Applicability of Mobile Contact Tracing in Fighting Pandemic (COVID-19): Issues, Challenges and Solutions

Aaqib Bashir Dar[a], Auqib Hamid Lone[b,*], Saniya Zahoor[b], Afshan Amin Khan[b], Roohie Naaz[b]

[a]*Independent Researcher, Jammu and Kashmir,India,190015*
[b]*Department of Computer Science and Engineering, NIT Srinagar, Jammu and Kashmir, India,190006*

Abstract

Contact Tracing is considered as the first and the most effective step towards containing an outbreak, as resources for mass testing and large quantity of vaccines are highly unlikely available for immediate utilisation. Effective contact tracing can allow societies to reopen from lock-down even before availability of vaccines. The objective of mobile contact tracing is to speed up the manual interview based contact tracing process for containing an outbreak efficiently and quickly. In this paper we throw light on some of the issues and challenges pertaining to the adaption of mobile contact tracing for fighting COVID-19. In essence we proposed an Evaluation framework for mobile contact tracing solutions to determine their feasibility and effectiveness. We evaluate some of the available contact tracing solutions in light of our proposed framework. Furthermore we presented possible attacks that could be launched against contact tracing solutions with necessary countermeasures to thwart any possibility of such attacks.

Keywords: COVID-19, Contact Tracing, Security, Privacy, Scalability.

1. Introduction

Secure Acute Respiratory Syndrome (SARS) is an atypical pneumonia that is characterized by a high rate of transmission, which began in Guangdong Province, China, in November 2002 [1]. One of the largest SARS outbreaks to date began in Singapore in mid-March 2003 [1] and was traced to a traveler returning from Hong Kong. Recently in China, several local health facilities in Wuhan, Hubei Province, reported clusters of patients with pneumonia of unknown cause that they supposedly and epidemiologically linked to a seafood and wet animal wholesale market in the province. However the due spread through untraced contacts eventually lead to it's spread on a global scale which is what we see today as a pandemic Covid-19. [2]. Contact Tracing is a key strategy for mitigating the impact of infections like COVID-19 on health care

*Auqib Hamid Lone
Email address: ahl@nitsri.net (Auqib Hamid Lone)

systems in specific and health of the population in general, thereby is expected to slow the spread of infectious diseases. It allows individuals of a country or a community to relieve distress from a community's containment measures, as it gives the corresponding infected individuals a chance to quarantine themselves voluntarily. Contact tracing is expected to increase the sensitivity followed by the readiness of a country, a community, or individuals for an emerging pandemic like novel CoronaVirus (COVID-19) by mitigating the already available flaws of the traditional detection which solely relied on symptoms. According to WHO [3], contact-tracing occurs in three steps:

1. *Identifying the Contact:* From the already confirmed positive cases, identifying those that the patient had contact with (according to the transmission modalities of the pathogen).
2. *Listing of Contacts:* Keep a record of possible contacts of the infected patients and inform those individuals.
3. *Contact Follow-Up:* A necessary follow-up of the patients that are believed to have come in contact with the infected individuals and those who are positive.

Containment is a primary road-map to quickly halt an outbreak, which might become an epidemic and then in the worst case into a pandemic, which is what happened in case of COVID 19. Containment is accomplished by rapid identification followed by the quarantine of that particular infected individual. The next step is to determine the people who they had contact with in the previous days or maybe weeks followed by the decontamination of the places that the infected individual has had travel history to. In essence, this process is expensive in terms of labor and prone to various errors with a focus on privacy related concerns. With a limited number of resources the government has, the process of contact tracing needs to be automated so as to stop the untraced spread of the disease. In order to understand why contact tracing is so important we need to determine how contagious a disease is which in turn depends upon the average number of individuals that will catch the disease from one infected individual. These features are mainly determined by parameters such as the infectious period, the rate of contact and the mode of transmission. Both incubation period and the mode of transmission are the functions of the nature of the disease causing pathogen. Thus only controllable parameter being the contact rate, which needs to be traced and controlled accordingly. Thereby, providing an idea about how important contact tracing is and how helpful it can be for lowering the rate of transmission of a disease before it's translation into a pandemic. Ferretti et al. [4], made predictions about whether contact tracing and isolation of known cases is enough to prevent the spread of the epidemic. They quantified the expected success of digital contact tracing and suggested some requirements for its ethical implementation. As the need arise, several proposals are being proposed to contain the further spread of this pandemic. It is equally important to have an evaluation criteria for these solutions so as to check which solution deems fit for adoption. Rest of the paper is organized as follows: Section 2 discusses about issues and challenges in adopting mobile contact tracing solutions. Section 3 presents proposed framework for evaluating contact tracing solutions. In Section 4 we evaluated some of the available contact tracing solutions in light of our proposed framework. Section 5 presents the taxonomy of the possible attacks on available contact tracing solutions and Section 6 finally concludes the paper. A brief summary of most of the

available contact tracing solutions is presented in the form of Table as an Appendix A.

