frontiers in Communications and Networks

REVIEW
published: 08 December 2020
doi: 10.3389/frcmn.2020.583376

Review and Critical Analysis of Privacy-Preserving Infection Tracking and Contact Tracing

William J. Buchanan[1], Muhammad Ali Imran[2]*, Masood Ur-Rehman[2], Lei Zhang[2], Qammer H. Abbasi[2], Christos Chrysoulas[1], David Haynes[1], Nikolaos Pitropakis[1] and Pavlos Papadopoulos[1]

[1] Blockpass ID Lab, School of Computing, Edinburgh Napier University, Edinburgh, United Kingdom, [2] Communication, Sensing and Imaging, James Watt School of Engineering, University of Glasgow, Glasgow, United Kingdom

Edited by:
Elias Yaacoub,
Qatar University, Qatar

Reviewed by:
Tyler Yasaka,
University of California, Irvine,
United States
Rongxing Lu,
University of New Brunswick
Fredericton, Canada

***Correspondence:**
Muhammad Ali Imran
muhammad.imran@glasgow.ac.uk

Specialty section:
This article was submitted to
IoT and Sensor Networks,
a section of the journal
Frontiers in Communications and
Networks

Received: 14 July 2020
Accepted: 07 October 2020
Published: 08 December 2020

Citation:
Buchanan WJ, Imran MA,
Ur-Rehman M, Zhang L, Abbasi QH,
Chrysoulas C, Haynes D, Pitropakis N
and Papadopoulos P (2020) Review
and Critical Analysis of
Privacy-Preserving Infection Tracking
and Contact Tracing.
Front. Comms. Net. 1:583376.
doi: 10.3389/frcmn.2020.583376

The outbreak of viruses have necessitated contact tracing and infection tracking methods. Despite various efforts, there is currently no standard scheme for the tracing and tracking. Therefore, many nations of the world have developed their own ways where carriers of disease could be tracked and their contacts traced. These are generalized methods developed either in a distributed manner giving citizens control of their identity or in a centralized manner where a health authority gathers data on those who are carriers. This paper outlines some of the most significant approaches that have been established for contact tracing around the world. A comprehensive review on the key enabling methods used to realize the infrastructure around these infection tracking and contact tracing methods is also presented, and recommendations are made for the most effective way to develop such a practice.

Keywords: COVID-19, contact tracing, tracking, privacy-preservation, bluetooth, RFID, wearables

1. INTRODUCTION

In December 2019, the Wuhan area of China was the first in the world to experience the spread of novel coronavirus disease 2019 (COVID-19). Zhou et al. (2020) found that in two hospitals in the area, of those who were discharged and had died, 48% had a co-morbidity with hypertension (30%) and coronary heart disease (8%) being the most common. It has since spread to many regions of the world. Horton (2020) states that the Contain-Delay-Mitigate-Research strategy of the UK government failed as they initially did not test every suspected case, isolate, quarantine, and trace their contacts. Scale of the crisis is highlighted with a delay of over 3 months on non-urgent surgeries (Iacobucci, 2020), and where there are worries around the mental health of those dealing with COVID-19 patients (Greenberg et al., 2020).

Heymann and Shindo (2020) specifies that close monitoring is required in order to match public health approaches to their social acceptance and stresses that there is a need of strong communication methods for self-protection, identification of symptoms, and seeking the treatment. The COVID-19 pandemic has necessitated a contact tracing system, which can be used to identify an infected individual, and then trace the people who have been in contact with that person. This provides ways to control the spread of COVID-19 by identifying the infected cases and their contacts and enforcing appropriate restriction of self-isolation or quarantine. It is likely that a contact tracing system will require the support of human contact tracers, thus making necessary the usage of a mobile phone application because the mobile phones are the only devices used frequently while supporting a wide range of functionalities. The key aspects of a contract tracing application are as follows:

- **Centralized or distributed?** A distributed infrastructure allows users to determine the other people that they have been in contact with, whereas a centralized approach uses a central server to store location tracing information.
- **Proximity based or Global Positioning System (GPS)?** This either involves using Bluetooth methods to track whether a person has been in close proximity to another person, or where GPS location is stored for a user.
- **Privacy-enhanced methods?** This involves the methods used to identify the user and their history of contacts.
- **Open or closed source?** An important aspect with contact tracing is whether the methods are open source. If this is the case, then it is extremely important if they can be peer-reviewed and by whom. Within a closed-source system, there is the uncertainty that for the bugs to be discovered, it usually takes longer periods of time while the products are already commercially used.

Hellewell et al. (2020) analyzed how well contact tracing could be used to suppress the spread of COVID-19. For this, they used the reproduction number (R0), the delay from symptom to isolation, contract tracing probability, transmission before symptom offset, and the percentage of sub-clinical infections.

Privacy plays a vital role within a contact tracing infrastructure. One quote with Raskar et al. (2020) defines:

> "Some of my patients were more afraid of being blamed than dying of the virus."
> -Lee Su-young, Psychiatrist at Myongji Hospital, South Korea

The rest of the paper is structured as follows: section II describes the underlying contact-tracing technologies, whereas section III analyzes all the proposed methods. Section IV discusses the DP-3T approach. Section V provides a view on the range of attacks on contact tracing methods, whereas section VI provides a critical analysis on the feasibility of creating a privacy-preserving contact tracing application. Section VII concludes the work.

2. UNDERLYING TECHNOLOGY

The fast spread of COVID-19 throughout the world caused by severe acute respiratory syndrome has made it an unprecedented national health crisis (Alimadadi et al., 2020). It has brought health services under colossal pressure and necessitates for novel solutions to combat the spread. Contact tracing is one of the crucial interventions that public health professionals rely on in managing the early stages of disease outbreaks.

In the public health realm, the process of identifying an infected patient, listing, and following the people who may have exposed themselves to the infection by coming into contact with them is termed as contact tracing. The process is reckoned to be an effective tool to prevent the spread of infection at a faster rate through timely provision of appropriate care to these people 2020.

Despite proving to be very useful in preventing the spread of a disease, the performance of conventional contact-tracing techniques (interviewing each patient and contacting people that have been exposed to the patient) is often inadequate in urban areas and during disease peaks (Swanson et al., 2018). Germany was able to hold off the disease for a few weeks by using manual contact tracing and moving COVID-19-positive patients to quarantine 2020, but the effectiveness of contact tracing relies on the faster growth of identified cases than the number of new infections (Eames and Keeling, 2003), which is not possible in manual tracing.

This limitation is stressed out by the exponential spread of the disease enabled by a higher-population density and frequent movement of urban residents. Digital tools utilizing existing technologies to gather information on the spread, key symptoms, and means the virus is employing to transfer are reckoned to be an effective response. Contact tracing is one of the key digital techniques that can not only enable the authorities to keep a track of the viral spread but can also play a pivotal role in identifying the potential carriers of the virus due to coming in contact with an identified patient. Twenty-nine countries around the world are now using mobile data to help with contact tracing COVID-19 cases (Hui, 2020).

This section summarizes the communications standards and methods that would best support the contact tracing approach and options already progressing that may help us get further faster.

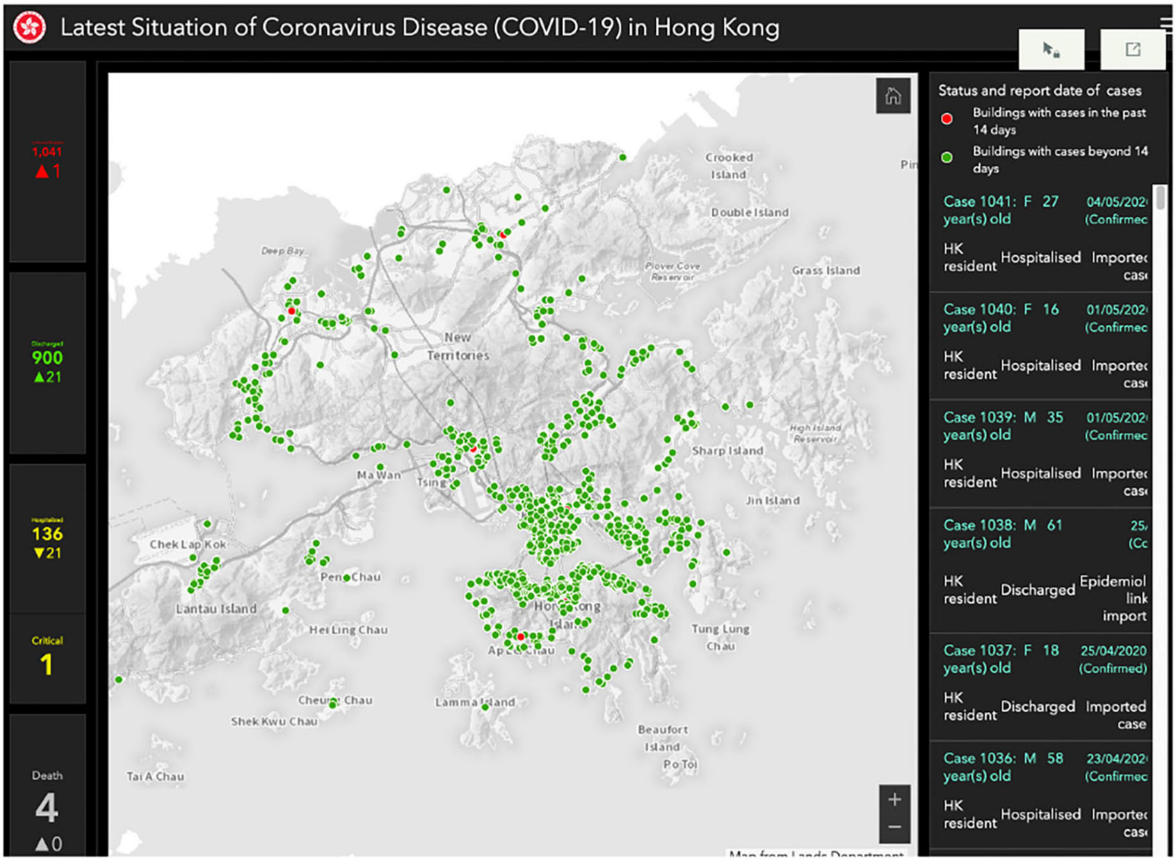
2.1. Broadcast, Selected Broadcast, Unicast, and Participatory Methods

The methods involved with COVID-19 tracing typically split into (a) crowd-sourced applications, (b) self-reporting systems, (c) centralized contact tracing, and (d) decentralized contact tracing. The importance of testing is underlined by Beeching, who outlines (Beeching et al., 2020):

> "Test, test, test" is the key to controlling the spread of SARS-CoV-2 and its clinical manifestation, covid-19, according to the World Health Organization. However, 3 months after notification of the novel coronavirus infection in China, there is inadequate access to appropriate diagnostic tests globally and confusion among healthcare professionals and the public about prioritization of testing and interpretation of results.

Raskar et al. (2020) reviewed the risks around contact tracing and defines the methods of broadcast, selected broadcast, unicast, and participatory methods. With **broadcasting**, the governments share the location of those who have been proven to be infected. Singapore and Hong Kong (**Figure 1**) have a detailed map of infected cases, whereas South Korea uses SMS messages about those who have tested positive.

With **selective broadcasting**, governments do not send out the information to the public about carriers and send only to a selected group, such as people within a geographical area. In this case, users will register for location information, through a specific App, or for their phone numbers. In this case, it



Status and report date of cases
● Buildings with cases in the past 14 days
● Buildings with cases beyond 14 days

Case 1041: F 27 year(s) old 04/05/202 (Confirmec
HK resident Hospitalised Importec case

Case 1040: F 16 year(s) old 01/05/202 (Confirmec
HK resident Hospitalised Importec case

Case 1039: M 35 year(s) old 01/05/202 (Confirmec
HK resident Hospitalised Importec case

Case 1038: M 61 year(s) old 25/ (Cc
HK resident Discharged Epidemiol link import

Case 1037: F 18 year(s) old 25/04/2020 (Confirmed)
HK resident Discharged Imported case

Case 1036: M 58 year(s) old 23/04/202 (Confirmec
HK resident Hospitalised Importec case

FIGURE 1 | Novel coronavirus infection in Hong Kong using ArcGIS.

may only send you information related to a carrier being in a certain location.

For **unicast**, people are informed when a carrier moves into contact with another person. This method was used in China for those who were suspected to be at risk. The message is then targeted to the person who goes close to a suspected carrier. Generally, it is poor in terms of privacy, and it requires detailed surveillance of citizens.

In terms of citizen engagement, the methods of **participatory sharing** is one of the strongest, as users share their locations with a central authority. They may also share information that allows others to understand the risks that they, and others, face. Unfortunately, this method may be open to abuse from fraudulent entities.

Raskar et al. (2020) have also analyzed the risks of these methods based on (**Table 1**) the following points:

- Accuracy: In this, unicast method has the lowest risk.
- Adoption: In this, broadcast method has the lower risk.
- Privacy: In this, broadcast, selected broadcast, and participatory methods have the lower risk.
- Consent: In this, practices vary greatly. For participatory, full consent is required.
- Systemic challenges: In this category, we are dealing with issues like fraud and abuse and the security of information. The risks are considered high in all the categories.

Contact tracing is seen to be a part of reducing the spread of the COVID-19 disease, and many countries of the world have moved to integrate technical solutions for contact tracing. These methods are mainly Bluetooth based where a Bluetooth beacon is sent between Bob and Alice when they are within a given proximity and for a minimum amount of exposure time. At the core of these methods is whether the approach is **centralized** (where those infected are matched on a central server), or **decentralized** (where individuals can do their own matching with full consent). Basically, there are three main entities involved: Bob (who is infected), Alice (who is in contact with Bob), and the HA (Health Authority), as shown in **Figure 2**. We may also introduce Grace, the government official, and Eve, the eavesdropper.

Within a centralized system, Bob and Alice are assigned identifiers that the HA can match whenever Bob and Alice are in contact. This is matched through a privacy-preserving rolling ID, which only the HA can match back to Bob and Alice. Once matched, the HA can then inform Bob and Alice that they have

TABLE 1 | Risks and challenges of contact-tracing technological approaches (reproduced from Raskar et al., 2020).

Intervention	Broadcast	Selected broadcast	Unicast	Participatory	PrivateKit
Accuracy	Limited	Limited	High	Limited	High
Adoption	High	Medium	Medium	Low	Medium
Privacy risks for carriers	Significant	Moderate	Moderate	Significant	Moderate to low
Private risks for local businesses	Significant	Significant	Moderate	Significant	Moderate to low
Privacy risks for users	Privacy-protected	Privacy at risk	No privacy	Privacy protected	Privacy protected
Privacy risks for non-users	Privacy at risk if carriers are identified	Privacy at risk if carriers are identified	Privacy at risk if carriers are identified	Privacy at risk if carriers are identified	Privacy at risk if carriers are identified
Consent of carries	Practices vary	Practices vary	Practices vary, often with little or no consent	Full consent	Full consent
Misinformation and panic	High risk	Medium risk	Medium risk	High risk	Medium risk
Security of information	Low-to-medium risk	Low-to-medium risk	High risk	Low risk	Low-to-medium risk

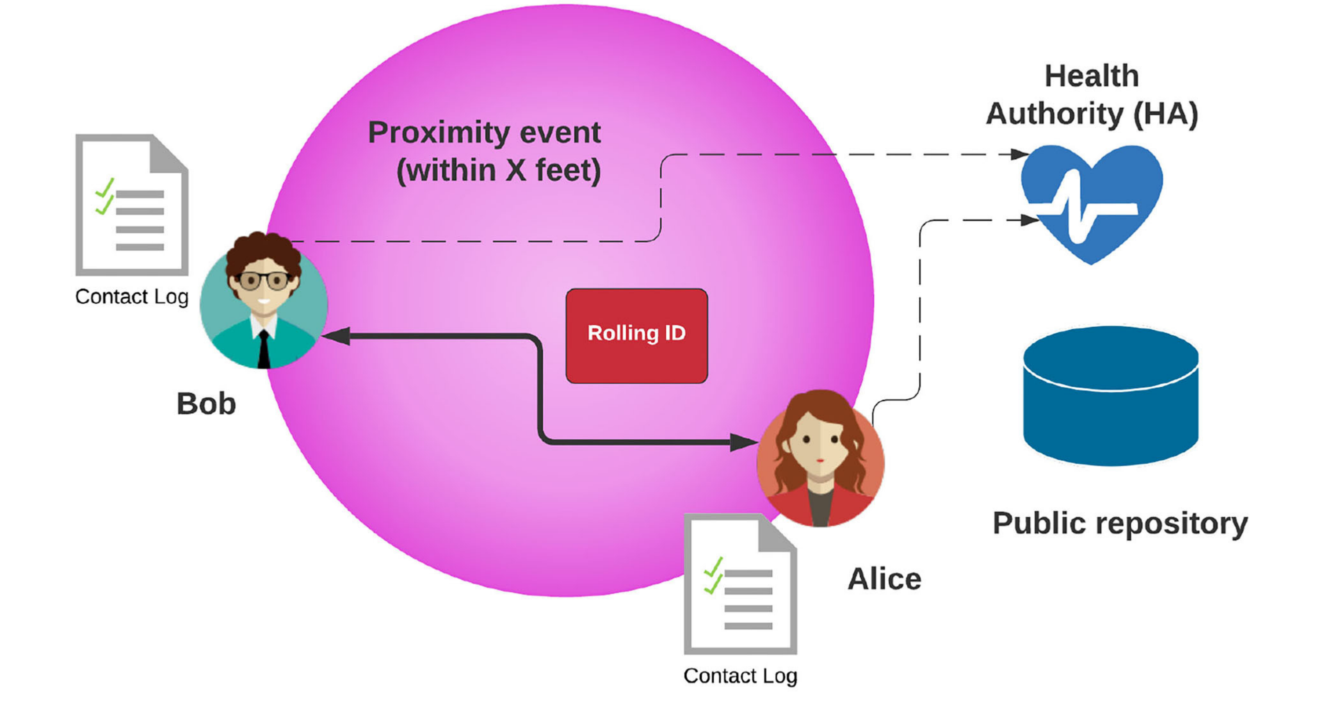


FIGURE 2 | Basic model of contact tracing.

been in contract. In a decentralized system, Bob and Alice send the rolling IDs they receive, and Bob can identify that he has COVID-19. The HA can then keep an ID resolver so that Alice can determine when she has been in contact with Bob. In this way, the HA does not know about the contact between Bob and Alice, but Alice will.

3. CONTACT TRACING APPS FOR COVID-19

Almost three quarters (72.6 %) of Internet users will access the web solely via their smartphones by 2025, which is equivalent to nearly 3.7 billion people (Handley, 2020). The proliferation of mobile devices presents a new opportunity for overcoming the challenges faced by conventional contact tracing techniques in terms of identifying, monitoring, and informing about the spread of a pathogen in densely populated areas, as is the case with COVID-19. A famous example is China, which relied on an elaborate surveillance architecture to actively monitor the location of its citizens using live data and mobility history to enforce self-isolation and conduct contact tracing. Several other countries, such as Korea, Singapore, Israel, Iran, and Russia (Tidy, 2020), have built solutions around the Chinese model. However, these attempts have led to criticisms on privacy and data protection.

A variety of different groups around the globe are working on the same lines to develop a contact-tracing app. The following subsections outline some of the key technologies either defined by organizations, country, or geographical region.

3.1. Apple and Google

Apple and Google have worked together to create an API integration for Bluetooth to track physical proximity between phones. If someone later receives a positive COVID-19 diagnosis, they can report it through the app, and any users who have been in recent contact with the infected person will receive a notification. The system is Bluetooth-only, fully opt-in, collects no location data from users, and no data at all from anyone without a positive COVID-19 diagnosis. Apple and Google chose perhaps the most privacy-friendly of the many different schemes that could allow automated smartphone contact tracing (Charara, 2020a).

