precautions.

The exact probability from table 2 can be calculated for User B as well. This way, we can give priorities to users and follow those priorities to test users.

Algorithm:

```
ClassInfo{
Var location;
Vartest_status;
VaruserID;
} main{
If(currentUser_has_chances){
            If (inProximity(otherUser)){
createAndSendChainInfo();
          }
       }
if (User_test_results == true){
```

```
informChainedUsers();
        }
}
```

A. Securing Locations

Securing locations means securing weak points. It is still necessary to prevent more contact with people after breaking the chain. People still have daily needs, and they can't be kept in quarantine at all times. For that, it is necessary to prevent people from making contact with each other. This paper proposes a unique way to tackle this problem by accessing the location's current sensitivity and showing that to users. This way, users will know the location's sensitivity and can easily decide whether to go or not.

Securing Location works in 5 easy steps.

- *Set Destination Location*: In this step, the user sets his destination location where he wants to go.
- *Choose Purpose:* In this step, the user will choose permission from the list and apply for it. After applying for permission, the user will be shown the sensitivity of the area where he wants to go.
- *Confirm Location***:** In this step, if sensitivity is shown high, the user will re-think and will decide whether he wants to go or not. Depending upon his decision, he will be shown a route to follow or taken to the main screen.
- *Follow Route:* In this step, the user will follow the route and will not go out of the route. In any case, if he goes out of route, it will be considered a violation, and he will be updated on servers.
- *Back to home:* In this step, the user will respond whether he came back or not. Depending upon his response, he will be taken to the main screen or again shown a route to home.

These are the five easy steps that the user needs to follow. And the user will not be bothered by the police. All processes which raise privacy concerns are done locally. The current model utilises the client's device to do all operations and preserves privacy.

D. Location Sensitivity

This is the task of the server in which the server will take the user's destination location and save it in the database. Depending upon the number of users present at that location range and the number of users tested positive, the server will decide the sensitivity of the location. Then the server will update information in the database.

Algorithm*:*

```
Database.getCurrentAccessedLoc(child(i))
{   Calculatedis(loc(child(i)): currentAccessedLoc(i))
{    if(inRange(5, 20))
{
Database.get(CurrentAccessedLoc.users) + 1;
   }
  }
}
if(Database.get(CurrentAccessedLoc.users)<10){
Database.get(CurrentAccessedLoc.sensitivity)
.set sensitivity “low” ;
}

if(Database.get(CurrentAccessedLoc.users)>10&&
Database.get(CurrentAccessedLoc.users)<20){
Database.get(CurrentAccessedLoc.sensitivity)
.set sensitivity “Med” ;
}
if(Database.get(CurrentAccessedLoc.users)>20){
Database.get(CurrentAccessedLoc.sensitivity)
```

```
.set(sensitivity “High” ; }
```

If the sensitivity of destination location is high user won't decide to go there. If sensitivity is medium, some users won't find it convincing, and they will avoid going there, thus preventing that location from being highly sensitive zones. This information can be used for determining the attention required by cities or places.

E. Route Security

This is the task of the client app in which the client app will take the user's destination location and save it in the database. As soon as the user leaves home, his status will be updated in the database as ***USER_OUT_OF_HOME,*** and the number of users out of home will be increased by one in the database. The user set as out of home client app will receive the route, and now the user will follow the route shown in the map using GPS. Meanwhile, the app will continuously watch over the user, and it will notify the user if a user is not following the route. Thus, it won't affect the sensitivity of other locations. When the user reaches the destination place, the number of users present at that place will be increased by one. Thus, increasing the sensitivity of the location. And that sensitivity will help other users. At last, the user will leave that location and will follow the route back home. As soon as the user reaches home, the client app acknowledges the server, and the server will destroy all location data and routes from the database.

Algorithm:

Data Storage and Security: It is essential to know how and where people's data will be handled. For that, this article suggests storing data locally as much as possible. Primary data will be (i) Name, (ii) Mobile Number, (iii) Location, (iv) Address, (v) Age, (vi) Sex. These data will be stored locally, and each user will generate a Unique Identification Number (UID). And all this data will be completely private to the user, and no one will access the data without a specific medical reason.