2. Issues and Challenges in Mobile Contact Tracing

In this section, we discuss issues and challenges pertaining to adaption of contact tracing solutions. Digital contact tracing speeds up the process of identification of the individuals who might have come in close contact with the contagious ones. However, before merging the traditional contact tracing with the state-of-the-art technology, there exist potential risks and issues there-by for every contact traced individual that need to be identified and addressed by the researchers. The Primary concern of which is securing the identity of infected individuals from each other, stopping the spread of misinformation, stopping snoopers from causing panic among the masses and withheld countries from establishing a surveillance state, even in the time of this crisis. Among the suggested solutions to be adapted as a digital contact tracing mechanism, some of which are based on GPS tracking and the ones that are based on Bluetooth based token sharing. However, there are issues with the underlying technology that are to be understood which otherwise might be leveraged by bad actors, surveillance state/government for misuse. Automatic Contact tracing systems based on Bluetooth communications was first proposed by Altuwaiyan et al [5] in 2018. The Bluetooth based systems can directly detect whether users came in proximity of each other. The proximity can be approximated by the strength of the signal which is reduced by obstructions like walls; therefore in a high risk environment for close contact like buildings or public transits it can more effectively and accurately reflect functional proximity [6]. However, with applications that evaluate exposure risk based on Bluetooth proximity exchange is in essence not sufficient because of the fact that apart from the human to human interaction, Coronavirus (COVID-19) can also transmit through common environments or commonly touched surfaces [7]. Another important drawback of pure Bluetooth based systems is the problem of slow or low rate of adoption which in turn limits the user base thus affecting the effectiveness of the system. Zeadally et al., in [8] has provided a detailed discussion on issues and possible attacks on Bluetooth technology. GPS is not secure by its inherent nature. There are also some functionalities that GPS based systems cannot provide. One of the main concerns is spoofing attacks where a spoofer creates a false GPS signal with an incorrect time and location to a particular receiver [9]. Warner et al., in [10] gave a simple demonstration to show GPS is vulnerable to spoofing.

Considering the advancements in technology, almost every second individual on earth carries a device which has the capabilities of being tracked through GPS with proper infrastructure [3]. The capabilities like that of tracking location trails with proper timestamps and the ability to log them can certainly allow one to compare infected individuals with that of the ones who have been in their close proximity thus enabling contact tracing. Now that we know what is at stake, it is also important to understand the magnitude of the grave consequences it can draw. But as contact tracing is widely being demanded. There are a number of proposals leveraging state-of-the-art technology to make contact tracing actually possible in practice. Though there's not a general framework or an assessment criteria to determine the level of privacy it provides or the extent to which a proposed system withholds certain attacks. But in the later part of

this paper, we propose an evaluation framework and evaluate some of the systems under the model to discuss the proposed solutions. Some examples of mass surveillance activities that can have some serious consequences are:
Israel passed a legislation that allows the government to track the mobile phone data of individuals suspected to be infected[11]. South-Korean government on the other hand has maintained a public database of known patients which contains information about their occupation, age, gender and travel routes [12]. With several problems arising one after the other, it is important to look closely at these solutions and evaluate them on certain parameters. In order to do that, we have proposed a model for evaluating contact tracing solutions and check how a solution behaves under these parameters. It gives an idea about which solution deems to fit to be adopted widely.

3. Proposed Evaluation Framework for Contact Tracing Solutions

The proposed evaluation framework is a five-step method for evaluating a particular contact tracing solution as shown in Figure 1. The steps of the framework are depicted in the diagram and are summarized below. The aim of our evaluation model is to categorize the contact tracing solutions so as to be able to identify each one easily and to have general criteria for the evaluation of contact tracing solutions. We will put some widely known proposals under the framework's assessment criteria and analyze them one by one.