The Apple/Google method works by Bob generating a unique 256-bit tracing key for his phone—and where this key must be kept secret (**Figure 3**). Every day he then creates a daily tracing key (diagnosis key), by creating a hash from the tracing key and the current day. From this hash, it should not be possible to determine his tracing key (as it is generated from the random 256-bit tracing key). Every 10 min, he creates a rolling ID key that is an HMAC identifier (a signed hash) of his daily tracing key and a counter for the number of 10 min that have passed that day.

When Alice comes into contact with Bob, she will receive her rolling ID through a Bluetooth Advertisement, and could then pass that back to the HA. The HA cannot correlate Bob from the rolling ID, and whether he has COVID-19 or not. Alice is just blindly sending it back to Trent, in order for the HA to track the contact or not. In order to preserve privacy, the HA should only track if Alice has been proven to be COVID-19 positive.

Once Bob has been proven to have COVID-19, he will send the daily tracing key to the HA, who can then match all the rolling ID keys to his identity. This will only happen for 1 day. As he must send these keys every day, the key feature on the phone will make the decision to send the key daily or not. To enhance security, this design has been updated to integrate AES encryption.

3.2. The United Kingdom

In the UK, KCL, Guys, and St Thomas' Hospitals in partnership with ZOE Global Ltd have proposed C-19 COVID Symptom Tracker 2020. The data are collected through daily self-reporting of a volunteer user and analyzed by machine learning and data science methodologies to predict high-risk areas in the UK while understanding symptoms, and the propagation of the virus.

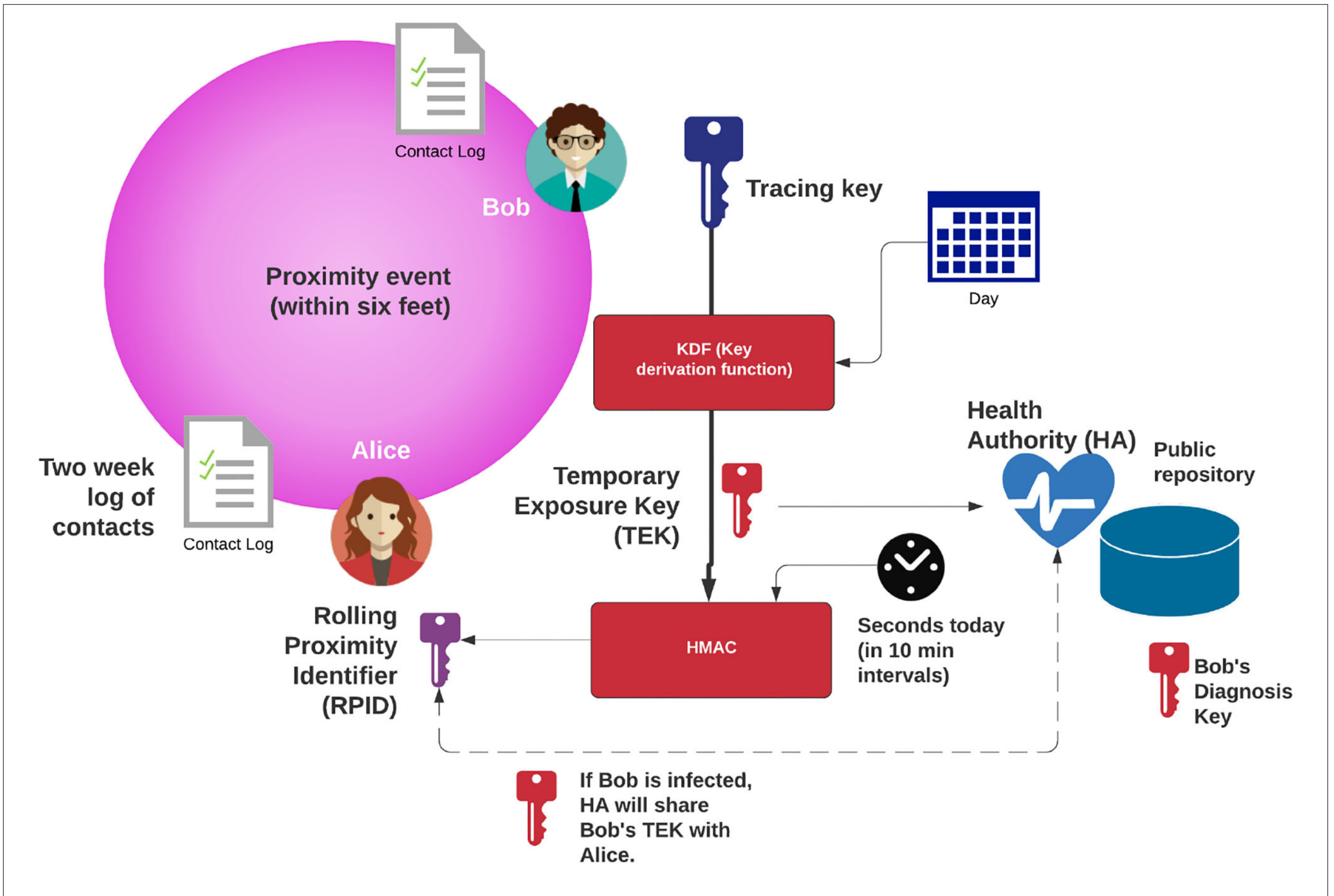

Contact Log
Bob
Proximity event (within six feet)
Tracing key
Day
KDF (Key derivation function)
Two week log of contacts
Contact Log
Alice
Temporary Exposure Key (TEK)
Health Authority (HA)
Public repository
Rolling Proximity Identifier (RPID)
HMAC
Seconds today (in 10 min intervals)
Bob's Diagnosis Key
If Bob is infected, HA will share Bob's TEK with Alice.

FIGURE 3 | Google/Apple ID tracing.

However, the specific application is not widely being adopted because it does not offer any real-time tracing.

Susan Major (Mayor, 2020) defines that around 700,000 people installed the COVID Symptom Tracker app (covid.joinzoe.com) within the first day of its release (**Figure 4**). The research team are critical that the current focus is on deaths rather than tracking the spread of the disease in the percentage of the population who were symptomatic (estimated between 5 and 60%). The App includes information related to age, sex, height, weight, and postcode and lists any chronic health conditions. Along with this users are asked about their current symptoms including whether they have a fever, persistent cough, unusual fatigue, shortness of breath, diarrhea, confusion, disorientation or drowsiness, and loss of appetite. Those reporting symptoms are then sent a home testing kit, and where the data received are then used to report whether they have COVID-19 or not. All of the data collected are anonymized and will be provided back, free of charge, to researchers.

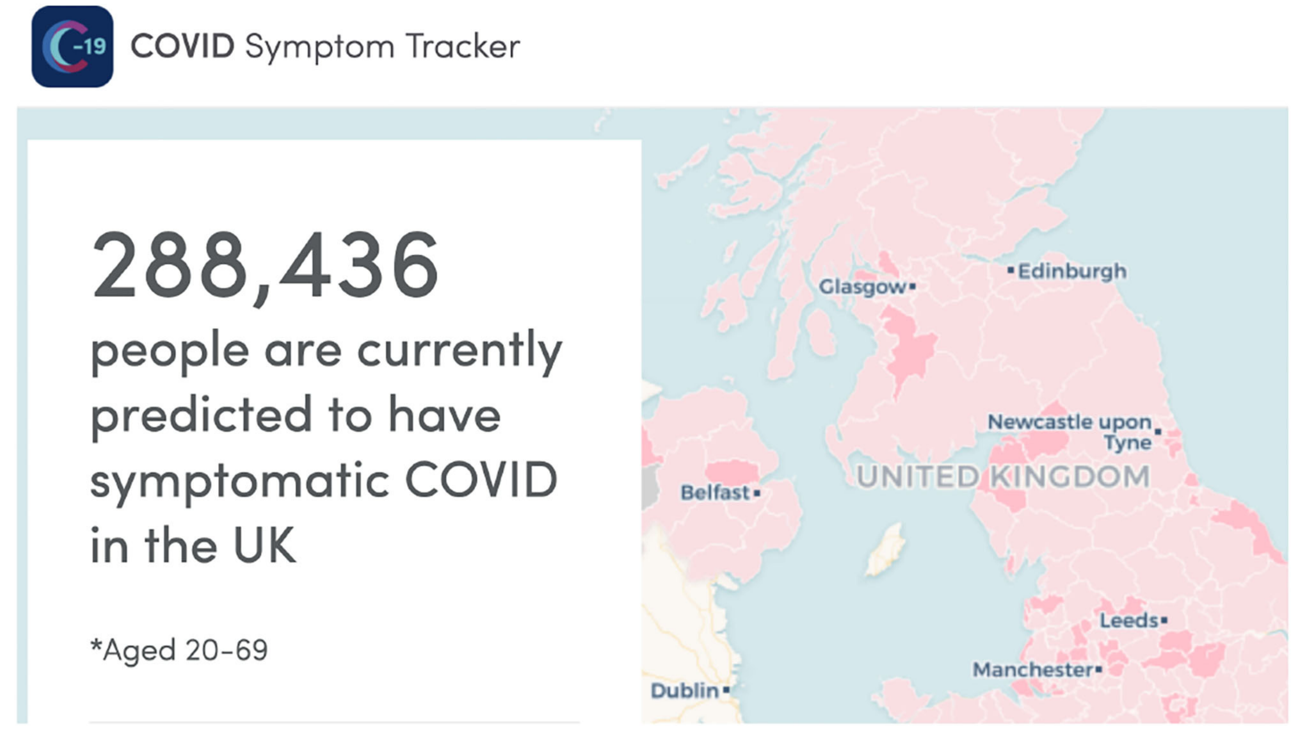
Babylon COVID-19 Care Assistant is developed by Babylon Health (a private healthcare provider) 2020. It is a separate section of an existing artificial intelligence (AI)-based App. As an existing user logs in, they are asked at the beginning of the triage if they are concerned about coronavirus. If they answer yes, they are diverted to the COVID-19 triage, which follows the same criteria of NHS111. The NHS representative provides people with updated information about coronavirus, allows them to log their symptoms, helps them get appropriate assistance, and advice to help them with not spreading the virus wider. The App includes a live chat run by clinical support staff and overseen by doctors.

The UK government developed an NHSX App based on Low Energy Bluetooth. Once installed, the app allowed the logging of the encrypted information of the users operating in the close proximity of the host into a database (Gould and Lewis, 2020). A COVID-19-positive case would lead to the app alerting everyone who was noted to be in the vicinity of the detected user. Within the NHSX App, we use elliptic curve cryptography and use a off-line key exchange method known as ECIES (Elliptic Curve Integrated Encryption Scheme). As illustrated in **Figure 5**, Bob receives an InstallationID, the public key of the HA (*PubKeyS*), and a symmetric key from the HA. Every day he then creates a daily public key pair:

$$DailyPriv = r \tag{1}$$

$$DailyPub = rG \tag{2}$$

where r is a random value and G is the base point on the chosen elliptic curve. Using the public key of the HA and his own daily private key (r), Bob generates a secret value (Z). This value can also be regenerated at the HA with the private key of the server ($PrivS$) and Bob's daily public key (rG). From Z, Bob generates the encryption key, which will protect the InstallationID for Bob. The symmetric key passed is used to sign for the Bluetooth beacon. Finally, Bob adds his daily public key to the beacon. This public key will be used to regenerate the secret value (Z) at the HA, and thus generate the same encryption key. **Figure 6** outlines



COVID Symptom Tracker

288,436

people are currently predicted to have symptomatic COVID in the UK

*Aged 20-69

FIGURE 4 | Covid.joinzoe.com.

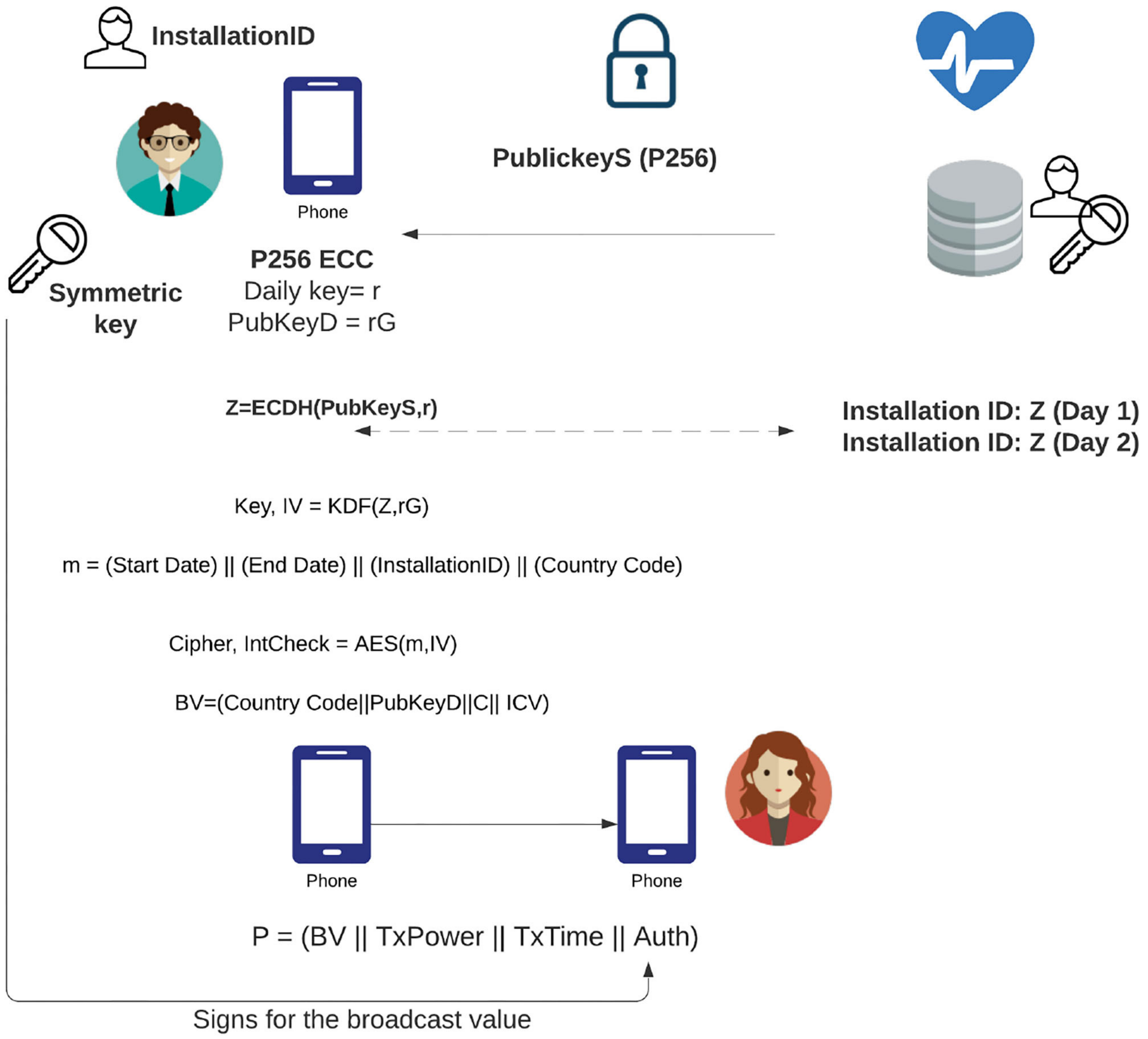

InstallationID
Phone
PublickeyS (P256)
P256 ECC
Daily key= r
PubKeyD = rG
Symmetric key
Z=ECDH(PubKeyS,r)
Installation ID: Z (Day 1)
Installation ID: Z (Day 2)
Key, IV = KDF(Z,rG)
m = (Start Date) || (End Date) || (InstallationID) || (Country Code)
Cipher, IntCheck = AES(m,IV)
BV=(Country Code||PubKeyD||C|| ICV)
Phone
Phone
P = (BV || TxPower || TxTime || Auth)
Signs for the broadcast value

FIGURE 5 | ECIES encryption with the NHSX App.

the decryption process using Bob's daily public key and the HA's private key.

The approach is thus centralized, and where Bob's identity is created by the HA, and then matched back. One possible weakness is where the private key of the HA is leaked, and which will allow all of the derived keys to be generated. Along with this, Bob's public key will be exposed for a day (rather than 10 min in the case of the Apple/Google contact-tracing method). It could thus be possible to trace Bob for 1 day by monitoring his Bluetooth beacons and matching his daily public key. After trails on the Isle of Wright, the app was found to be good at determining distances between devices, but it only found 4% of Apple devices and 75% of Android devices (Staunton, 2020). This led to cancellation of the centralized approach, and a move toward the hybrid approach.

BeepTrace (Xu et al., 2020a) is a blockchain-enabled fully distributed privacy-preserving solution for COVID-19 contact tracing. In this approach, blockchain is adopted to bridge the user/patient and the authorized solvers to desensitize the user ID and location information. Compared with the dominating active mode that adopts Bluetooth or similar technologies to exchange information among contacted users, BeepTrace proposes a passive model by using GPS or some similar device without direct information exchange at the end user side.

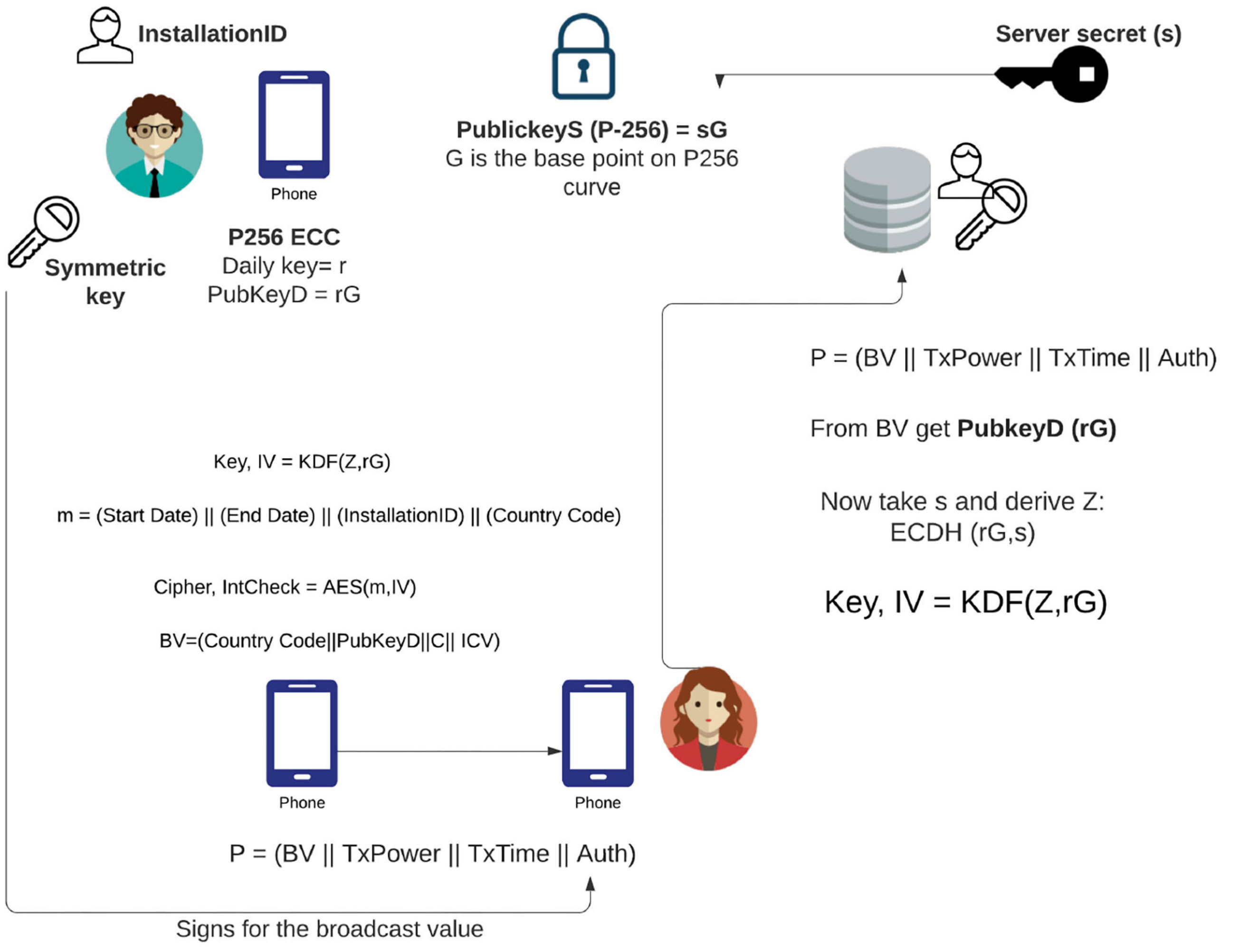

InstallationID
Phone
Symmetric key
P256 ECC
Daily key= r
PubKeyD = rG
PublickeyS (P-256) = sG
G is the base point on P256 curve
Server secret (s)
P = (BV || TxPower || TxTime || Auth)
From BV get PubkeyD (rG)
Now take s and derive Z:
ECDH (rG,s)
Key, IV = KDF(Z,rG)
Key, IV = KDF(Z,rG)
m = (Start Date) || (End Date) || (InstallationID) || (Country Code)
Cipher, IntCheck = AES(m,IV)
BV=(Country Code||PubKeyD||C|| ICV)
Phone
Phone
P = (BV || TxPower || TxTime || Auth)
Signs for the broadcast value

FIGURE 6 | Decrypting Bob's ID with the NHSX App.