Algorithm:

```
PrivateClassUser{
        Var Name,
        Mobile_Number,
          Location,
 Address,
          Age,
Sex;
chargrantAccess(medical_purpose){…}

        Publicvar UID;
}
```

UID, made public, will create a chain of infection, and only authorised personals and servers will access it. After creating a chain, chain data will be uploaded to servers to detect the breakpoint and analysing the purpose. As soon as the server prioritises patient UID, user data will be shared with regional doctors for further processing. The whole process will be end to end secured with a standard encryption process. Storing data using blockchain helps manage the chain more efficiently and adds one more layer of security to the system.

EFFECTS

Industries: Some industries have a huge infrastructure in which there are many sections to work. It is hard to maintain social distancing in that situation. Routine testing of all workers at entry is not possible. And there are many chances that workers will meet another worker from another section too. So, there will be hard to stop spread if someone gets infected. To prevent the

spread, we must know who has the most chances of infection next. So, huge men power needed industries will have the benefit of it. And government can keep watching whether industries are maintaining social distances or not using location sensitivity.

Transportation: Transportation after lockdown is a big challenge, especially in Mumbai, where local trains are the most used public transportation. If we want to reduce traffic at any location, we have to stop people from going there. And for that, location sensitivity will do the perfect work. The app can track down how many people are there on a train by exchanging location info and proximity range. If there are more people, then the threshold value all other users willing to use that train will be notified and choose another train. In public transport, it is still hard to maintain social distance even with fewer people inside it. So, using a chain of infection, we can efficiently track down how many persons in the queue might be infected and be notified for tests sooner.

Predicting Data: If the government can track the live spread of corona, then the government can take necessary actions more efficiently. It is possible with predicting data with machine learning and neural network. When a chain of infection is created, data will be indicated for a single chain and other chains—ultimately resulting in big chain prediction, which might affect the whole area. So that area can be sealed before it gets infected.

Getting Priority: The chain of infection allows doctors to get the priority of patients. There are many situations in which some patients lacked care and been more infected. So, If any user has created a long chain, then he must be tested first to protect other people in the chain.

CONCLUSION

Single source protocol provides authentic data and controls rumours among nations. Using the chain of infection, we can decide which area needs more care instead of using each user's data, which is more secure and preserves privacy.

REFERENCES

1. Hariz Baharudin, Lester Wong, Straits Times, Published on Date 21st March 2020 5:00 AM SGT.https://www.straitstimes.com/tech/singapore-app-allows-forfaster-contact-tracing
2. BlueTrace White Paper, By Jason Bay, Joel Kek, Alvin Tan, Chai Sheng Hau, Lai Yongquan, Janice Tan, Tang AnhQuy, Government Technology Department, Singapore, Published on April 9 2020.
3. https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf
4. BlueTrace, Singapore Government, Published on April 9, 2020.
5. https://github.com/OpenTrace-Community
6. Private kit: safe paths by MIT and Harvard https://safepaths.mit.edu/
7. Orlando Imperatore, MIT Media Lab, Project Safe Paths, by. https://www.media.mit.edu/projects/safepaths/overview/
8. Private Kit White paper, MIT University, Published on March 19, 2020.
9. https://arxiv.org/pdf/2003.08567.pdf
10. COVID Safe Paths, https://github.com/tripleblindmarket/covidsafe-paths

11. On the privacy of TraceTogether, the Singaporean COVID-19 contact tracing mobile app, and recommendations for Australia, By Dr Hassan Asghar, Dr Farhad Farokhi, Associate Professor Ben Rubinstein, Melbourne School of Engineering, Published on April 6, 2020. https://eng.unimelb.edu.au/ingenium/technology-and-society/on-the-privacy-of-tracetogether,-the-singaporean-covid-19-contact-tracing-mobile-app,-and-recommendations-for-australia

12. Suraksha setuplocy April 11, 2020, Government of India,https://web.archive.org/web/20200414082653/https:/web.swaraksha.gov.in/ncv19/privacy/

13. Anand Venkatanarayanan, "How The Aarogya Setu App Handles Your Data", Bloomberg Quint, last Updated on April 17 2020, 1:40 PM. https://www.bloombergquint.com/coronavirus-outbreak/covid-19-how-the-aarogya-setu-app-handles-yourdata

14. 1 in 4 Coronavirus Carriers Could Be Asymptomatic, by Aylin Woodward, Science Alert, Business Insider, 3rd APRIL, 2020 https://www.sciencealert.com/here-s-what-we-know-so-farabout-those-who-can-pass-corona-without-symptoms