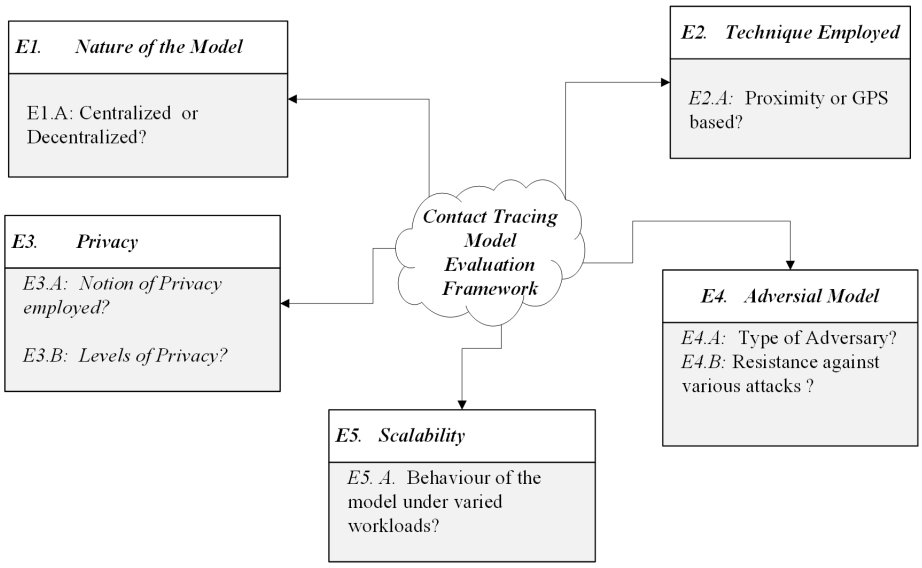

Figure 1: Basic Contact Tracing Evaluation Framework

- **Nature of the model (Centralized or Decentralized)**
  The question of whether a solution should be centralized or decentralized is of central importance in contact tracing because of the fact that in centralized systems we have a semi-trusted authority like a Health Authority or a government

authority in our case. For example in the case of Singapore's TraceTogether app [13], the government keeps a database that links tokens to phone numbers and identities. They can build a list of all other people they have been in contact with after an infected user is compelled to upload his data. With these things into consideration, no individual would want to be exploited by a central authority in any circumstances. Thus, the notion of decentralization gives individuals a sigh of relief. We look at it as a policy that fulfills the necessary requirements of contact tracing while providing the privacy we want. However, Vaudenay in [14] provided great insights into security and privacy analysis by arguing that the decentralization, contrary to common belief that decentralization solves the privacy concerns of centralized systems. Rather, it introduces some new attack vectors against privacy itself. For literature relevance, we have organized proposals in A.1 and characterized them in a context that we feel is important to contact tracing.

- **Technique Employed (Proximity based or GPS based)**
  Our second assessment criterion is to understand the technique employed upon which the contact tracing solution works. Since the idea is to track the people who came in contact with each other, the two mechanisms that can help us to determine this are Proximity based and GPS based which are what maximum solutions rely on, some of the solutions employ the use of both. The widely adopted solution is Proximity based due to all the evident reasons. Since Proximity based solutions are usually more accurate compared to GPS based solutions [15], it is one of the reference selection parameters. Among the other parameters is its ability to classify close contacts with a significantly lower false positive rate than GPS [15], its low power consumption and the rate of adoption. The rate of adoption is another important parameter for contact tracing solutions. It is quite evident that people are wary of tracking the location data, which can hamper its adoption and pave a way for Proximity based solutions.

- **Privacy**
  Privacy is the backbone of contact tracing solutions. Safeguarding privacy should be the first step in devising contact tracing solutions. Privacy of individuals has not been a concern in some of the contact tracing proposals. Some countries have even adopted the notion of mass surveillance to track people in the name of contact tracing [16]. Although there is not a single notion of privacy that can guarantee with certainty the privacy requirements that a contact tracing solution needs but we can try to formulate certain notions of privacy so as to make privacy preserving a real thing in practice. To that end, we adapt the notions used by Cho et al., in [17], because these notions seem to be general to all the schemes and relevant to the design of contact tracing solutions. We have defined levels of privacy of the proposed models based on the desired notions of privacy they provide. We define (L1) as the first level which encompasses the first notion, i.e. Privacy from Snoopers. The second notion is considered as level second (L2)

which includes Privacy from Users. The third and final notion is regarded as the (L3) which takes Privacy from Authorities into consideration.

- **Adversarial Model Evaluation**
  Considering the importance of data being uploaded for effective detection of individuals who have been in contact with a contagious one and the privacy concerns that come along with it. In our opinion, a semi-honest Model of privacy [18] is expected to be the best fit. We also take into consideration various roles of an adversary or a nefarious actor as to what he can do to invade the privacy of users. The analysis of a contact tracing system in the adversarial model will be focusing on how the proposed system is behaving under various attacks and its ability to countermeasures against certain attacks. We will discuss the possible attacks that we have seen in different proposals as of now and their possible countermeasures. A separate section on attacks will be followed later where some generic attacks will be taken into consideration along with attacks that are possible due to the vulnerabilities in the technology being adapted. We do realize that some proposals might be viewed in light of some different adversarial models along with the roles of the adversaries. But to our knowledge, the best model to be taken into consideration will be the semi-honest model. We will be evaluating each proposal under this setting.