3.3. The European Union

The European Pan-European Privacy Preserving Proximity Tracing Initiative (PEPP-PT) proposes an open source Bluetooth-based platform sharing software, standards, and services that can be utilized for the development of COVID-19 contact-tracing apps. Each national health authority can tweak the software according to its own policies and processes. The software aims at measuring proximity data and alerting the traced contacts of a user if detected positive to COVID-19 while adhering to privacy. As an EU initiative, it has a wide approach across national borders 2020.

One of the methods that has been published that tries to address this balance is PEPP-PT. With this, a device requests and ID from the tracking service (Trent) and is given a one-time anonymized ID (and which includes an obfuscation of the country ID). It then use Bluetooth beacons and possibly Wi-Fi to discover and identify neighbors. The method defined in PEPP-PT then uses the signal strength method to estimate the distance someone is away. Note that this is not a GPS tracking method and will just give a circular radius around a person, and possibly amount of time that they were near another phone.

The users must install the tracking application on their phone-possibly they must be forced to do this by their government-and then it will be used to track contacts between one phone and another.

The results are then sent back to Trent with a device identifier for Alice's phone (possibly the Bluetooth MAC address). If the device is a registered device with an anonymous ID, it will send back its neighbor's ID and an estimation of location, and also store this as in the history log.

Overall, there is no personal information stored, and the device just stores anonymized IDs. The history is then deleted when there is a test that the user of the device does not have SARS-Cov-2, but remains encrypted until there is a test to prove that they do not have the virus.

If the user has been proven to have it, the health authority registers the device with a TAN code, and with consent, they register onto a tracking system, and where they allow others they have been in contact with to be alerted to the possible threat of infection. There is no personal information stored. If the phones are from different countries (identified in the anonymous ID), there is an alert send to the health care provider in the other country.

3.4. DP-3T

The DP-3T is decentralized and open sourced (Troncoso et al., 2020). It involves a collaboration of eight different countries. It general defines a number of objectives:

- Anonymous identifier donation: This uses a short-term anonymous identifier (ID) and includes a measure of the Bluetooth signal strength.
- Logging the proximity history: This only stores proximity information when within an epidemiologically sufficient proximity. No geo-location information is stored.
- Usage of the proximity history: The data are stored in an encrypted form if the user has not been tested, or is clear. When tested positive, the Health Authority contacts the user, and provides a TAN code, and where the user then consents to reveal their history.
- Country-dependent trust service operation: If the phones are from different countries (identified in the anonymous ID), there is an alert send to the health care provider in the other country.

3.5. France

In France, Covidom App is developed to monitor COVID-19 patients who have been through Paris hospitals and either identified as COVID-19-positive or suspected of being infected but do not require hospitalization but are staying at home (Martinetti, 2020). The application is based on a daily digital online questionnaire asking the patient about their respiration, heart rate, and temperature. Depending on the response of the patient, the healthcare team is alerted and contacts the patient to adapt the follow-up and treatment. The app is voluntary and does not have any real time contact tracing capability.

3.6. Poland

In Poland, Home Quarantine App is developed and endorsed by the Government. Its use is mandatory for 14 days to people returning to Poland from abroad and for those who are COVID-19-positive (Hamilton, 2020). The app is based on Instagram and require the people to upload their selfies within 20 min of receiving an alert. Instagram's geolocation and facial recognition capabilities are used to ensure that the people are adhering with self-quarantine.

3.7. Germany

Germany has Corona Data Donation App that gathers the vital signs (pulse, temperature, sleep) of volunteers and analyze the probability of testing positive for COVID-19 using wearable technology (Busvine, 2020). An online interactive map is generated based on this information to depict the geographical spread of the virus.

3.8. Russia

The Russian Social Monitoring App tracks the self-isolated COVID-19 patients' whereabouts through user's calls, location, camera, storage, network information, and other data (Maynes, 2020).

3.9. China

In China, Health Code App—developed by the Government, WeChat, and Alipay—tracks people's symptoms and issues real-time individual health status using a three-color scheme (green, yellow, and red) (P. Mozur and Krolik, 2020). Real-time location and tracing based on GPS, existing WeChat/Alipay payment system, mobile network, and traffic data with advanced machine learning/big data analytic is employed to enable accurate detection and fast alerting. The app usage is compulsory and may lead to potential data/privacy issues as well as discriminating behaviors based on color schemes.

3.10. South Korea

In South Korea, Corona 100 m (Co100) App allows those who have been ordered not to leave home to stay in contact with case workers and report on their progress (Wray, 2020). The app uses GPS to keep track of infected people's location to make sure they are not breaking their quarantine. It also alerts users when they come within 100 m of a location visited by an infected person. Machine learning/data science tools are however not used to track/trace travel history and make real-time alerts to the public. The app is not mandatory, and a user can opt out.

South Korea's Ministry of Interior has also introduced a mandatory GPS-based Self-quarantine Safety Protection App to support officials to monitor citizens in quarantine 2020. An alert is sent to both patient and case worker, if the patient leaves their quarantine zone. Citizens can self-report their symptoms.

3.11. Singapore

Singapore have introduced TraceTogether, a Bluetooth-based app that traces and identifies those who have been exposed to a COVID-19-infected person 2020. The scan history is stored locally. The participation is voluntary, and no real-time alerting and tracing is available. TraceTogether uses Bluetooth and keeps a track of all the contacts made within a 21-days period (McCall, 2020). It only stores contacts and not the actual locations of the phone. If the Ministry of Health requires the contact history, they ask the user for consent to share it. The logs are encrypted on the device, and only decrypted once the logs are uploaded on the Department of Health website. Contract tracers then use the logs to match to those who the user has been in contact with. Bluetooth was selected due to the inability of GPS to locate accurately within buildings (as the GPS methods on phones only estimate within buildings).

3.12. India

In India, AarogyaSetu App uses GPS and Bluetooth to track the people who have symptoms and identify people who have been in close proximity to them 2020. The participation is voluntary, and the location and contact history stay on the device unless a user is COVID-19 infected in which case the person's data is sent to the cloud. The app traces travel/contact history but no real-time alerting is available.

COVID-19 Quarantine Monitor Tamil Nadu App is also an Indian initiative that tracks a quarantined user. The voluntary used app enables live location tracking via GPS and generates alerts (Sivapriyan, 2020a). The Apps in India have no underlying legal framework for privacy protections in place.

3.13. The United States

In the United States, MIT developed Safe Paths App, which uses Bluetooth to track users and share locations between them (Sivapriyan, 2020b). Safe Paths collects users' location data, keeping a time-stamped log every 5 min, and is encrypted and stored locally. In total, 28 days of data can be stored in the app in under 100 kb of space (that's less storage space than a single photo takes up). If a user is tested positive for COVID-19, they can share these data to health official by using a QR code, thereby facilitating contact-tracing 2020. It also compares recent locations against the path of an infected person and alerts them of potential contact. SafePaths uses Bluetooth tracing and GPS methods (Cho et al., 2020). **Figure 7** outlines that SafePaths has strong methods of data privacy and data utility (Raskar et al., 2020).

With SafePaths, the server limits clients to *N* location points per exchange, and also limits the number of queries that a client can request every day. This stops an adversary mapping out a whole geographical area with continual requests.

How We Feel App, developed by Pinterest with the help from Harvard, Stanford, MIT, University of Maryland, Weill Cornell, and the Howard Hughes Medical Institute, gathers the data on user's health, age, and zip code (information, such as name, phone number, or email is not collected). The data are then aggregated and shared with researchers, public health professionals, and doctors 2020.

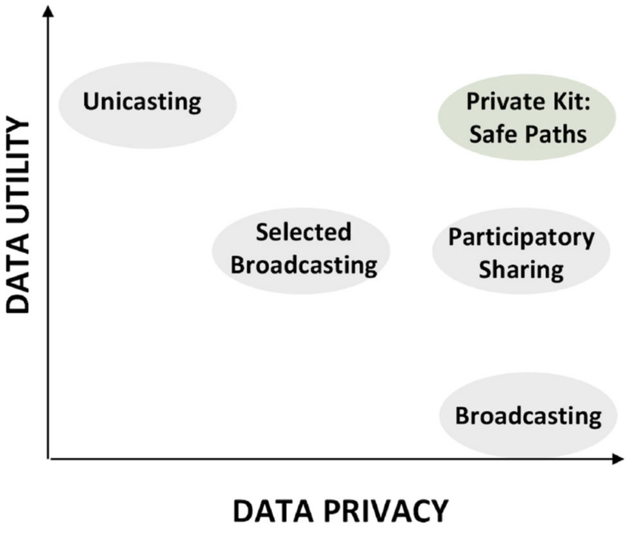


FIGURE 7 | Data privacy and data utility.

MIT is developing a Bluetooth-based Private Automatic Contact Tracing App, where individuals enable their phone to continuously send out random data strings and keep a log of those from other participating devices it has encountered (Muoio, 2020). When a user is diagnosed with COVID-19, they would receive a QR code notifying a cloud system of their status. All other participants in the system would be able to scan the collective logs and would be warned of a potential (but still anonymous) COVID-19 contact.

The US Health Weather Map App is created by Kinsa Insights and Oregon State University. It is currently being used to track *typical illness levels*, such as self-reported fevers (**Figure 8**). This type of application could be used to crowd source population health information, and on a scale that public health authorities would struggle with.

3.14. Iran

The Iranian Ministry of Health developed a contact-tracing app requiring the user to register using his/her mobile number. The app uses GPS data to identify the user's location. It also requests permission for identifying the user's activity and shares the self-declared attributes of the user with the server including gender, name, height, and weight (Chrysaidos, 2020). Although removed from the Google Play Store, the app is still available from other application stores (Cimpanu, 2020).

3.15. Israel

The "Hamagen" App from Israel's Health Ministry collects location history of the user using GPS in the background and compares the user's movement with the health ministry's data. If a user has come in close contact with a COVID-19-positive user, an alert is sent to the user directing them to a website containing details on further actions. Though it is stressed that all the information is stored on the user's smartphone, the App comes alongside controversial temporary powers granted to Shin Bet security agency allowing them to track the movements of smartphones users via their devices and sending alerts to those who may have been exposed to COVID-19 being in contact with a confirmed infected user (Winer, 2020a).

3.16. Australia

The Australian government has launched a Bluetooth-based contact-tracing app COVIDSafe. The voluntary participation registers a user with name, age range, postcode, and phone number. The system creates a unique encrypted reference code for the user. When the app recognizes another device having the COVIDSafe App, it notes the date, time, distance, and duration of the contact, and the other user's reference code in the form of encrypted data in the user's phone.[1] When a user is detected as COVID-19 positive, this app data are acquired by the health officials who the send the alerts of possible exposure to the people traced as being in contact with that user.

[1] Covidsafe app. Available online at: https://www.health.gov.au/resources/apps-and-tools/covidsafe-app (accessed May 6, 2020).

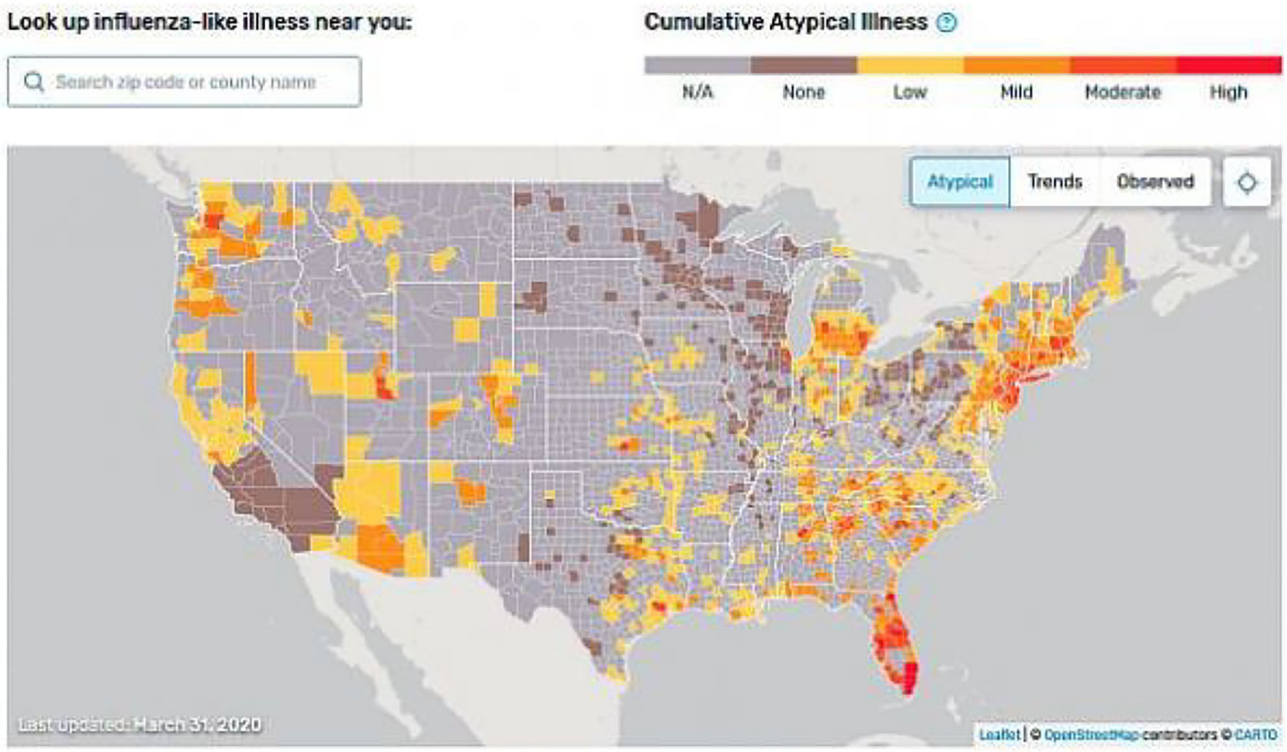

Look up influenza-like illness near you:
Search zip code or county name
Cumulative Atypical Illness
N/A
None
Low
Mild
Moderate
High
Atypical
Trends
Observed
Last updated: March 31, 2020
Leaflet | © OpenStreetMap contributors © CARTO

FIGURE 8 | Fever map in the United States.

3.17. EPIC

The EPIC contact tracing system uses homomorphic encryption in matching users up for possible contacts in a defined time window (Altuwaiyan et al., 2018). First, Alice defines data in time stamps and stores homomorphically encrypted timestamps for her location:

```
E(TIME1)a E(Location1)a
E(TIME2)a E(Location2)a
E(TIME3)a E(Location2)a
```

where E(TIMEx)a is the homomorphically encrypted timestamp value, and E(Locationx)a is the homomorphically encrypted location information. Then, Alice and Bob upload their homomorphically encrypted time stamp and location information to the HA, who stores these values:

```
E(TIME1)a E(Location1)a
E(TIME2)a E(Location2)a
E(TIME3)a E(Location2)a
E(TIME1)b E(Location1)b
E(TIME2)b E(Location2)b
E(TIME3)b E(Location2)b
```

The HA cannot tell either the time stamp or the location information. Alice is now identified as having COVID-19, and the server can identify her encrypted values and runs a homomorphic difference on the timestamps and location (**Figure 9**).

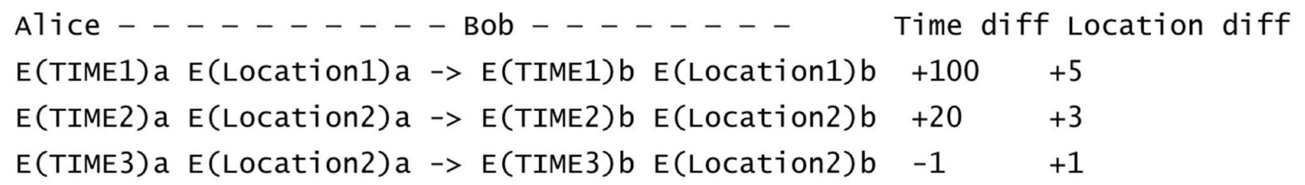
Here the HA cannot tell where Bob and Alice were and at what time, but they can tell that there was a match for a 1-s difference and if they were 1 m away from each other. In this way, Bob could be informed of a possible infection. Other information is also stored, which can be used for the matching process, such as the device type, the SSID of the wireless access point that they connected to, and the RSSI (Received Signal Strength Indication), as shown in **Figure 10**.

3.18. TraceSecure

In TraceSecure (Bell et al., 2020), the authors proposed two private contact tracing methods using Bluetooth signals. The first one extends the TraceTogether application (Cho et al., 2020) by integrating a secure message-based protocol, while the second one incorporates a public key infrastructure that elaborates additive homomorphic encryption.

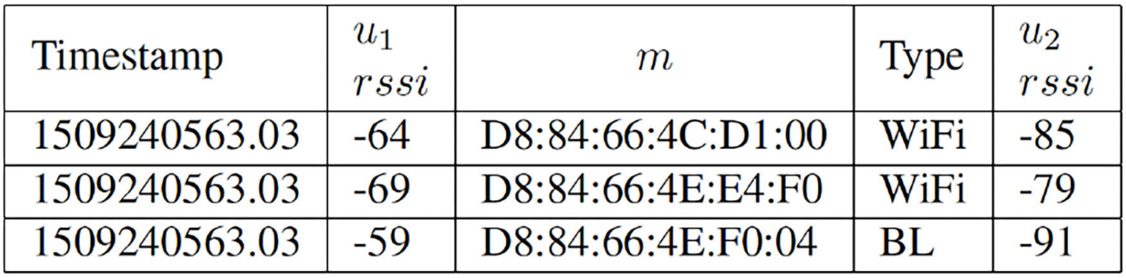
3.19. Cryptographic Preservation of Privacy

Another approach based on GPS location data that incorporates strong encryption techniques, such as Private Set Intersection (PSI), has also been developed (Berke et al., 2020). The goal was the development of an infrastructure that not only promotes stronger privacy guarantees than the methods being adopted from the governments, but also feasible practically. However, the performance overhead of a technique like this is being questioned



```
Alice − − − − − − − − − − − Bob − − − − − − − − −      Time diff Location diff
E(TIME1)a E(Location1)a -> E(TIME1)b E(Location1)b  +100    +5
E(TIME2)a E(Location2)a -> E(TIME2)b E(Location2)b  +20     +3
E(TIME3)a E(Location2)a -> E(TIME3)b E(Location2)b  -1      +1
```

FIGURE 9 | Google/Apple ID tracing.



Timestamp	u_1 $rssi$	m	Type	u_2 $rssi$
1509240563.03	-64	D8:84:66:4C:D1:00	WiFi	-85
1509240563.03	-69	D8:84:66:4E:E4:F0	WiFi	-79
1509240563.03	-59	D8:84:66:4E:F0:04	BL	-91

FIGURE 10 | Signal strength.

(Bell et al., 2020). Though the Epione (Trieu et al., 2020) solution uses lightweight cryptography to provide strong privacy, a real-world implementation has not been developed yet.

4. KEY ENABLING TECHNOLOGIES

Location data are pivotal to any contact-tracing solution. These solutions are based on the assumption that if two persons have shared a close proximity, they have contacted with each other. AI-based technologies, such as facial recognition can be employed to reduce the number of false positives however; their limited availability restricts their usage. On the other hand, universal usage of mobile devices, smartphones, and Internet, GPS, Bluetooth beacons, Wi-Fi, telecom cell towers, and social media can be effectively used to collect the user's location data. GPS, Wi-Fi routers, and cell towers provide absolute location data in the form of geolocation coordinates while Bluetooth pairing gives relative location data in the form of some reference description of the location, for example, both persons shared the same bus (Tang, 2020).

Bluetooth tracing has emerged as the most suitable method for contact tracing in the backdrop of COVID-19 (Brack et al., 2020). However, it has its own deficiencies that limits its capabilities. Methods, such as private messaging for notifications of possible contacts after collecting Bluetooth IDs (Cho et al., 2020), use of geolocation information (Winer, 2020b), using Wi-Fi access, cellular network usage, social media, radio frequency identification, and wearable devices have the potential to be used as contact tracing enablers. It is also possible to use smartphone built-in sensors, such as gyroscope and magnetometer to correlate similar locations without revealing the actual coordinates where they occurred (Jeong et al., 2019).

Contact tracing solutions does not have a uniform system architecture. While countries rush to deploy the contact tracing apps, they raise a multitude of privacy and data protection issues. In this section, we discuss the technologies that can be effectively used to carry out contact tracing in the backdrop of COVID-19.

4.1. Real-Time Location System (RTLS)

Real-Time Location System (RTLS) refers to any system that accurately determines an item or person's location. RTLS is not a specific type of system or technology, but rather is a goal that can be accomplished with a variety of systems for locating and managing assets. An important aspect of RTLS is the time at which users are tracked, and these data can be used in different ways depending on the application. For example, some applications only need timestamps when a user passes through an area, while other RTLS applications require much more granular visibility, and entail that time data be updated constantly. An ideal RTLS can accurately locate, track, and manage assets, inventory, or people and help authorities to make knowledgeable decisions based on collected location data. RTLS is used across many industries including manufacturing, mining, and healthcare industries.

All RTLS applications will consist of a few basic components including a transponder, a receiver, and software to interpret the data. The complexity of the system, chosen technology, and scope of the application will determine the amount of hardware and software required to create the ideal RTLS.

- **Global Navigation Satellite Systems (GNSS)**: Ever-growing demand of navigation and positioning facilities to be available in portable devices has made the GNSS an essential part of the modern communication applications, especially the mobile phones. A Federal Communications Commission (FCC) adoption to enhance the provision of emergency services by tracking a user's location through his mobile also necessitates the integration of the GPS to the cellular phones (Miller, 1998). The usage of GNSS for navigation-enabled smartphones is predicted to rise to 6.5 billion in 2020 2017.

GNSS facilitates innovative tracking solutions, including the deployment of local geofences that trigger an alarm when a user leaves the perimeter. GPS delivers the navigation and positioning services worldwide being the only fully functional satellite navigation system at present. The navigation systems are based on a fundamental positioning procedure where knowing the distance from an unknown location to a certain number of known locations allows finding the coordinates of the unknown position. In the GPS, a number of satellites orbiting the earth provide the known locations while the position of the user on earth with a receiver is the unknown location (Logsdon, 2012).

To determine 3-D position of the receiver, the principle of triangulation is used through the measurements of time delay between transmission and reception of each GPS radio signal transmitted by the GPS satellites. The distance between the user and the satellite is calculated from this time delay as the speed of signal (equals to the speed of light) is already known. The GPS signals also carry information about the location of the satellites. By determining the position of and distance to at least three satellites, the GPS receiver can compute its position in terms of latitude, longitude, and height (**Figure 11**). However, a fourth satellite is also required for a timing offset that occurs between the clock in the receiver and those in the satellites due to poor synchronization. Using the data from

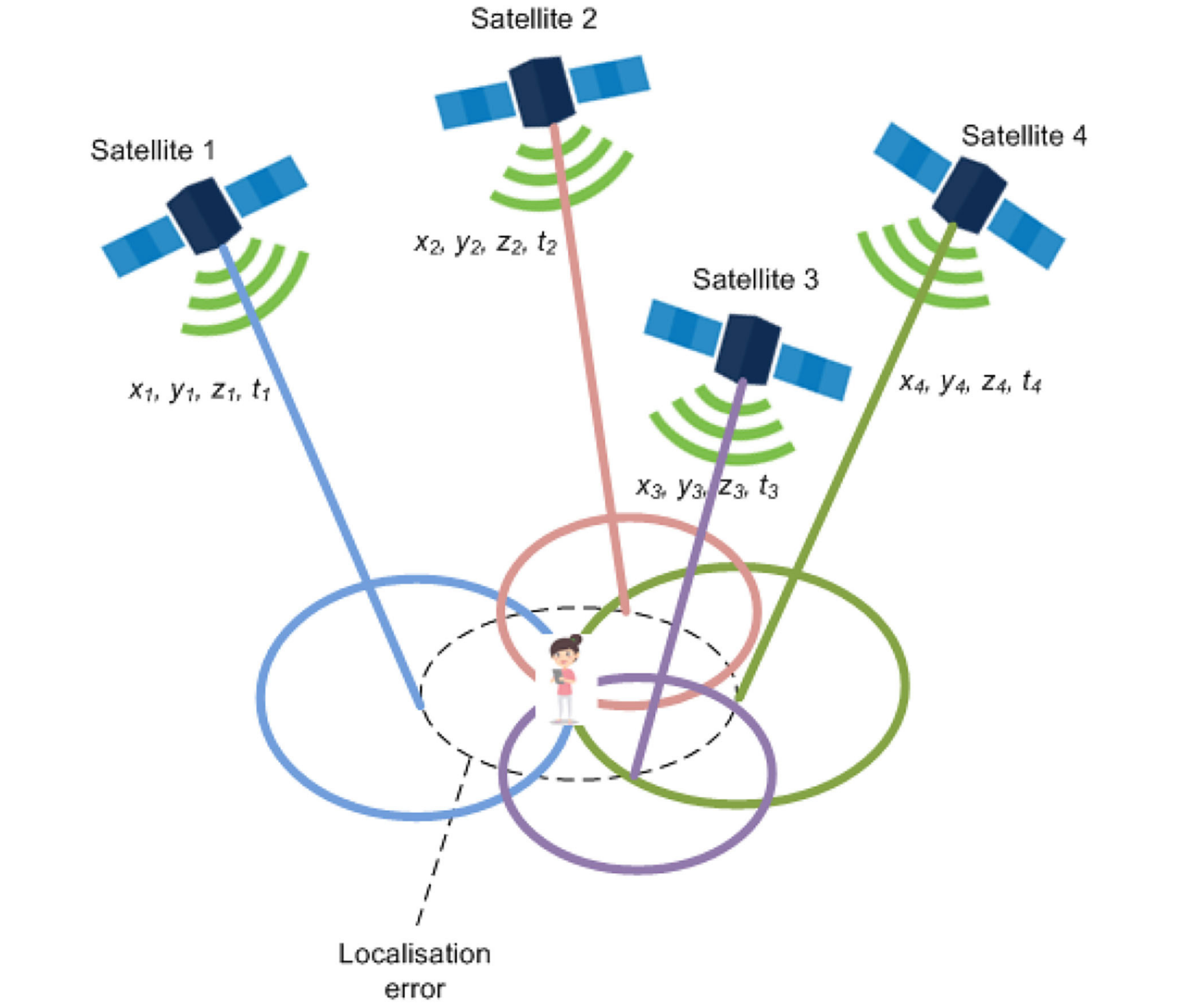


FIGURE 11 | Global positioning system (GPS) position calculation using triangulation.

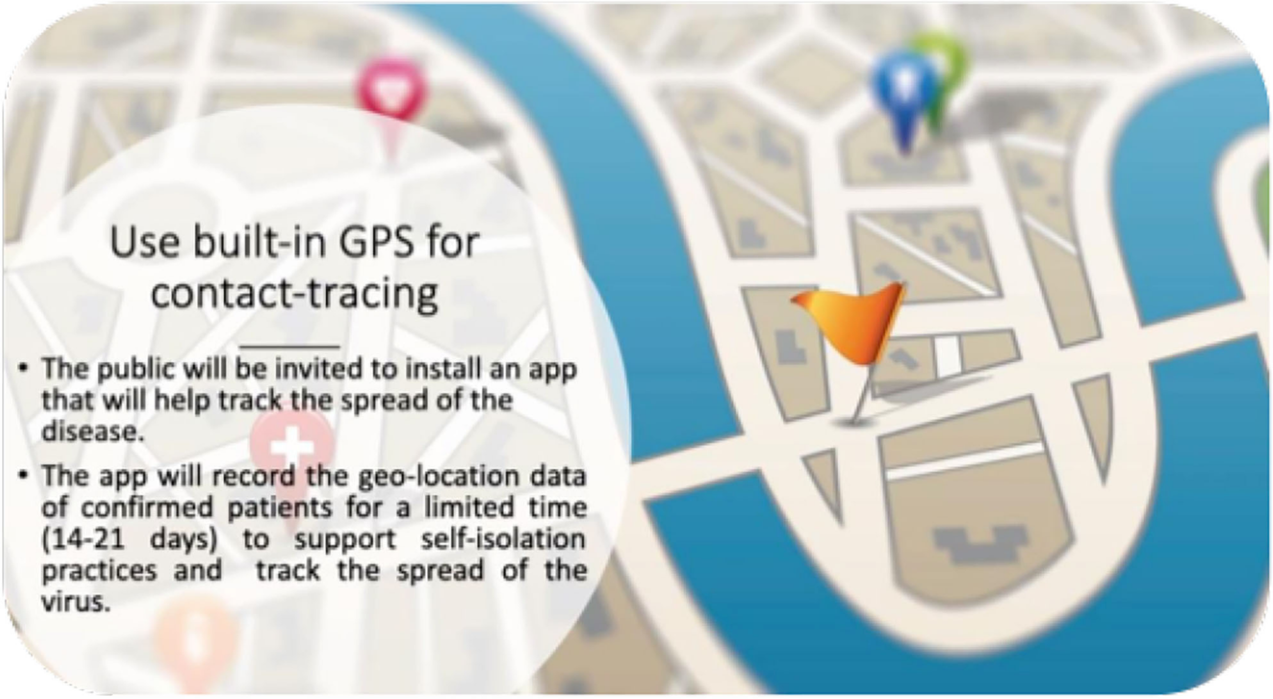
the fourth satellite, the receiver can find this timing offset and hence can eliminate it (El-Rabbany, 2002; Ur Rehman, 2010; Logsdon, 2012; Januszewski, 2018).

GPS localization is a fundamental tool in identifying the location of a smartphone user. By maintaining the database of geolocation information, people whose devices were in the same area in a certain time duration can easily be found. In the context of COVID-19, a user's mobility history could be maintained for the last 14 days and securely stored on a restricted cloud server. Mobile phones whose owners have tested positive would be flagged on the app, and big data analytics would be used to determine which other phones have been in the proximity of that positive case within the historic window. Targeted messages could then be sent to phones that came in close contact, advising owners on whether to seek self-isolation or medical help. There would be minimal need for personal information as only the GPS location of the phone is required to identify the risk of exposure. Location and GPS data would also help officials to build maps of "transmission zones" that could paint a picture of how and where the disease is spreading (**Figure 12**).

GPS tracking however is a significant drain on mobile phone batteries and is not accurate enough as GPS-enabled smartphones are typically accurate within a 4.9 m caused by signal blockage due to buildings, bridges, trees, etc., indoor, or underground use and multipath reflection. Privacy is also another issue that restricts the wide usage of GPS for public location tracking. Another concern is spoofing attacks where a spoofer creates a false GPS signal with an incorrect time and location to a particular receiver (Dar et al., 2020).

- **Bluetooth**: Contact tracing apps leveraging Low-power Bluetooth Communication (LBC) passively collect information about surrounding Bluetooth IDs by doing regular scans (Altuwaiyan et al., 2018). The user grants the app access to the phone's Bluetooth, which it uses to search for nearby Bluetooth devices (within 5–10 m range). The phone then stores the list of Bluetooth devices it has encountered. Traditionally, a centralized approach is adopted where scans of individuals are uploaded to a central server database administered by health officials. Each scan includes the information of control flags, adjacent node ID, contact start time, contact end time and distance (discretized to "Close," "edium," and "Far" based on RSSI value) from the near contact. Pairwise matching scores between user data and the database are regularly calculated to identify contacts, whom a given user has been close to in the past 14 days.

If a user turns COVID-19-positive, the list of Bluetooth devices encountered can be fetched, and the owners advised on whether to get tested or go into self-isolation. Additionally, Bluetooth beacons could be placed at specific locations, such as grocery stores or in train coaches to determine which phones have visited those locations (at a specific date and time) (Vaudenay, 2020). This system can also alert venue managers to close or carry out a general sanitization of the location/venue if a severe case or cluster of cases are identified (Avitabile et al., 2020). Bluetooth addresses some



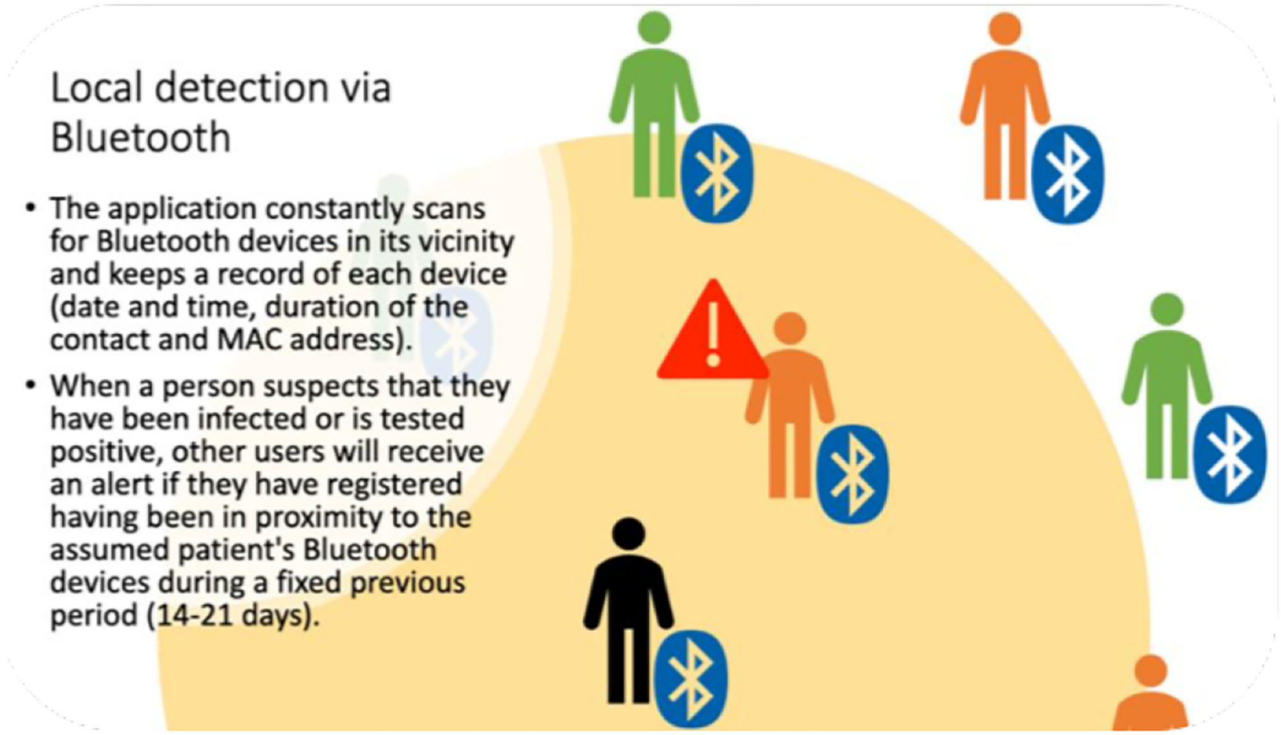
Use built-in GPS for contact-tracing

- The public will be invited to install an app that will help track the spread of the disease.
- The app will record the geo-location data of confirmed patients for a limited time (14-21 days) to support self-isolation practices and track the spread of the virus.

FIGURE 12 | Active global positioning system (GPS) tracking.

disadvantages of GPS and expands the usability of the app with further qualities, as shown in **Figure 13**.

Systems using Bluetooth communication for automatic contact tracing has been first proposed by Altuwaiyan et al. (2018). However, there are challenges to be addressed: First, apps like TraceTogether 2020 that works on similar idea of exploiting LBC for contact tracing are prone to information leakage due to centralized architecture. Second, the range of Bluetooth is more than 1.5 m and can penetrate through walls, hence people in different rooms and behind other obstacles may also be regarded as being in contact generating false positives as shown in **Figure 14**. Bluetooth addresses some disadvantages of GPS and expands the usability of the app with further qualities, as shown in



Local detection via Bluetooth

- The application constantly scans for Bluetooth devices in its vicinity and keeps a record of each device (date and time, duration of the contact and MAC address).
- When a person suspects that they have been infected or is tested positive, other users will receive an alert if they have registered having been in proximity to the assumed patient's Bluetooth devices during a fixed previous period (14-21 days).

FIGURE 13 | Local detection via Bluetooth.

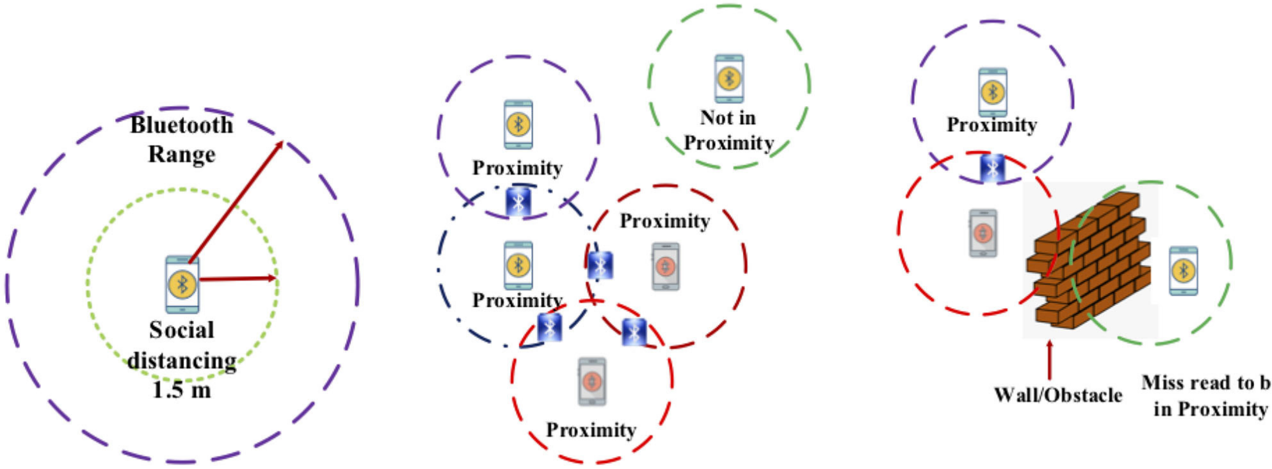


FIGURE 14 | Proximity and not-in-proximity scenarios in Bluetooth contact tracing.