- **Scalability**
  After a contact tracing solution is being developed, it is then important to understand and analyze how it adapts under various parameters. For a widespread adoption of a contact tracing proposal, it is important to understand its scalability in terms of the number of users adopting the same and the varied workloads under which the system has to go through. For brevity, we will be discussing scalability in terms of the number of users adopting this technology and the behaviour of the mobile application to varied workloads.

4. Evaluation of the proposed solutions

In this section, in light of the proposed evaluation framework as described in section 3. We evaluated and analyzed some of the proposed contact tracing solutions only. The reason being lack of available information about the proposed solutions. However, we have provided brief summaries of most of the solutions in Table A.1 as an Appendix. Owing to clear understanding and simplicity, we adapt Tang's notations [15] to indicate the workflow of contact tracing solutions. We briefly describe the architecture of each solution. We will give insights into some contact tracing solutions and discuss them in light of our framework. We start with a solution which is the first proposed privacy-preserving contact tracing solution that paved a way for other proposals.

4.1. EPIC

Altuwaiyan et al's [5] model is an efficient privacy preserving contact tracing for detecting infection that enables users to upload their data securely to the server and if

in case someone gets infected, others can check whether they ever came in contact with him. No unnecessary information is disclosed to the server. A matching score is used to represent the result of the contact tracing. The technical specifications are described below.
The participating entities in the system model are:

- Smartphones
- short-range wireless devices like Access points
- Bluetooth devices and
- A server (the server stores the encrypted data from the users and the timestamps in plaintext)

The phases of the architecture are described below.

Setup or initialization Phase
Since no special setup is needed. We assume that this phase has occurred.

Scanning or Sensing Phase
During this phase, the user's smartphones will collect raw data about nearby short-range wireless signals WiFi and Bluetooth by performing timely adaptive wireless scanning.

Reporting phase or Detection Phase
When a user is detected as positive, then he will upload his data to the server which is encrypted with corresponding timestamps for each network scan. The data: Wireless Device Unique Identifier (**BSSID**), Wireless Signal Strength indication (**RSSI**) and Wireless Signal type (**WiFi, Bluetooth**) are depicted as tuples of data points (t_x , ($m_{i,1}$, $r_{i,1}$, $p_{i,1}$), ...,($m_{i,n_{i,x}}$, $r_{i,n_{i,x}}$, $p_{i,n_{i,x}}$)) where ($m_{i,1}$, $r_{i,1}$, $p_{i,1}$) depicts information about the first encountered device. $m_{i,1}$ is the hashed unique identifier, $r_{i,1}$ is the strength of the detected signal and $p_{i,1}$ is the device type for time intervals t_0 and so on.

Tracing phase
When a user is identified to be infected and a user wants to check whether he has been in close contact with an infected patient, he sends a request which includes his public key. The server matches the scans between the infected user u_i and the requested user is based on timestamps. Note that the timestamps are stored in plaintext on the server. The second step after matches are found is to check whether these two individuals have scanned similar wireless devices. The server has the information of the infected individual in plaintext already. However, no information about a regular user is available to the server. The server uses the user's public key which it received and encrypts each mi where $m_i u_i$. The server returns a matrix which has the encrypted subtraction of all pairs of m_i and m_n using a homomorphic encryption scheme multiplied by a random value d added by the server to prevent u_n from knowing unnecessary information about u_i.

	$m_{i,2}$	$m_{i,3}$
$m_{n,1}$	Enc($(m_{n,1} - m_{i,2}) + d_{1,2}$)	Enc($(m_{n,1} - m_{i,3}) + d_{1,3}$)
$m_{n,2}$	Enc($(m_{n,2} - m_{i,2}) + d_{2,2}$)	Enc($(m_{n,2} - m_{i,3}) + d_{2,3}$)
$m_{n,4}$	Enc($(m_{n,4} - m_{i,2}) + d_{4,2}$)	Enc($(m_{n,4} - m_{i,2}) + d_{4,3}$)

The results of the matrix are then decrypted by the user and a binary array is retrieved corresponding to the decryption result. 1 indicates that two wireless devices matched and vice versa. The user i also sends $r_{i,y}$ with the matched $m_{i,y}$ where $1 < y < n_{i,x}$. EPIC is also a new method to measure the distance between two smart devices as is evident from the proposal itself. This in practice is more accurate than other solutions.