Figure 14. The effectiveness of Bluetooth-based approach however depends on the massive adaptability of the App 2020 and slow or low rate of adoption reduces its usefulness (Dar et al., 2020).

The privacy concerns can be addressed by incorporating cryptographic techniques to generate random keys and use them instead of phone IDs', which are not just anonymous, but pseudonymous, constantly changing their "ID," and that cannot be tracked back to an individual (Gold, 2020). These contact-tracing keys will sit on your device, rather than in a centralized server. Moreover, peer-to-peer decentralized contact-tracing mechanisms (Brack et al., 2020) can be incorporated using distributed hash tables that makes use of blind signatures to ensure messages about infections are authentic and remain unchanged. Although Bluetooth can, with its wide range, detect another phone in its vicinity but cannot pinpoint which direction the contact is coming from. Ultra-wide band chips (Greenberg, 2020) in the latest smart phones can help since it is possible to determine how close a person is by sending billions of pulses across a wide range of frequencies. However, the limitation is that not many phones have UWB (ultra-wideband) chips and they can only communicate with each other.

- **Wi-Fi Router Tracing**: Wi-Fi currently carries more than 60% of the world's Internet traffic (Charara, 2020b). Smartphone-based localization methods employing wireless signals, such as Wi-Fi enjoy more popularity due to the use of off-the-shelf internal sensors, and relatively low cost (Huang et al., 2020). Ubiquity of Wi-Fi access through massive deployment of Wi-Fi routers can be exploited to gain the knowledge of a user's mobility data. These mobility traces are unique and identify the users accurately giving information about home and work locations, visited places, and personality traits (De Montjoye et al., 2013a,b). High-resolution mobility patterns of entire social systems can perform an important role to ensure social distancing and combat the spread of epidemics including COVID-19 on multiple scales (Eubank et al., 2004; Liang et al., 2013; Sun et al., 2014; Sapiezynski et al., 2015).

When a smartphone user is within the range of a publicly available Wi-Fi and wishes to use it, it transmits a probe request to the router containing its globally unique Media Access Control (MAC) address. The router assigns a unique IP address to the user and maintain an entry into the Dynamic Host Client Protocol (DHCP) table. Most of the providers also ask for additional information, such as name, email, location tracking, etc., to use it for business adverts. Using RSSI, MAC address, personal information, and timestamps for the probe request of a user, the router can easily generate a Wi-Fi signal map detecting the location of a user and duration of his presence based on the services used (**Figure 15**). Cross-referencing and basic analysis of logs from various routers will enable tracking in the locations a user visited, how long he spent in a specific area and how fast he moved from place to other. The average coverage range of the Wi-Fi is 80 m outdoors and 50 m indoors, limiting positioning to 4–15 m. A combination of Wi-Fi with GPS is being used by Google, Apple, Microsoft, Skyhook, etc., to improve positioning (De Montjoye et al., 2013b).

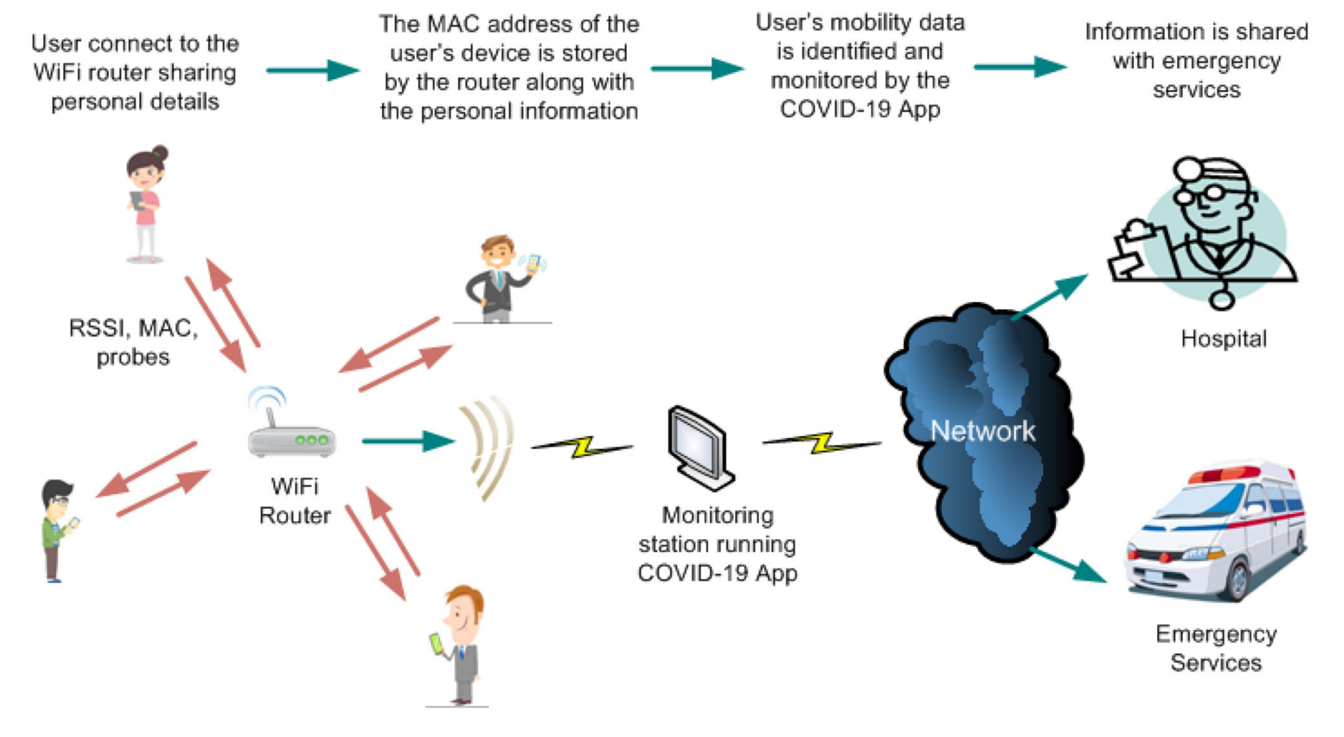

User connect to the WiFi router sharing personal details
The MAC address of the user's device is stored by the router along with the personal information
User's mobility data is identified and monitored by the COVID-19 App
Information is shared with emergency services
RSSI, MAC, probes
WiFi Router
Monitoring station running COVID-19 App
Network
Hospital
Emergency Services

FIGURE 15 | Wi-Fi contact-tracing approach.

The mobility data of an app user who self-diagnoses would identify the locations they have visited and people who have been in the vicinity (using the same router for Wi-Fi access). An alert would then be generated to advise these people to self-isolate.

- **Radio Frequency Identification (RFID)**: RFID is one of the major identification technologies used today covering almost every aspect of our daily life. Applications of this electromagnetic waves-based identification method include access to buildings and transportation, animal tracking, patient monitoring, personal identification, facilitating the inventory and shipping of goods, assembly lines and supply chains, tagging food and retail items, localization, and even providing assistance for visually impaired persons (Chawla and Ha, 2007; Finkenzeller, 2010; Dobkin, 2012).

  RFID technology has accomplished a major development in the last decade, mainly due to the reduction in the cost of RFID chips and huge developments in microelectronics and RF domains. **Figure 16** illustrates a typical RFID system that comprises a set of remote transponders known as RFID tags and an RFID reader. RFID tags include an antenna and an application-specific integrated circuit (ASIC) also known as a chip, containing the data about the tagged object. The RFID reader generates a query signal toward the RFID tags and the tag replies back with data. The readers are usually connected with some embedded systems, host computers having application software to collect and share data.

  The passive ultra high-frequency (UHF) tags typically consist of three elements: (1) transponder (packed in ASIC or simply an RFID chip), (2) antenna, and (3) dielectric substrate. Passive tags are usually very simple devices (**Figure 6**) and therefore, much cheaper (typically costing around $0.10) than other types of radio devices. Passive tags do not require maintenance and have a long life, which is limited by the degradation of the label material rather than the use of batteries. Passive tags are expected to be readable for 10–20 years in many environments (Harrop and Das, 2005; Landt, 2005; Das, 2010, 2016, 2018; Zanella et al., 2014; Al-Fuqaha et al., 2015; He and Das, 2015; Griggs et al., 2018).

  UHF RFID uses passive tags attached to the smartphones and objects. It enables tracking of location of COVID-19 patient as well as items touched/used by him through RTLS. The RFID reader antenna with beam steering capability will be used to read tag angle and RSSI; the tag proximity with other tags will be estimated by applying signal processing and machine learning techniques. RFID reader antenna will also not interfere with other RFID readers behind the walls/obstacle. A hybrid of Bluetooth and RFID can therefore be used to mitigate the drawbacks of Bluetooth and improve the accuracy (**Figure 17**). The hybrid technique also has significant privacy advantages over GPS-based location tracking.
- **UWB 5G Positioning**: 5G networks use large antenna arrays and ultra-wide bandwidths (UWB). They enable a decimeter level accuracy in location systems. Unlike other positioning technologies, such as GPS, Bluetooth, or Wi-Fi, UWB technology uses RF signal's Time Difference of Arrival (TDOA) or time of flight to estimate the distance between target and reference base station that provides more accuracy with much more precise range measurement as shown in **Figure 18**. However, these systems are not yet fully operational.

4.2. Mobile Network Tracing

Mobile network operators already hold information on subscriber location and mobility history, albeit the resolution of

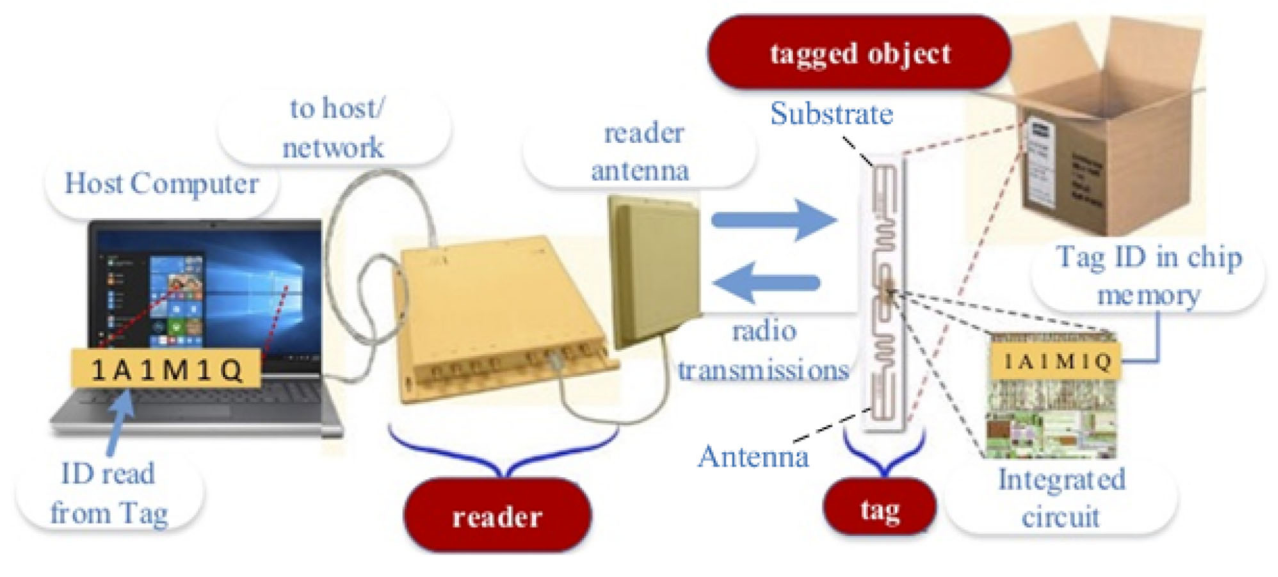


FIGURE 16 | Key components in a typical radio frequency identification (RFID) system.

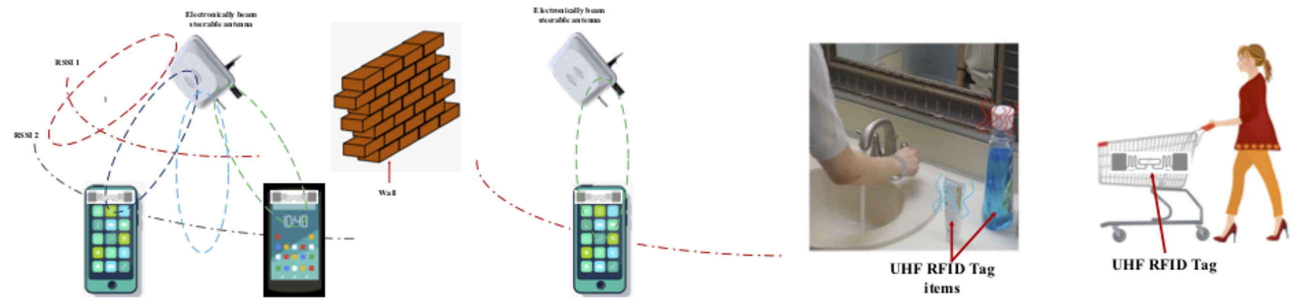

Electronically beam steerable antenna
RSSI 1
RSSI 2
10:40
Wall
Electronically beam steerable antenna
UHF RFID Tag items
UHF RFID Tag

FIGURE 17 | Reading the proximity of radio frequency identification (RFID) tags using UHF RFID technology with beam steerable antennas.

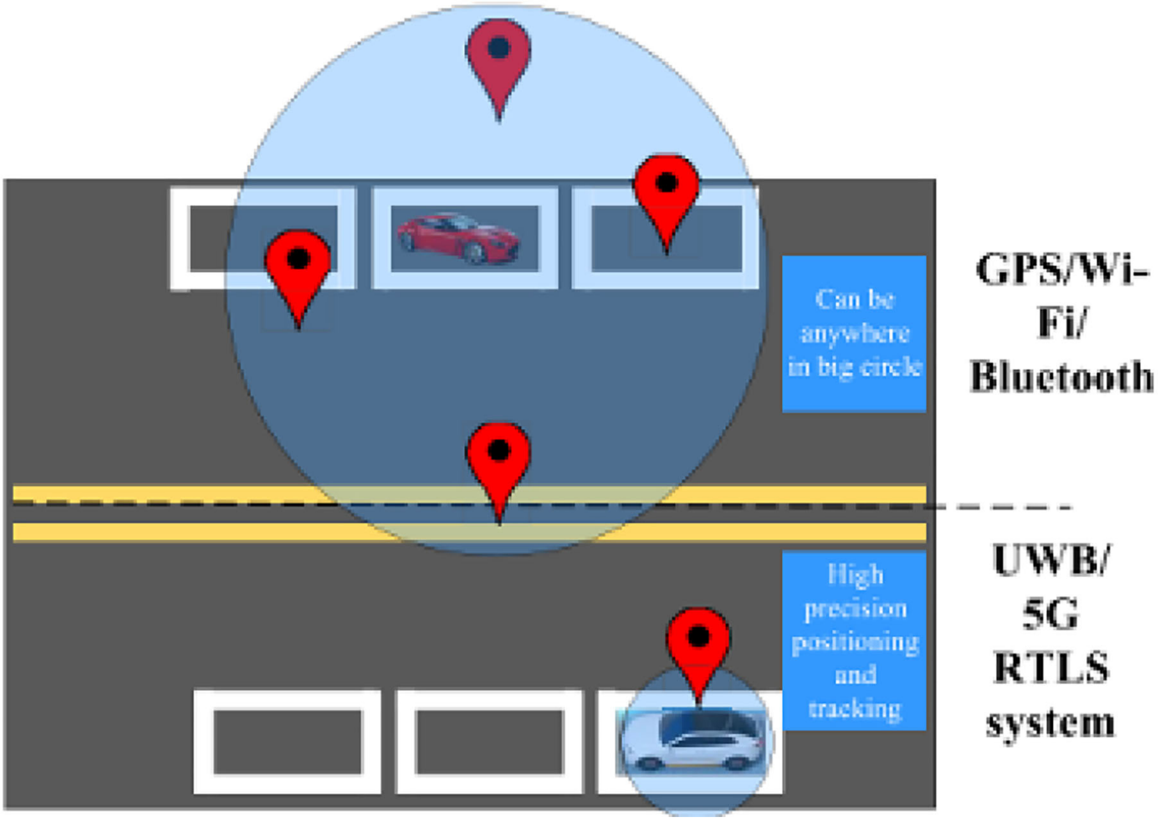
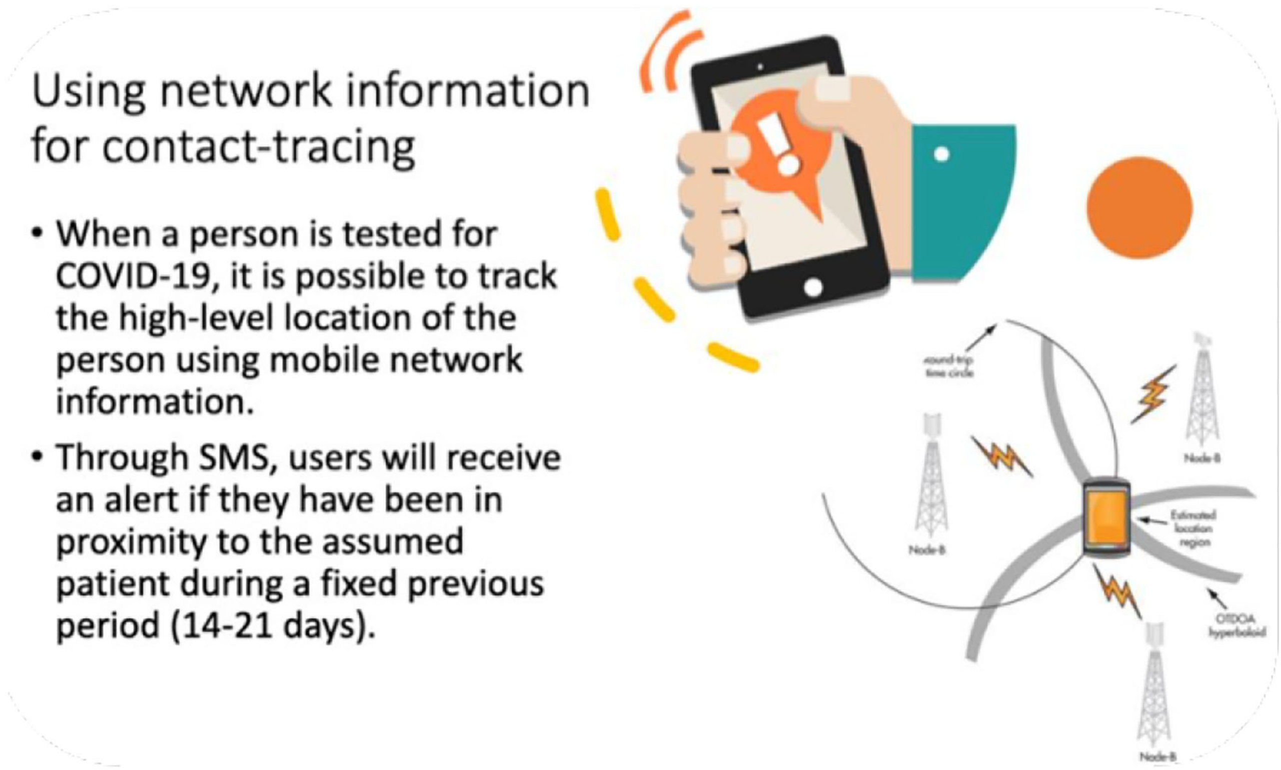

Can be anywhere in big circle
GPS/Wi-Fi/ Bluetooth
High precision positioning and tracking
UWB/ 5G RTLS system

FIGURE 18 | Difference between accuracy of 5G ultra high-frequency (UWB) and other positioning systems.

the subscriber localization is only down to the base station level. However, with the growing trend of small cells covering urban centers and the implementation of AI techniques, this mode of tracing could be efficient and useful. This solution involves using mobile network information and radio control signals to get the user's location and mobility history, as shown in **Figure 19**. This information can be used for high-level epidemiological studies to determine the spread of the disease especially after crowded events, such as religious gatherings, parties, concerts, or sporting events (likely to open gradually after the lockdown is progressively relaxed). Text messages will be sent to subscribers asking them to opt out if they do not wish to participate.

4.3. Crowd Sourcing of Social Media

Social media analytic can be expanded by fusing together additional data sources, such as License Plate Recognition (LPR), smart city CCTV, ATM transactions, and credit card purchases to help recreate the possible corona virus exposure path (2020; Chen et al., 2011; Garcia-Herranz et al., 2014; Karisani and Karisani, 2020). Leveraging graph database and



Using network information for contact-tracing

- When a person is tested for COVID-19, it is possible to track the high-level location of the person using mobile network information.
- Through SMS, users will receive an alert if they have been in proximity to the assumed patient during a fixed previous period (14-21 days).

FIGURE 19 | Contact tracing using network information.

graph inference algorithms, we can model complex interactions of individuals/group of individuals by linking and correlating information from heterogeneous digital data sources (online activity and check-ins, ATM transactions and LPR to detect visited locations, and geolocation information inferred from mobile phone data or Wi-Fi tracing) (Xu et al., 2020b). In these types of specialized databases, people, places, and things are treated as "nodes" and the connections between them are called "edges" that makes up the COVID-19 contact network. These networks consisting of nodes and edges make it possible to illuminate collected knowledge clearly, to uncover connections, and to recognize patterns, and graph analytic can be used to detect contacts of infected people (clusters). A contact network is not necessarily a social network, since contacts might be family, friends, acquaintances, or strangers. We can pick up a disease from a sick family member at home or from a stranger via an inopportune sneeze in a crowded coffee shop.

Human networks evolve into what social scientists call "small-world networks"—we tend to cluster together via the social dynamic of hemophilia (i.e., birds of a feather flock together). A small-world network is made up of connected clusters where there are more connections within the cluster than between the clusters. Shortest path algorithms can also be used to trace infection paths across multiple contact points within clusters, thus revealing disease pathways. Identifying "super-spreaders" or super-spreading events among the infected patients can be conveniently studied and visualized from a graph network perspective. Two-mode network approach (Chen et al., 2011) can be adopted to create COVID-19 contact network, such as shown in **Figure 20**, consisting of different layers, personal and geographical, which emphasizes the relationships between other individuals and their visits to high-risk locations. This would enable proximity tracking of all the other individual/group of individuals who are most likely be in contact with the carrier or are present in the same time and space.

4.4. Wearable Devices

Wearable devices enable mobile computing and wireless networking and collect data, track activities, and provide customized experiences to the user's needs and desires. Wearable technology has successfully moved past the adoption stage and now stands at the brink of massive diversification with an explosion in popularity and applicability. Wearable devices have found applications in almost every aspect of our daily life including consumer electronics, healthcare, sports and fitness, enterprise and industry, and media and entertainment (Abbasi et al., 2016). Smart glasses, smart watches, wristbands, fitness and health trackers, smart clothing, and smart jewelry are the most popular wearable devices. The global market of the wearable technology was estimated at $24.6 billion in 2019 and is expected to hit the $38.41 billion mark by 2025 2020. It would cause the wearable devices market to grow from 216 million devices in 2019 to 614.3 million units in 2025 2020.

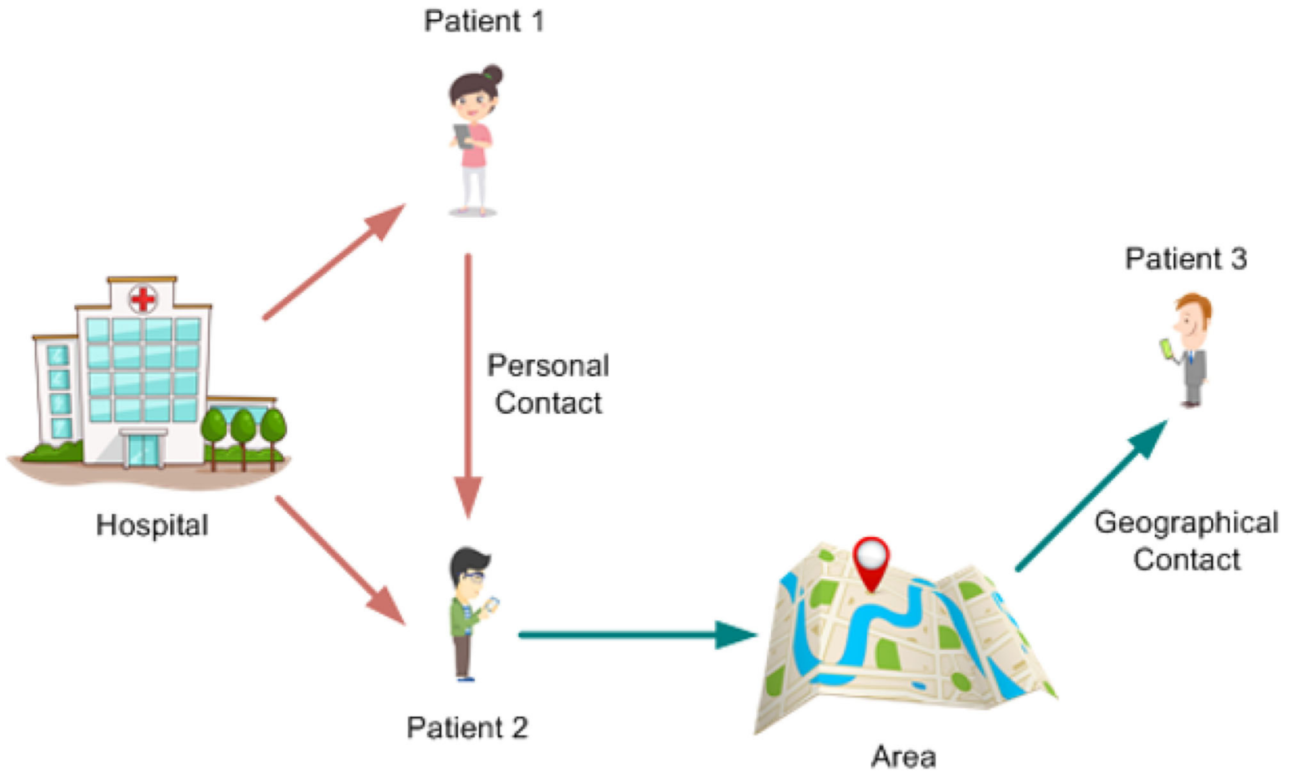


FIGURE 20 | Example of contact network creation using two-mode network approach.

Wearables make use of a number of technologies including cellular, Near Field Communication (NFC), Bluetooth, Wi-Fi, GPS, UWB, Long-Term Evolution (LTE), and 5G for information gathering, communication, and localization. A typical wearable device can perform the contact tracing feature for COVID-19 by tracking the location of the user through GPS tracker as well as proximity sensors utilizing Bluetooth, UWB radio, and LTE/5G connectivity. When a user becomes COVID-19 positive, they updates their status that prompts alerts to others who have been in contact with them based on proximity and location data history. The wearable devices can also be used effectively to enforce the self-isolation/quarantine through monitoring of geolocation of the user and raising alarm when such a person moves out of their house. **Figure 21** shows a possible working scenario of the wearable devices for contact tracing. Use of multiple technologies makes wearables quite versatile in terms of performance, range, and accuracy.

Health data like heart rate, skin temperature, cough, and blood oxygen saturation collected from wearable devices can also be effectively used to detect the onset and progression of illness caused by COVID-19 (Viboud and Santillana, 2020). By leveraging wearable technology either off-the shelf solutions like Fitbit or customized solutions (electronic bracelets equipped with vital signal monitoring, geolocation sensor, proximity sensors powered by Bluetooth, GPS), contact tracing can be enhanced by connecting it to a mobile app, such as StayHomeSafe 2020. Scripps Health, Stanford Medicine, and Fitbit are collaborating in a study to assess the ability of wearable devices to track, trace, and isolate COVID-19 patients.[2]

Estimote has created a range of wearable devices called the "Proof of Health" wearables for COVID-19 contact tracing at the level of the local workplace (Etherington, 2020).[3] The device that can be worn using a lanyard or like a wristwatch (**Figure 22**) has passive GPS location tracking, Bluetooth, and UWB proximity sensors, a rechargeable battery, and built-in LTE. A change in the user's health status, such as COVID-19 suspected or confirmed, flags the alarm and alert the people who have been in contact with them. This however requires use of Estimote's wearable devices by the whole work force in that facility.

The Proximity Trace device developed by Triax Technologies, Inc., is affixed to a safety hat or worn on the body with a lanyard alerting the user when they are too close to another user. In case of a COVID-19-positive user, the company can perform contact tracing and identify possible exposures using historical data logged in passively by the user's device.[4] Similar

[2] Scripps, stanford working with fitbit to assess wearables' covid-19 tracking abilities. Available online at: https://www.healthcareitnews.com/news/scripps-stanford-working-fibit-assess-wearables-covid-19-tracking-abilities (accessed May 5, 2020).

[3] Estimote. Available online at: https://estimote.com/wearable/ (accessed May 5, 2020).

[4] Triax technologies launches social distancing and contact tracing IoT solution, helping keep workers safe during covid-19 and beyond. Available online at: https://www.powermag.com/press-releases/triax-technologies-launches-social-

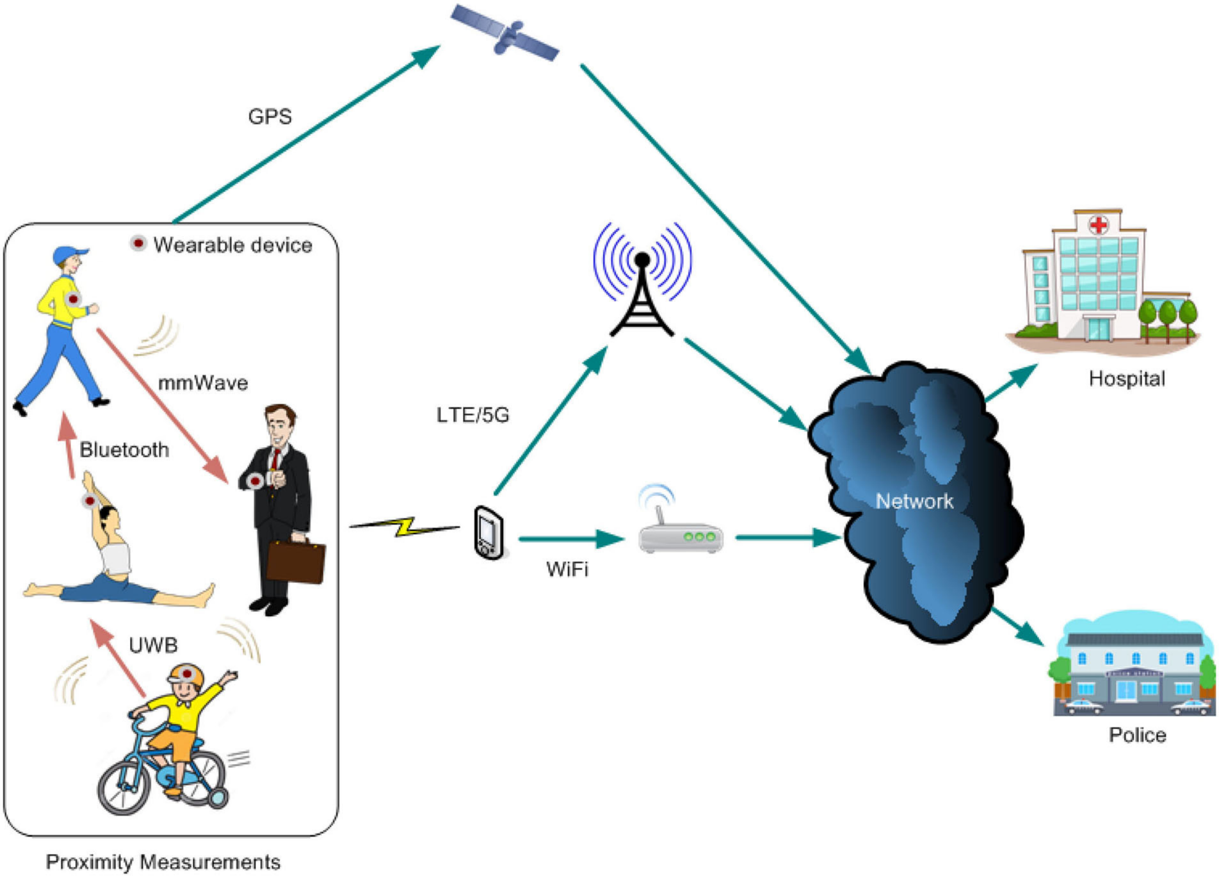


FIGURE 21 | Use of wearables for contact tracing.

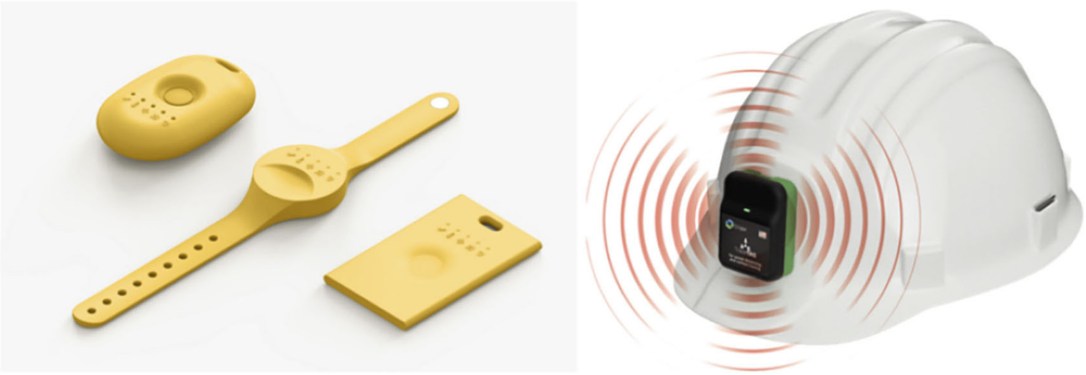


FIGURE 22 | Examples of wearables for contact tracing (Etherington, 2020) (see text footnote 4, respectively).

solutions are also offered by Blackline Safety Corp.[5] Workforce, a contact tracing app, that is compatible with the wearable wrist bands for contact tracing and tracking is developed by Ascent Solutions.[6]

Wearable Bluetooth/GPS-enabled wristbands have been tested for contact tracing, enforcing the social distancing and observing the lockdown during COVID-19 pandemic in

distancing-and-contact-tracing-iot-solution-helping-keep-workers-safe-during-covid-19-and-beyond/ (accessed May 2, 2020).

[5] Blackline safety adds industrial contact tracing capability to its intrinsically safe cloud-connected wearables. Available online at: https://www.businesswire.com/news/home/20200427005130/en/Blackline-Safety-Adds-Industrial-Contact-Tracing-Capability (accessed May 2, 2020).

[6] Covid-19 solutions. Available online at: https://www.myascents.com/covid-19-tracking-solutions (accessed May 2, 2020).

countries including Bulgaria, South Korea, Hong Kong, Belgium, Lichtenstein, and India.[7]

These wearable devices must be synced to their home location through smartphone's GPS and any active patients can be tracked and made to remain in that location until cleared. An alert is sent to the monitoring station if the wearer moves further than 15 m away from their phone. The location and proximity data of such individuals can be mapped to a centralized web-based dashboard as a warning mechanism or can be coupled with centralized tracing applications like TraceTogether 2020.

5. ATTACKS

There are a range of attacks on contact-tracing method. As contact tracing is heavily reliant on the use of data science and machine learning, it inherits the vulnerabilities of those areas. Let us consider a systematic monitoring of people's proximity, which results in a classification mechanism depending on that proximity if there is high probability for an infection. A potential instance of the recorded interactions is a sample that is classified using utility function f either as probably infected or not infected. Let us assume that we have an input space $\mathcal{X} = \{x_i\}$ and of course an output space $\mathcal{Y} = \{y_i\}$, where x_i is an instance of the interactions and y_i is the output of that instance determined by f, i.e., $f(x_i) = y_i$. We make the assumption that our initial system has been trained using N samples from the real world where we know the interactions of people and how many of them were eventually infected. Those samples form the training set $\mathcal{S}$ and it has derived the *system perception*, denoted by $\hat{y}$. After the end of the training phase, our designed system receives new samples from the real-world environment and classifies them. We are able to define this as the *run-time phase* of our system. For every new event $\hat{x}_i, f$ gives a new output $f(\hat{x}_i) = \hat{y}_i$. We have the following cases:

- If $\hat{x}_i$ are probably infected and our system does not recognize them as such, they are called false negatives that cause a loss l to our system.
- If $\hat{x}_i$ are probably infected and our system recognizes them as such, they are called true positives. They might also be not infected. In either case, there is no loss to our system.
- If $\hat{x}_i$ are not infected and our system recognizes them as probably infected, they are called false positives and cause a loss λ to our system.

The attacker of the specific system wants to avoid being self-isolated because of their contact with infected people. The aim of the attacker is to maximize the impact the attack has on the system by maximizing $|f(\hat{x}_i) - y_i|$. Consequently, a challenge of the system that defends its functionality is to find a utility function that minimizes the losses, measured as the distance of $f(\hat{x}_i)$ to the real output y_i.

5.1. Attacks on Data Privacy

5.1.1. Membership Inference Attacks

An adversary is able to perform a membership inference attack (Shokri et al., 2017) by querying the model and exploiting the returned confidence values to distinguish if data were part of the training. In a contact-tracing application, the returned output to the users would include if the person has been in contact with a COVID-19 patient, alongside with a confidence score of this classification. An adversary is able to exploit this information, with knowledge extracted from public data sets, to identify if people's data were part of the ML training.

5.1.2. Model Inversion Attacks

In Model Inversion (MI) attacks (Fredrikson et al., 2014, 2015; Zhang et al., 2019), the adversary's goal is to reproduce the sensitive training data. The threat model of MI attacks involves access to the training model, as well as the confidence scores that are returned as the output of it. In the contact-tracing app, the ML model should be hidden from the users, since there is no need for them to access it.

5.1.3. Data Poisoning Attacks

The adversary can poison the training data set. To accomplish their goal, they *derive* and *inject* a point to decrease the classification accuracy (Biggio et al., 2012; Laishram and Phoha, 2016; Muñoz-González et al., 2017; Steinhardt et al., 2017; Yang et al., 2017; Jagielski et al., 2018). This attack has the ability to completely distort the classification function during its training, thus allowing the attacker to divert the classification of the system according to their taste. In a real-world scenario, the attacker needs to have privileged access to a contact tracing application, being a member of either the development or the administration team. This scenario is rather unrealistic as a single person would not be responsible for handling the training data set without any supervision.

5.2. Attacks on Model Privacy

5.2.1. Evasion Attacks

The attacker can undertake an *evasion* attack against classification during the testing phase, thus producing a wrong system perception. In this case, the goal of the adversary is to achieve misclassification of their data, for example, remaining unnoticed. In a real-world scenario with a contact tracing app, the attacker would want to confuse the system about the interactions they had with other people. Moreover, the attacker can compromise the targeted system by being spotted out as potentially infected. This can be easily achieved by using many different phones in too many different locations. There was an incident where a person caused an artificial traffic jam on Google maps using a wagon full of Phones (Wired, 2020). This incident changed the perception of the system about road traffic, forcing Google maps to assume that there was a traffic jam when it was not busy.