Taking into account the privacy of the proposal model, the infected individuals are supposed to reveal the location data to the server where the network identifiers are hashed. It is to be noted that since network identifiers are often static, this gives the server the freedom to compute the location data points of the infected users. Another important thing to note is that since the timestamps are stored in plain-text which means at a particular timestamp the location of the user is available to the server. So, based on our evaluation criteria, it is clear that homomorphic encryption is used to ensure that the queries remain private. The manipulations are done on the encrypted data itself. While, the level of privacy this solution provides is L1, L2 and L3 but there are some serious concerns when it comes to L3 i.e. Privacy from Authorities. Like we discussed above, there's a possibility of attacks and some serious privacy leaks that should be avoided and surely certain measures should be taken into consideration and if the modifications are done right, we assume the L3 privacy will be provided in its entirety. Speaking of the model in light of the model of privacy, it is important to consider that the notion of semi-honest model fits the purpose here. To this end, we have seen that the privacy concerns here are the deductions that the server can do based on the information being uploaded thereby linking users based on particular timestamps. However, note that we do not take the case of a malicious actor contaminating the database with faulty queries. Speaking of scalability as another important factor which impacts its widespread adoption, the proposed model has developed an android application and tested it under various scenarios. Though the number of users that the app was tested with was 10. It is worth taking into consideration the system behaviour when the number increases 10x which is another simpler case. Though some scenarios are discussed in the proposed model itself, the overhead will surely increase as the number of users increases.

4.2. TraceTogether

TraceTogether[13] is the first mobile application based adoption of contact tracing. A system developed by Singapore's Government Technology Agency along with the Ministry of Health to tackle the ongoing pandemic. The app operates by exchanging time varying tokens via Bluetooth connections between nearby phones.

The entities in the this solution are:

- Users and
- Ministry of Health (MoH)

It is believed that the Ministry of Health (MoH) of Singapore government is to be trusted to protect the users information thus making this solution a centralized one. It is to be noted that a user might be compelled by the authorities to release his data on the app in case someone is diagnosed with COVID19 and it is a crime in Singapore not to assist the Ministry of Health in mapping one's movements.

Setup or Initialization Phase During this phase, the users download the TraceTogether app [13] and installs it on the phone. The app then sends the phone number to MoH and receives a pseudonym from them. MoH stores in its database the pair (NUM_i, ID_i) where NUM_i is the phone number of the user i and the ID_i is the pseudonym generated by the authority against this number. The authority then generates the secret key K and selects an encryption algorithm Enc. Before the app was launched, the MoH of Singapore selected some time intervals $[t_0, t_1, ...]$, which will end right when the pandemic is over. For a user i, MoH sends the initial pseudonym $TID_{i,x}$ = Enc(ID_{i,t_x}; K) to the user's app at the beginning of time interval t_x for x_0.

Scanning or Sensing Phase User broadcasts $TID_{i,x}$ at the time interval $[t_x, t_{x+1})$ for all x_0. Users store the TID's of each other along with the signal strength i.e. if user i and j come in range of Bluetooth communication they will store ($TID_{i,x}$, $TID_{j,x}$ SigStren) where the first two entries are the corresponding pseudonyms of the users i and j respectively at time interval t_x and SigStren is the signal signal between their devices.

Reporting phase or Detection Phase If a user is tested positive for COVID-19 then he'll have to comply with MoH and upload the locally stored data to MoH's database.

Tracing phase After user i stores the data on to the MoH'server, MoH then decrypts every single $TID_{j,x}$ and obtains ID_j through which they can lookup his NUM_j and then do the necessary followup.
Now that, the proposal is completely well understood. It is quite clear that the proposed contact tracing solution is a proximity based centralized one where the centralized authority is the Ministry of Health. The encryption technique is chosen by the authority so the notion of privacy is not clear in a sense that it is under the direct control of MoH. Speaking of the level of privacy, the app provides L1 and L2 levels of privacy since time varying tokens offer privacy among the users. However, it is to be noted that the time varying nature of these random tokens also provides privacy from snoopers to a greater extent if refresh rate is well set, because if the rate is too frequent then the server will have to store huge number of tokens and if the rate is slow then the user can be tracked down by a snooper while walking down the street. Here we use the Semi-honest model of privacy which is quite obvious due to the fact that the solution

is centralized and under complete control of the MoH of the Singapore government. Though the central authority is following the protocol but if needed, they can deviate from it depending upon the circumstances. Since the proposed model relies on the authority (trusts) thereby lacks L3 level of privacy because there is a possibility of a linkage attack[19]. The behaviour of TraceTogether [13] under various modifications is given in [17].
Speaking of scalability, though it is not clear how many people have installed the application, it is a voluntary choice for the Singaporean's to install the app. But the noticeable part here is, if a large number of individuals in Singapore adapt this technology as a measure to stop the spread of COVID19, the amount of location data at certain points of time which is exposed to the authorities will be huge and can draw huge consequences. There's a possibility that a malicious user can manipulate (i.e. add or delete) the data collected by the app. Another possibility is of relay attacks. In addition, some other attacks proposed by Vaudenay in analysis of DP-3T [14]. Since there's an advantage of identifying individuals but at the cost of an expensive trade-off between privacy and utility.

4.3. Reichert's MPC based Solution

Reichert's MPC based solution [20] consists of two parties under semi-honest security settings. This solution leverages that fact that the already available applications of contact tracing which use location-based-services and store their history locally and Health Authorities can use the data points of infected individuals to initiate an MPC session with anyone who wants to trace themselves.
The participating entities are:

- Users and
- Health Authority (HA) offers data matching as a service after collecting and storing the geolocation data of the individuals.

The phases of the proposed solution can be briefly discussed below:

Setup or Initialization Phase During the setup phase, Health Authority (HA) prepares the cryptographic keys for later use in generation of garbled circuits.

Scanning or Sensing Phase In this phase, users record their geolocation data points on the fly for different time intervals $[t_0, t_1,...]$. At a particular time tx, a user A generates and stores a tuple $(t_x, l_{x,u}, l_{x,v})$, where $l_{x,u}$ and $l_{x,v}$ represents latitude and longitude of the location respectively. The health authority can then use these data points in order to initiate a MPC session with every individual who wants to trace themselves.

Reporting phase or Detection Phase If a user is detected positive for COVID19, then he will share the data points with the HA.

Tracing phase The Health Authority sends a garbled circuit to all those that are interested. Each user has to perform oblivious communication with the HA. Based on

the shared data points, the participating parties together will determine where the trajectories of infected and non-infected individuals intersect. A joint computation is performed by the HA and the users and by performing a secure binary search on the ORAM. If an element is found, then the user has been in close contact with an infected individual.

In light of our proposed framework, the model is geolocation based and has a central Health Authority. Garbled circuit (GC) construction which is fundamental to Multi-party Computation is used to seek privacy between the users such that no information about the inputs and outputs are revealed. The level of privacy this solution offers is L1 and L2. Since the model we're taking into consideration is semi-honest, discussing that the proposed solution does offer L3 privacy will be misleading. There are several attacks that are possible on this proposed solution. Since this contact tracing solution is a theoretical cryptography solution, the other aspects are overshadowed. There's a possibility of a DDoS attack in a situation where the number of users grows exceedingly large. In that case, HA will have to prepare garbled circuits for all the individuals thereby increasing the overhead and complexity, which in turn will drop its efficiency. The attacks that are technology specific are not considered in this analysis since we have a separate section devoted to attacks which cover attacks on GPS based systems as well. Scalability on the other hand will be a bottleneck since there are factors that will hinder the adoption of this solution unless necessary countermeasures are taken in this regard.

4.4. CAUDHT

This is a decentralized system based on distributed hash tables which limits the responsibilities of a HA to just confirming results of confirmed positive individuals by minimizing the amount of data that the centralized authority can derive from the protocol. The system is believed to be adaptable to proposals like DP-3T, though as an extension and not as a replacement.
The entities in the CAUDHT [21] model are:

- Users and
- Distributed Hash table (DHT)
- Health Authority (HA) is merely used to retrieve signatures for the corresponding Bluetooth low energy (BLE) ID's which verifies the infected individual.

The phases of this proposed solution are briefly described below:

Setup or Initialization Phase
During the setup phase, we assume that the users have installed the app and a common DHT is chosen as a store-and-retrieve postbox where storage is provided as a key-value store. Apart from this, the HA needs to publish its public key before the protocol is run for infection verification.

Scanning or Sensing Phase
The CAUDHT protocol offers several protocol mechanisms and sensing in the proposed solution takes place as the collection mechanism. In the collection mechanism, the BLE IDs are broadcasted after a scan is performed to look for nearby devices. Each device advertises an ID which is stored when a signal is picked up from a device. These IDs are generated by means of an asymmetric key pair where the secret key is stored on the phone and the corresponding public key is broadcasted. This allows later verification that the contact with an infected individual actually happened. The scan retrieves 256bit ID which occurs automatically in android and iOS[22]. The BLE IDs are stored locally on a user's phone.