5.2.2. Model Extraction Attacks

The adversary in model extraction attacks (Tramèr et al., 2016) is trying to reconstruct a ML model that is similar to the original

[7] Coronavirus: People-tracking wristbands tested to enforce lockdown. Available online at: https://www.bbc.co.uk/news/technology-52409893 (accessed May 2, 2020).

by identifying the decision boundaries of it. The attackers aim to have complete access to an ML model that behaves similarly with the original, in order to perform an attack on Data Privacy, as seen in section 5.1.

5.2.3. Model Poisoning Attacks

Model poisoning attacks are quite similar to the data poisoning attacks (discussed in section 5.1.3) as an adversary injects "hidden" poisons to the training model in order to behave maliciously only on their trigger (Gu et al., 2017; Liu et al., 2017). However, model poisoning attacks, opposed to data poisoning attacks, do not require access to the ML training procedure, and elaborate scenarios where the ML model is sent to the users, such as Federated Learning (Konečnỳ et al., 2016; McMahan et al., 2016; Bonawitz et al., 2017; McMahan and Ramage, 2017). In the contact tracing scenario, the ML model can be sent to the users for training, and then to protect the privacy of the users, a secure aggregation technique collects and aggregates all the trained models, before returning it to the ML coordinators. That enables the model poisoning threat possibility, since a malicious user can poison the received model before sending it back, and since the secure aggregation is in place, the ML coordinators cannot identify that the final trained model is being poisoned.

6. CRITICAL ANALYSIS

The discussion on user and contact tracing opens up a whole lot of questions, and the most fundamental of these is that we do not actually have any real infrastructure to implement privacy-preserving methods. It is likely that a COVID-19 App would be a pin-point app where the data gathered for location and contact tracking could be easily abused. Furthermore, in the absence of a universally acceptable standard, it would have limited scope outside a country's borders. Our major problem is that we have built data infrastructures that mirror those from the 1980s where we care little about the core rights of the data we gather. Once captured, the owner becomes the entity who captured the data, and without the trustworthiness of the transactions involved, we leave it open to abuse for malicious activities.

6.1. Who Is Trent?

We often trust our health authorities a great deal more than we trust our governments. If the data go to clinical staff for analysis, we perhaps find that more acceptable than someone in law enforcement. Thus, the fundamental question in the whole system is how we can make sure that Trent is someone trusted. This could be a trusted entity who handles the data on behalf of the citizen (and preserves their privacy on their behalf) or a health authority that Alice trusts? It is unlikely that we should trust anyone other than health authorities, and also we need to make sure that the data gathered are only kept for the required amount of time. Any tracing of contacts should not be kept for longer than it is required, it should be used only for the clinical purposes and only provided to trusted health professionals (**Figure 23**).

6.2. Where Is Carol?

There are no trusted mechanisms to integrate a formal test for COVID-19. we therefore proposed Carol the Tester. Carol the Tester would be able to define a state of testing: positive, clear, and

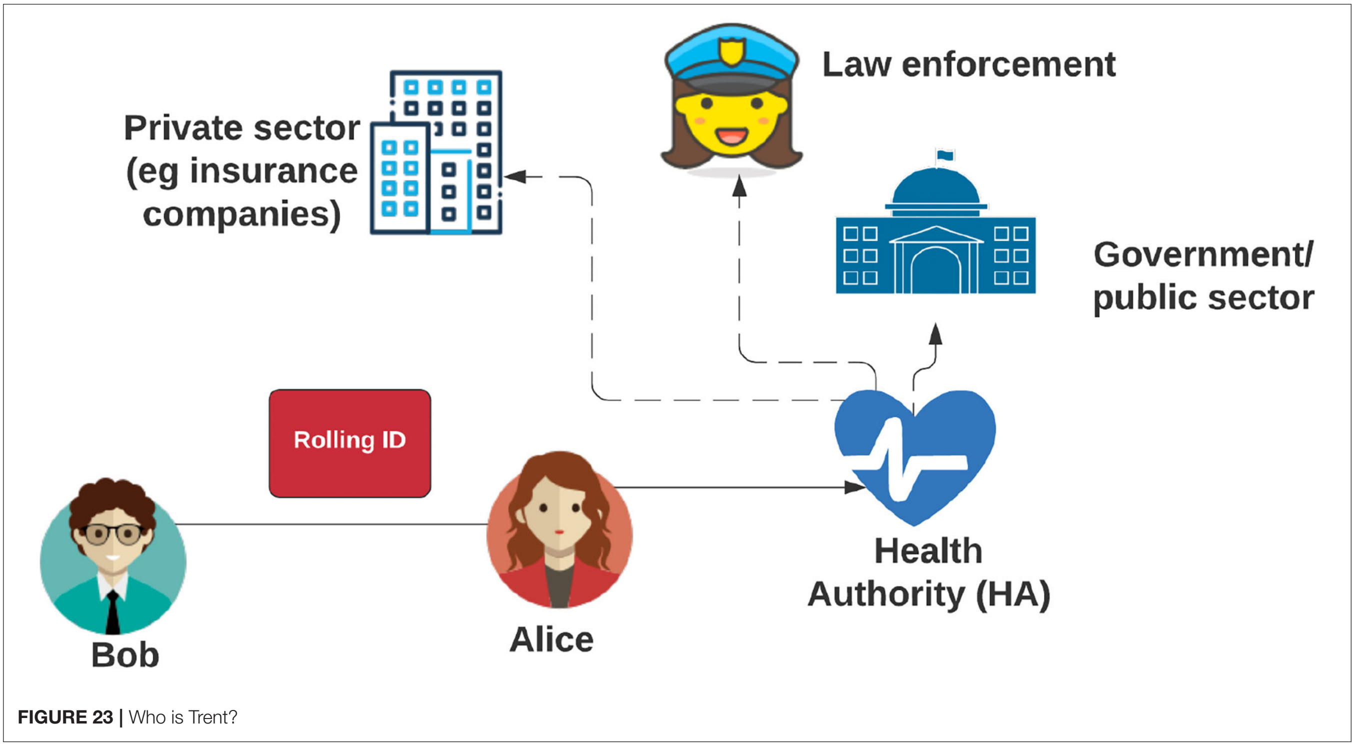


FIGURE 23 | Who is Trent?

suspected, and will have followed a scientific process to provide Alice's COVID-19 status.

6.3. What Is Carol's Attestation?

We do not want the government to control testing, making availability of a trusted network of testers-from our own country and from other trusted places, eminent. Thus, we need a trusted way for a number of testers to sign the attestation that Alice has COVID-19, or when she has been identified to be negative. A new attestation will revoke a previous one. So, will this attestation be in the form of passporting system with digital verification allowing Alice to carry a digital passport of being free from COVID-19, and that can be passed to others?

6.4. Clear Role for Trent

Overall, Trent must be the health authority and not the government. Trent must be the one who marks the status of Alice as clear, suspected, not known, and positive. In this way, Trent is responsible for defining the status of Alice and the tracking will only happen when there is a positive status applied to her.

6.5. Trent Must Be the Health Authority

Border control, and which countries/testers do you trust? The basic flaw of having just one health authority involved is that there needs to be a trust between health authorities in different countries. In this way, we can trace over borders, when the travel reopens. A trust network for Carol in each country needs to be defined along with the definition of attestation process so that it can be shown at borders. Countries thus will define the testing trust network, where Carol's testing is acceptable cross-border.

6.6. There Is No Real Integration of Identities

How we are going to properly identify Bob, Trent, or Alice? With having a private key signing for Alice and Trent, there is no real way of knowing that Alice is Alice and Trent is Trent. Thus, we need someone for each core identity to be certified for the things they are signing. This might include the health authority to self-certify.

6.7. There Is No Clear Mechanism for Alice's Consent

A fundamental flaw is the consent mechanisms that Alice must give to Trent in order to flip her current COVID-19 statement, especially in the changing it to a positive state. While Trent may have the rights to record Alice as being positive, he may need Alice's consent as to whether she is okay with her COVID-19 state being broadcast to others.

Normally when an app is installed on a mobile device, the user should be alerted to the privacy implications of the use of their personal data and would then need to give their consent before proceeding. The consent would in this instance cover the transmission of personal data to health authorities or other official bodies. Under the EU General Data Protection Regulation (GDPR), it could be argued that vital interests of individuals would be an alternative legal basis for gathering and sharing these personal data (European Parliament, 2016). This would apply to life-or-death situation and this could be difficult to argue solely on the basis that there is a possibility of death following exposure to an infected individual. The other legal basis for processing personal data would be public interest, and this might be more easily justified on the basis that protecting public health is in the public interest. Following GDPR principles will be particularly important as the UK is likely to continue to be subject to EU law during the pandemic.

6.8. Long-Term Data Retention

The UK's Data Protection Act 2018 allows for personal data to be kept for research purposes so long as reasonable steps are taken to protect individual identity (UK Parliament, 2018). Pseudonymization may offer some protection, but is not a guarantee that privacy will be preserved. For instance, the data could be combined with published data sets, such as electoral registers to identify individuals.

6.9. Lack of Incentive for Uptake

To make the app a success, there should be strong incentives for uptake. It may not be sufficient to appeal to public-spirited attitudes when there is a strong disincentive of increased personal restrictions. If an individual receives an alert that they have been in close proximity to a suspected infected individual, they are advised to self-isolate. This will depend on the criteria that are applied to different levels of alerting, the accuracy of the proximity measures and the degree of self-reporting. It is possible that incentives, such as legal sanction and law enforcement are more likely to work in authoritarian states, whereas social pressure might work better in mono-cultural conformist societies. For a pluralistic and democratically accountable society offering privileges, such as access to travel or greater freedom of movement might be better motivators.

6.10. Poor Data Quality

Data quality will affect the contact tracing approach in several ways: Where it depends on self-reporting of COVID-19 symptoms, not everyone will do so. Will the authorities act on self-reporting in order to respond rapidly, or wait for the outcome of COVID-19 tests to confirm the self diagnosis? The follow-up tests are not completely accurate and have varying levels of type 1 and type 2 errors. The potential emergence of a new, more virulent mutant strain of COVID-19 may affect the criteria used to assess risk (potential to transmit in less time or at an increased distance, for instance) (Korber et al., 2020).

6.11. No Binding of Data

There is no method that truly binds the capture of contact data to the entities involved in a trusted way. The only thing it does is to mask Alice until she is proven to have COVID-19, after which her data can be revealed to others without any restrictions.

6.12. There's No Signing Involved

A fundamental trait of the modern world is that we introduce proper digital signing. As a minimum, we should see key pairs being created for devices and entities where IDs and tracking are signed by private keys, and checked for the correctness of the signer. There are many trusted signing methods, which can be used to anonymize the signer.

7. CONCLUSIONS

We have identified a number of existing technologies including GPS, Bluetooth, Wi-Fi, RFID, wearable devices, and social media fingerprints that can effectively provide the tracks of a COVID-19 patient. The potential contacts/proximity users can efficiently be identified and notified of the threat, and hence advice to self-isolate. **Table 2** summarizes their key benefits along with the disadvantages.

The Bluetooth approach, being pursued at various stages by governments across Europe and Latin America, as well as in Australia and many Asia nations, requires a majority of people in a geographic area to adopt it for it to be effective. These apps are also considered to be interfering with vital signs monitoring applications, such as diabetes monitoring (Biggs, 2020). Some countries, including South Korea and Israel, are using high-tech methods of contact tracing that involve tracking peoples' location via phone networks. But such centralized, surveillance-based approaches are viewed as invasive and unacceptable in many countries for privacy reasons.

The Bluetooth-based apps are also more privacy-friendly than tracking techniques that use GPS or cellphone data. They use Bluetooth to broadcast and receive an encrypted, pseudonymous signal from nearby phones and create a log of interactions that remain on the phone, so users' names and numbers are not disclosed. Social Media approach also has good potential but

TABLE 2 | Comparison of COVID-19 contact tracing enabling technologies.

Technology	Pros	Cons	Users
GPS	• Availability of real-time location information. • Locating users in real-time who contracted the virus. • Identifying the demand and need for healthcare in an area. • Identify virus hot spots with Geo-data. • Local information and awareness for patients and carers. • Enabling care professionals to continue the upmost service in care.	• High storage and computational requirements. • Possible issues with indoor localization. • Social fears of being tracked and the lack of trust in the use of personal/health.	Everyone
Bluetooth	• Wide availability. • Low-power requirements. • List of all devices that have "made contact" is readily available. • Reduced requirement for storage and computational resources.	• Inaccuracy of proximity approximation. • 5–10 m scanning range causing false positives. • Real-time location information is not available. • Requires a higher level of programming to make sure the Bluetooth connectivity is enabled and responsive to the requirements of the application.	Everyone
Bluetooth plus UHF RFID	• Able to track the contacts with accuracy and double check. • Can track the belongings and items in use of the patient.	• Tagging items and deploying RFID readers with phase RSSI and phase reading will incur cost.	Everyone
Wi-Fi router tracing	• Widely available worldwide as handling 60% of the internet traffic. • Wide range of different types of existing Wi-Fi routers can be readily used with no extra hardware.	• Relatively low accuracy. Hybrid techniques, such as using the built-in accelerometer and gyroscope with Wi-Fi can improve the accuracy.	Everyone
Mobile network tracing	• No app installation is required. • Transparent to the user. • Larger public access, who, if desired, could opt-out of the programme.	• List of devices that have made contact is not available. • Only high-level localization information is available. • Participation of network operators is required to increase coverage.	Mobile Operators
UWB 5G	• High accuracy.	• Not yet fully operational.	Everyone
Crowd sourcing of social media and tracking financial transactions	• A pre-outbreak pattern can be identified indicating the areas where the virus could strike next. • Could generating near-real-time information for public health officials that could help tracking its spread.	• Privacy is a major concern as the accuracy of such models depends on the location information and other data sources including financial transaction information.	Government entities
Wearable devices using Bleutooth/GPS/Wi-Fi	• Suitable for high traffic and dense areas including indoors, malls, homes. • Enables tracking as well as geofencing the infected patients. • Allows remote tracking of quarantined patients. • Increased coverage and reliability. • No need of a smartphone, hence cost effective.	• Requires a customized wearable device. • Requires the user to have the app running at all times. • Can generate false positives as range is higher than 1.5 m.	Everyone

is marred by authentication restrictions. Wearables appear to be a dynamic and effective solution as have the capability to make use of multiple technologies with improved efficiency and higher accuracy.

The main issues that surround these enablers of a potential contact tracing application include privacy concerns, security loopholes, lack of testing, and part use of the smartphones. The privacy concerns need to be eradicated through GDPR compliance, transparent development of the app, and data usage and reassurance about the temporary nature of the surveillance.

AUTHOR CONTRIBUTIONS

WB and MI contributed to the main idea and overall structure of the paper, and the writing. MU-R contributed to review on contact tracing APPs for COVID-19, key enabling technologies of GPS, RFID. LZ contributed to privacy-preserving contact tracing idea. QA contributed to the key enabling technologies including wearable devices, RFID. CC contributed to attacks analysis. DH contributed to critical analysis. NP contributed to review on contact tracing APP for COVID-19. PP contributed to the introduction and contact tracing APP review. All authors contributed to reviewing and editing the paper.

ACKNOWLEDGMENTS

The authors also acknowledge inputs and discussions from the following colleagues: Dr. Ahmed Zoha, Dr. Yusuf Sambo, Dr. Shuja Ansari, and Dr. Kia Dashtipour. We acknowledge the funding for the Scotland 5G Centre, which has partially supported the work behind this document.

REFERENCES

(2017). *Gnss Market Report*.

(2020). *Bluetooth Phone Apps for Tracking Covid-19 Show Modest Early Results*. Reuters. Available online at: https://www.reuters.com/article/us-health-coronavirus-apps/bluetooth-phone-apps-for-tracking-covid-19-show-modest-early-results-idUSKCN2232A0 (accessed May 1, 2020).

(2020). *Covid-19 Care Assistant*. Available online at: https://www.babylonhealth.com/coronavirus/covid-19-care-assistant (accessed May 4, 2020).

(2020). *Covid Graph. Fighting Covid-19 With Graph Technology*. Available online at: https://covidgraph.org/news/ (accessed May 1, 2020).

(2020). *Covid Symptom Tracker*. Available online at: https://covid.joinzoe.com (accessed May 3, 2020).

(2020). *Germany Increases Coronavirus Threat to High*. Available online at: www.spiegel.de/international/germany/germany-increases-coronavirus-threat-to-high-a-a8fa63e2-2123-4c8c-aa73-f557244aaf07 (accessed May 2, 2020).

(2020). *How To Use Aarogya Setu App and Find Out If You Have Coronavirus Symptoms*. Economic Times. Available online at: https://economictimes.indiatimes.com/tech/software/how-to-use-aarogya-setu-app-and-find-out-if-you-have-covid-19-symptoms/articleshow/75023152.cms (accessed May 3, 2020).

(2020). *How We Feel*. Available online at: https://howwefeel.org (accessed May 5, 2020).

(2020). *Korea's Self Quarantine Safety Protection App to Monitor People*. Geospatial World. Available online at: https://www.geospatialworld.net/apps/covid-19/koreas-self-quarantine-safety-protection-app-to-monitor-people/ (accessed May 4, 2020).

(2020). *Meticulous Research, Global Wearable Computing Devices Market: Size, Share, Demand and Outlook 2020–2025*. Available online at: https://www.marketwatch.com/press-release/global-wearable-computing-devices-market-size-share-demand-and-outlook-2020-2025-2020-03-12 (accessed May 4, 2020).

(2020). *Mordor Intelligence, Smart Wearable Market–Growth, Trends, and Forecast (2020–2025)*. Available online at: https://www.mordorintelligence.com/industry-reports/smart-wearables-market (accessed May 4, 2020).

(2020). *Pepp-pt*. Available online at: https://www.pepp-pt.org (accessed May 4, 2020).

(2020). *Stayhomesafe Mobile App User Guide*. Available online at: https://www.coronavirus.gov.hk/eng/stay-home-safe.html (accessed May 5, 2020).

(2020). *Tracetogether*. Available online at: https://www.tracetogether.gov.sg (accessed May 3, 2020).

(2020). *Tracking Coronavirus Spread*. Available online at: https://www.popularmechanics.com/technology/apps/a31742763/covid-19-app-private-kit-safe-paths (accessed May 5, 2020).

(2020). *World Health Organization*. Available online at: https://www.who.int/news-room/q-a-detail/contact-tracing (accessed May 1, 2020).

Abbasi, Q. H., Rehman, M. U., Qaraqe, K., and Alomainy, A. (2016). *Advances in Body-Centric Wireless Communication: Applications and State-of-the-Art*. London: Institution of Engineering and Technology.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: a survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor*. 17, 2347–2376. doi: 10.1109/COMST.2015.2444095

Alimadadi, A., Aryal, S., Manandhar, I., Munroe, P. B., Joe, B., and Cheng, X. (2020). Artificial intelligence and machine learning to fight covid-19. *Physiol. Genomics* 52, 200–202. doi: 10.1152/physiolgenomics.00029.2020

Altuwaiyan, T., Hadian, M., and Liang, X. (2018). "Epic: efficient privacy-preserving contact tracing for infection detection," in *2018 IEEE International Conference on Communications (ICC)* (Kansas City, MO: IEEE), 1–6. doi: 10.1109/ICC.2018.8422886

Avitabile, G., Botta, V., Iovino, V., and Visconti, I. (2020). *Towards Defeating Mass Surveillance and SARS-CoV-2: The Pronto-C2 Fully Decentralized Automatic Contact Tracing System*.

Beeching, N. J., Fletcher, T. E., and Beadsworth, M. B. (2020). *Covid-19: Testing Times* (BMJ).

Bell, J., Butler, D., Hicks, C., and Crowcroft, J. (2020). Tracesecure: towards privacy preserving contact tracing. *arXiv* 2004.04059.