Reporting phase or Detection Phase
After a user is tested positive, he is supposed to retrieve HA's signature for every shared BLE ID in a blind way. For this purpose, textbook RSA is used for blind signatures in order to verify an infected user. Since HA's public key is available to all, the users can verify that the individual is actually the infected one and not a malicious one. When a user had come in contact with an infected user it had received the BLE IDs from that user. Since the IDs are public keys, she encrypts her own BLE ID that she advertised during the last time she encountered this specific ID of that particular user. The infected user then accesses the DHT and stores the signatures of encrypted BLE ID at the DHT addresses corresponding to the user who came in contact with an infected user.

Tracing phase
This phase in the proposed solution is called the Pooling mechanism. In order to check whether a user has been in contact with an infected person, they need to periodically query the DHT. After a user is detected positive, he leaves a message in the corresponding contact's postbox. Since the message was encrypted with the corresponding contact's public key, the corresponding contact can search for this key in the DHT. An encrypted result will be returned which can then be decrypted by the corresponding user who holds the secret key.
Speaking of the proposed model in light of our framework, it is decentralized and uses proximity based tracing. Distributed Hash Tables (DHTs) are used to allow decentralization rather than relying on a central database. The levels of privacy this solution offers is L1, L2 and L3. Although there are several underlying issues with the proposed solution where future modifications are needed, we highlight some of them here. In the semi-honest model setting, we consider a scenario where a malicious positive patient could claim to have seen the random BLE IDs which in turn will make users believe they have contracted the disease. This is avoided by the lookup which is provided by DHT. The system resists against linkage attacks possible by the Health Authority. An eavesdropper cannot claim to be infected since a signature from the Health Authority uniquely determines an infected user from a non-infected one. Non-infected users can also try to learn about the ones who came in contact with an infected one. If a message is placed in the DHT when an infection is confirmed, an eavesdropper can conclude that the user has been in contact with an infected user. In order to prevent this, postboxes can hold more than one message and users can write random messages into their own or other users' postboxes. Only the meaningful will be taken and the random ones

discarded. The security of the system is enhanced with the use of DHT and Blind Signatures. In terms of how scalable the solution is, DHT is more scalable than the options available like Tor [23] to be used for hiding a user's identity. As proposed by the model, growth of the DHT does not affect the scalability problem. DHT overflow is avoided by deleting the older entries preferably after 14-21 days because for that period only, the data is useful. The amount of data stored in the DHT is constant no matter how many participants there are since all users are part of the DHT's set of nodes.

4.5. Berke et al's location based system

Berke et al's [24] contact tracing model is a GPS based solution for contact tracing that leverages partitioning of fine-grained GPS locations and private set intersection allowing the system to detect when a user came in close proximity with positive patients to assess and inform them of the risk privacy preservation of individuals.
The entities or participating entries of the system are:

- Users in possession of a smartphone and
- Server (used to store the redacted, transformed and encrypted data)

The various phases of the system can be described briefly below:

Setup or Initialization Phase
It is assumed that users possess a smartphone capable of collecting and storing data.

Scanning or Sensing Phase
As the users move throughout the day, timestamped GPS points are collected within a user's device. The data is collected in the form of tuples of latitude, longitude and time: (latitude, longitude, time).

Reporting phase or Detection Phase
A user's app scans/checks for matches between their collected points and the points shared by users who were diagnosed as positive carriers so as to identify points of contact. Though the GPS points are never directly compared to find the matches, they are instead matched to a 3-dimensional grid where two dimensions are latitude and longitude while as the third dimension is time. They are then obfuscated using a deterministic one-way Hash function (e.g. NIST Standard SHA256).

Tracing phase
When a patient is diagnosed as a positive carrier, they share their redacted, anonymized, hashed point intervals to the server. Users periodically share their point intervals with the central server to detect if their hashed point intervals matched with anyone diagnosed to be a positive carrier. This happens by means of a Private set protocol.
Speaking of this solution in light of our framework, this is a GPS based solution where privacy preservation is done using either manual or automatic redaction, obfuscation using a deterministic hash function along with Private set intersection. Though the system provides L1 and L2 level privacy. It is highly likely that the system provides L3 level privacy though the semi-honest nature of the server suggests that it can be