Berke, A., Bakker, M., Vepakomma, P., Raskar, R., Larson, K., and Pentland, A. (2020). Assessing disease exposure risk with location histories and protecting privacy: a cryptographic approach in response to a global pandemic. *arXiv* 2003.14412.

Biggio, B., Nelson, B., and Laskov, P. (2012). Poisoning attacks against support vector machines. *arXiv* 1206.6389.

Biggs, T. (2020). *Covidsafe May Interfere With Diabetes-Monitoring Apps*. Available online at: https://amp.smh.com.au/technology/covidsafe-may-interfere-with-diabetes-monitoring-apps-20200501-p54oyd.html (accessed May 6, 2020).

Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., et al. (2017). "Practical secure aggregation for privacy-preserving machine learning," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY), 1175–1191. doi: 10.1145/3133956.3133982

Brack, S., Reichert, L., and Scheuermann, B. (2020). *Decentralized Contact Tracing Using a DHT and Blind Signatures*.

Busvine, D. (2020). *Germany Launches Smartwatch App to Monitor Coronavirus Spread*. Reuters. Available online at: https://www.reuters.com/article/us-health-coronavirus-germany-tech/germany-launches-smartwatch-app-to-monitor-coronavirus-spread-idUSKBN21P1SS (accessed May 2, 2020).

Charara, S. (2020a). *Amazon and Apple Are Quietly Building Networks That Know the Location Of Everything*. Wired. Available online at: https://www.wired.co.uk/article/amazon-sidewalk-apple-u1-networks (accessed April 30, 2020).

Charara, S. (2020b). *Here's How Wi-Fi Actually Works*. Available online at: https://time.com/3834259/wifi-how-works/ (accessed April 28, 2020).

Chawla, V., and Ha, D. S. (2007). An overview of passive rfid. *IEEE Commun. Mag.* 45, 11–17. doi: 10.1109/MCOM.2007.4342873

Chen, Y.-D., Chen, H., and King, C.-C. (2011). "Social network analysis for contact tracing," in *Infectious Disease Informatics and Biosurveillance*, eds Castillo-Chavez, C., Chen, H., Lober, W. B., Thurmond, M., and Zeng, D. (Boston, MA: Springer), 339–358. doi: 10.1007/978-1-4419-6892-0_15

Cho, H., Ippolito, D., and Yu, Y. W. (2020). Contact tracing mobile apps for covid-19: privacy considerations and related trade-offs. *arXiv* 2003.11511.

Chrysaidos, N. (2020). *Iranian Coronavirus App Collecting Sensitive Information*. Available online at: https://blog.avast.com/iranian-coronavirus-app-collecting-sensitive-information-avast (accessed May 5, 2020).

Cimpanu, C. (2020). *Spying Concerns Raised Over Iran's Official Covid-19 Detection App*. Available online at: https://www.zdnet.com/article/spying-concerns-raised-over-irans-official-covid-19-detection-app/ (accessed May 5, 2020).

Dar, A. B., Lone, A. H., Zahoor, S., Khan, A. A., and Naaz, R. (2020). *Applicability of Mobile Contact Tracing in Fighting Pandemic (Covid-19): Issues, Challenges and Solutions*. Cryptology ePrint Archive, Report 2020/484. Available online at: https://eprint.iacr.org/2020/484

Das, R. (2010). *RFID Forecasts, Trends by Territory and Lessons (RFID Europe 2010)*. IDTechEx Report.

Das, R. (2016). *RFID Forecasts, Players and Opportunities 2016–2026*. IDTechEx Report.

Das, R. (2018). *RFID 2018–2028: Rain and NFC, Market Status, Outlook and Innovations*. IDTechEx report.

De Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., and Blondel, V. D. (2013a). Unique in the crowd: the privacy bounds of human mobility. *Sci. Rep.* 3:1376. doi: 10.1038/srep01376

De Montjoye, Y.-A., Quoidbach, J., Robic, F., and Pentland, A. S. (2013b). "Predicting personality using novel mobile phone-based metrics," in *International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction* (Springer), 48–55. doi: 10.1007/978-3-642-37210-0_6

Dobkin, D. M. (2012). *The RF in RFID: UHF RFID in Practice*. Oxford: Newnes.

Eames, K. T., and Keeling, M. J. (2003). Contact tracing and disease control. *Proc. R. Soc. Londo. B Biol. Sci.* 270, 2565–2571. doi: 10.1098/rspb.2003.2554

El-Rabbany, A. (2002). *Introduction to GPS: The Global Positioning System*. Artech House.

Etherington, D. (2020). *Estimote Launches Wearables for Workplace-Level Contact Tracing for Covid-19*. Available online at: https://techcrunch.com/2020/04/02/estimote-launches-wearables-for-workplace-level-contact-tracing-for-covid-19/ (accessed May 5, 2020).

Eubank, S., Guclu, H., Kumar, V. A, Marathe, M. V., Srinivasan, A., Toroczkai, Z., et al. (2004). Modelling disease outbreaks in realistic urban social networks. *Nature* 429, 180–184. doi: 10.1038/nature02541

European Parliament (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* (Strasbourg).

Finkenzeller, K. (2010). *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. New York, NY: John Wiley & Sons.

Fredrikson, M., Jha, S., and Ristenpart, T. (2015). "Model inversion attacks that exploit confidence information and basic counter measures," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 1322–1333. doi: 10.1145/2810103.2813677

Fredrikson, M., Lantz, E., Jha, S., Lin, S., Page, D., and Ristenpart, T. (2014). "Privacy in pharmacogenetics: an end-to-end case study of personalized warfarin dosing," in *23rd $USENIX$ Security Symposium ($USENIX$ Security 14)*, 17–32.

Garcia-Herranz, M., Moro, E., Cebrian, M., Christakis, N. A., and Fowler, J. H. (2014). Using friends as sensors to detect global-scale contagious outbreaks. *PLoS ONE* 9:e92413. doi: 10.1371/journal.pone.0092413

Gold, J. (2020). *Contact Tracing Via Bluetooth Could Help Track Covid-19 Transmission*. Network World. Available online at: https://www.networkworld.com/article/3538333/contact-tracing-via-bluetooth-could-help-track-covid-19-transmission.html/ (accessed May 1, 2020).

Gould, M., and Lewis, G. (2020). *Digital Contact Tracing: Protecting the NHS and Saving Lives*. Available online at: https://www.nhsx.nhs.uk/blogs/digital-contact-tracing-protecting-nhs-and-saving-lives/ (accessed May 3, 2020).

Greenberg, A. (2020). *How Apple and Google Are Enabling Covid-19 Bluetooth Contact-Tracing*. Available online at: https://www.wired.com/story/apple-google-bluetooth-contact-tracing-covid-19/ (accessed May 3, 2020).

Greenberg, N., Docherty, M., Gnanapragasam, S., and Wessely, S. (2020). Managing mental health challenges faced by healthcare workers during covid-19 pandemic. *BMJ* 368:m1211. doi: 10.1136/bmj.m1211

Griggs, W. M., Verago, R., Naoum-Sawaya, J., Ordóñez-Hurtado, R. H., Gilmore, R., and Shorten, R. N. (2018). Localizing missing entities using parked vehicles: an RFID-based system. *IEEE Internet Things J.* 5, 4018–4030. doi: 10.1109/JIOT.2018.2864590

Gu, T., Dolan-Gavitt, B., and Garg, S. (2017). Badnets: identifying vulnerabilities in the machine learning model supply chain. *arXiv* 1708.06733.

Hamilton, I. A. (2020). *Poland Made an App That Forces Coronavirus Patients to Take Regular Selfies to Prove They're Indoors or Face a Police Visit*. Available online at: https://www.businessinsider.com/poland-app-coronavirus-patients-mandaotory-selfie-2020-3 (accessed May 4, 2020).

Handley, L. (2020). *Nearly Three Quarters of the World Will Use Just Their Smartphones to Access the Internet by 2025*. Available online at: https://www.cnbc.com/2019/01/24/smartphones-72percent-of-people-will-use-only-mobile-for-internet-by-2025.html (accessed May 2, 2020).

Harrop, P., and Das, R. (2005). *RFID Forecasts, Players and Opportunities 2005–2015*.

He, X., and Das, R. (2015). *RFID in China 2015–2025: Status, Applications and Markets*. IDTechEx report.

Hellewell, J., Abbott, S., Gimma, A., Bosse, N. I., Jarvis, C. I., Russell, T. W., et al. (2020). Feasibility of controlling covid-19 outbreaks by isolation of cases and contacts. *Lancet Glob. Health* 8, E488–E496. doi: 10.1016/S2214-109X(20)30074-7

Heymann, D. L., and Shindo, N. (2020). Covid-19: what is next for public health? *Lancet* 395, 542–545. doi: 10.1016/S0140-6736(20)30374-3

Horton, R. (2020). Offline: Covid-19 and the NHS—"a national scandal". *Lancet* 395:1022. doi: 10.1016/S0140-6736(20)30727-3

Huang, G., Hu, Z., Wu, J., Xiao, H., and Zhang, F. (2020). Wifi and vision integrated fingerprint for smartphone-based self-localization in public indoor scenes. *IEEE Internet Things J.* 7, 6748–6761. doi: 10.1109/JIOT.2020.2974928

Hui, M. (2020). *Singapore Wants All Its Citizens to Download Contact Tracing Apps to Fight the Coronavirus*. Available online at: https://qz.com/1842200/singapore-wants-everyone-to-download-covid-19-contact-tracing-apps/ (accessed May 2, 2020).

Iacobucci, G. (2020). Covid-19: all non-urgent elective surgery is suspended for at least three months in England. *BMJ* 368:m1106. doi: 10.1136/bmj.m1106

Jagielski, M., Oprea, A., Biggio, B., Liu, C., Nita-Rotaru, C., and Li, B. (2018). "Manipulating machine learning: poisoning attacks and countermeasures for regression learning," in *2018 IEEE Symposium on Security and Privacy (SP)* (San Francisco, CA: IEEE), 19–35. doi: 10.1109/SP.2018.00057

Januszewski, J. (2018). *GNSS Frequencies, Signals, Receiver Capabilities and Applications*. Szczecin: Zeszyty Naukowe Akademii Morskiej w Szczecinie.

Jeong, S., Kuk, S., and Kim, H. (2019). A smartphone magnetometer-based diagnostic test for automatic contact tracing in infectious disease epidemics. *IEEE Access* 7, 20734–20747. doi: 10.1109/ACCESS.2019.2895075

Karisani, N., and Karisani, P. (2020). Mining coronavirus (covid-19) posts in social media. *arXiv* 2004.06778.

Konečnỳ, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., and Bacon, D. (2016). Federated learning: strategies for improving communication efficiency. *arXiv* 1610.05492.

Korber, B., Fischer, W., Gnanakaran, S. G., Yoon, H., Theiler, J., Abfalterer, W., et al. (2020). Spike mutation pipeline reveals the emergence of a more transmissible form of SARS-CoV-2. *bioRxiv* 2020.04.29.069054. doi: 10.1101/2020.04.29.069054

Laishram, R., and Phoha, V. V. (2016). Curie: A method for protecting svm classifier from poisoning attack. *arXiv* 1606.01584.

Landt, J. (2005). The history of rfid. *IEEE Potent.* 24, 8–11. doi: 10.1109/MP.2005.1549751

Liang, X., Zhao, J., Dong, L., and Xu, K. (2013). Unraveling the origin of exponential law in intra-urban human mobility. *Sci. Rep.* 3:2983. doi: 10.1038/srep02983

Liu, Y., Ma, S., Aafer, Y., Lee, W.-C., Zhai, J., Wang, W., et al. (2017). *Trojaning Attack on Neural Networks*. West Lafayette, IN: Department of Computer Science Technical Reports.

Logsdon, T. (2012). *The Navstar Global Positioning System*. Springer Science & Business Media.

Martinetti, I. (2020). *App Developed in Record Time to Help Monitor French Covid-19 Cases*. Available online at: http://www.rfi.fr/en/france/20200327-covidom-app-developed-in-record-time-to-help-monitor-french-covid-19-cases-coronavirus-e-health (accessed May 4, 2020).

Maynes (2020). *Moscow io Launch New Surveillance App to Track Residents in Coronavirus Lockdown*. Available online at: https://www.npr.org/sections/coronavirus-live-updates/2020/04/01/825329399/moscow-launches-new-surveillance-app-to-track-residents-in-coronavirus-lockdown?t=1587926849583 (accessed May 3, 2020).

Mayor, S. (2020). *Covid-19: Researchers Launch App to Track Spread of Symptoms in the UK* (BMJ).

McCall, B. (2020). Shut down and reboot—preparing to minimise infection in a post-covid-19 era. *Lancet Digit. Health* 2, E293–E294. doi: 10.1016/S2589-7500(20)30103-5

McMahan, B., and Ramage, D. (2017). *Federated Learning: Collaborative Machine Learning Without Centralized Training Data*. Google Research Blog.

McMahan, H. B., Moore, E., Ramage, D., Hampson, S., et al. (2016). Communication-efficient learning of deep networks from decentralized data. *arXiv* 1602.05629.

Miller, G. (1998). Adding gps applications to an existing design. *RF Des*. 21, 50–57.

Muñoz-González, L., Biggio, B., Demontis, A., Paudice, A., Wongrassamee, V., Lupu, E. C., et al. (2017). "Towards poisoning of deep learning algorithms with back-gradient optimization," in *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security* (Dallas, TX), 27–38. doi: 10.1145/3128572.3140451

Muoio, D. (2020). *Mit's Covid-19 App Uses Smartphones' Bluetooth to Anonymously Spot Disease Contacts*. Available oline at: https://www.mobihealthnews.com/news/mits-covid-19-app-uses-smartphones-bluetooth-anonymously-spot-disease-contacts (accessed May 5, 2020).

Mozur, P. R. Z., and Krolik, A. (2020). *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags*. New York Times. Available online at: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html (accessed May 3, 2020).

Raskar, R., Schunemann, I., Barbar, R., Vilcans, K., Gray, J., Vepakomma, P., et al. (2020). Apps gone rogue: maintaining personal privacy in an epidemic. *arXiv* 2003.08567.

Sapiezynski, P., Stopczynski, A., Gatej, R., and Lehmann, S. (2015). Tracking human mobility using wifi signals. *PLoS ONE* 10:e0130824. doi: 10.1371/journal.pone.0130824

Shokri, R., Stronati, M., Song, C., and Shmatikov, V. (2017). "Membership inference attacks against machine learning models," in *2017 IEEE Symposium on Security and Privacy (SP)* (San Jose, CA: IEEE), 3–18. doi: 10.1109/SP.2017.41

Sivapriyan, E. (2020a). *Coronavirus: Tamil Nadu Launches App to Provide Advice to Those Under Home Quarantine*. Available online at: https://www.deccanherald.com/national/south/coronavirus-tamil-nadu-launches-app-to-provide-advice-to-those-under-home-quarantine-816562.html (accessed May 3, 2020).

Sivapriyan, E. (2020b). *Private Kit: Safe Paths; Privacy-by-Design Covid19 Solutions Using GPS + Bluetooth for Citizens and Public Health Officials*. Available online at: http://safepaths.mit.edu (accessed May 4, 2020).

Staunton, D. (2020). *Britain's 'World Beating' Covid-19 Tracing App Had One Problem–It Didn't Work*. Available online at: https://www.irishtimes.com/news/world/uk/britain-s-world-beating-covid-19-tracing-app-had-one-problem-it-didn-t-work-1.4298623

Steinhardt, J., Koh, P. W. W., and Liang, P. S. (2017). "Certified defenses for data poisoning attacks," in *Advances in Neural Information Processing Systems*, eds Guyon, I., Luxburg, U. V., Bengio, S., Wallach, H., Fergus, R., and Vishwanathan, S. (Curran Associates, Inc.) 30, 3517–3529. Available online at: https://proceedings.neurips.cc/paper/2017/file/9d7311ba459f9e45ed746755a32dcd11-Paper.pdf

Sun, L., Axhausen, K. W., Lee, D.-H., and Cebrian, M. (2014). Efficient detection of contagious outbreaks in massive metropolitan encounter networks. *Sci. Rep*. 4:5099. doi: 10.1038/srep05099

Swanson, K. C., Altare, C., Wesseh, C. S., Nyenswah, T., Ahmed, T., Eyal, N., et al. (2018). Contact tracing performance during the ebola epidemic in Liberia, 2014–2015. *PLoS Negl. Trop. Dis*. 12:e0006762. doi: 10.1371/journal.pntd.0006762

Tang, Q. (2020). Privacy-preserving contact tracing: current solutions and open questions. *arXiv* 2004.06818.

Tidy, J. (2020). Available online at: https://www.bbc.com/news/av/world-asia-52104798/coronavirus-how-china-s-using-surveillance-to-tackle-outbreak/ (accessed May 3, 2020).

Tramèr, F., Zhang, F., Juels, A., Reiter, M. K., and Ristenpart, T. (2016). "Stealing machine learning models via prediction APIS," in *25th {USENIX} Security Symposium ({USENIX} Security 16)* (Austin, TX), 601–618.

Trieu, N., Shehata, K., Saxena, P., Shokri, R., and Song, D. (2020). Epione: lightweight contact tracing with strong privacy. *arXiv* 2004.13293.

Troncoso, C., Payer, M., Hubaux, J.-P., Salathé, M., Larus, J., Bugnion, E., et al. (2020). *Decentralized Privacy-Preserving Proximity Tracing*. Lausanne: Github DP-3T Documents 12.

UK Parliament (2018). *Data Protection Act 2018* (London).

Ur Rehman, M. (2010). *Characterisation of human body and environmental effects on the performance of mobile terminal antennas* (Ph.D. thesis), Queen Mary University of London, London, United Kingdom.

Vaudenay, S. (2020). *Analysis of DP3T*. Cryptology ePrint Archive, Report 2020/399. Available online at: https://eprint.iacr.org/2020/399

Viboud, C., and Santillana, M. (2020). Fitbit-informed influenza forecasts. *Lancet Digit. Health* 2, E54–E55. doi: 10.1016/S2589-7500(19)30241-9

Winer, S. (2020a). *Health Ministry Launches Phone App to Help Prevent Spread of Coronavirus*. Available online at: https://www.timesofisrael.com/health-ministry-launches-phone-app-to-help-prevent-spread-of-coronavirus/ (accessed May 3, 2020).

Winer, S. (2020b). *To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data*. New York Times. Available online at: https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html?referringSource=articleShare (accessed May 3, 2020).

Wired (2020). *An Artist Used 99 Phones to Fake a Google Maps Traffic Jam*. Available online at: https://www.wired.com/story/99-phones-fake-google-maps-traffic-jam/ (accessed May 5, 2020).

Wray, S. (2020). *South Korea to Step-Up Online Coronavirus Tracking*. Smart Cities World. Available online at: https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109 (accessed May 3, 2020).

Xu, H., Zhang, L., Onireti, O., Fang, Y., Buchanan, W. J., and Imran, M. A. (2020a). BeepTrace: blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond. *arXiv* 2005.10103.

Xu, P., Dredze, M., and Broniatowski, D. A. (2020b). The twitter social mobility index: measuring social distancing practices from geolocated tweets. *arXiv* 2004.02397.

Yang, C., Wu, Q., Li, H., and Chen, Y. (2017). Generative poisoning attack method against neural networks. *arXiv* 1703.01340.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., and Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet Things J*. 1, 22–32. doi: 10.1109/JIOT.2014.2306328

Zhang, Y., Jia, R., Pei, H., Wang, W., Li, B., and Song, D. (2019). The secret revealer: generative model-inversion attacks against deep neural networks. *arXiv* 1911.07135. doi: 10.1109/CVPR42600.2020.00033

Zhou, F., Yu, T., Du, R., Fan, G., Liu, Y., Liu, Z., et al. (2020). Clinical course and risk factors for mortality of adult inpatients with covid-19 in Wuhan, China: a retrospective cohort study. *Lancet* 395, 1054–1062. doi: 10.1016/S0140-6736(20)30566-3

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.