compromised as well. Speaking of attack vectors in the semi-honest setting, several things are to be taken into consideration. Since, for the wide adoption of Bluetooth based solutions special applications are required that could suffer from slower or limited adoption. Thus, the fact that the applications on a user's phone are already collecting the user's GPS location histories, this solution leverages the fact that this is infact important to more quickly roll out their system as a life saving alternative for contact tracing technology. They provided a simple scheme that uses Diffie-Hellman protocol [25] to better understand how Private set intersection supports the privacy goals set by the model. There certainly are privacy risks if a model is constructed based on their intermediary implementation which involves publishing of data points to a flat data file for other users to download rather than having a server perform private set intersection protocol. The concern with this is the attacker's attempt to reconstruct location histories of users diagnosed as carriers and possible re-identification of those from their shared anonymized data. There are other issues when it comes to tradeoff between privacy, adoption and possible risks which might be the deciding factor for scalability. However, it is also suggested that the proximity and GPS location sharing should be opt-in.

4.6. DP-3T

Before we get into the technical details of the best known system for contact tracing, at least until now. We will talk about DP-3T's [26] inclusion in PEPP-PT as a potential candidate followed by its exclusion which received serious backlash from the scientific community amidst this pandemic. A team of 25 researchers from 8 European institutes collaborated to produce a privacy-preserving contact tracing solution on a fast-track basis. The transparent process of DP-3T makes it a different and trustworthy system for contact tracing from the already available solutions. Though PEPP-PT has not commented on why they excluded DP-3T from their website but this raised serious concerns among the scientific community where they feel this is unacceptable under any circumstances. 300+ scientists from all over the world have signed a document highlighting four principles that they feel should be adopted while going in the direction of designing contact tracing systems. Decentralization and Open Sourceness lies at the very core of DP-3T. The entities present in the DP-3T are:

- The Users
- Health Authority (HA)
- Server (Note that the backend server is used for matching activities between the users)

The phases of the proposed solution are briefly described as below:

Setup or Initialization Phase
It is assumed that a user possesses a smartphone that is capable of collecting and storing data. User i in this phase generates a random initial daily key SK_i, and computes the following-up daily keys based on a chain of hashes: i.e. the key for day 1 is

$SK_{i,1} = H(SK_{i,0})$ and the key for day x is $SK_{i,x}$= H($SK_{i,x-1}$). The identifiers for a user i on a particular day x is generated as follows (say n ephemeral IDs are required in a day): $EphID_{i,x,1}$ ||...||EphID$_{i,x,n}$ = PRG(PRF($SK_{i,x}$, "broadcastkey")). Note that length of SK is not specified but the suggested length is HMAC-SHA 256 key.

Scanning or Sensing Phase
In this phase, ephemeral IDs $EphID_{i,x,1}$,...,$EphID_{i,x,n}$ are broadcasted in a random order by user i. At the same instant of time, the received ephemeral IDs are stored on his smart phone along with the corresponding proximity of the device, duration, some auxiliary data, and coarse time indication.

Reporting phase or Detection Phase Suppose that a user i is tested positive for COVID19, then he will be instructed by the Health Authority (HA) to upload his key $SK_{i,x}$ to the backend server where x denotes the first day on which user i became infectious. After this, the user chooses a new daily key $SK_{i,y}$ depending on the day when this event occurs. As it is not mentioned by Troncoso et al., in [26] whether this key should be sent to the server but it is believed that this key should also be sent to the server due to the fact that user i might continue to be infectious.

Tracing phase
The tracing phase involves periodic broadcasts $SK_{i,x}$ from the server after user i has been confirmed to be positive. After receiving $SK_{i,x}$, another user j can recompute the ephemeral IDs for day x as follows: PRG(PRF($SK_{i,x}$, "broadcastkey")). In the same way user j can compute IDs for the remaining days as well. With EphIDs, user j can check whether any of the computed IDs appears in his local storage. Based on the related information like proximity, duration, auxiliary data and coarse time indication, he can take the measures needed.
In light of our evaluation framework, the solution is decentralized and proximity based. The analysis part done by Vaudenay in [14] discussed that there are 13 possible attacks on DP-3T, on which a detailed document as a reply to this analysis was uploaded by the DP-3T community. The community verified 1 attack among 13 as a potential attack which can also be mitigated. The Privacy level that the solution provides is L1, L2 and L3. But there are concerns regarding the adaption and the behaviour of the solution under varied situations. The white-paper of the solution mentioned "Several contact events" as a possible threat. We categorize the attacks possible in a separate section on attacks with their possible countermeasures. The analysis of Vaudenay [14] discussed that decentralization creates more threats than it seems to solve. It will be great to see how the solution works in practice and it's scalability will be tested as the number of users increases. Though, the reference implementation is given. It will be too early to evaluate it based on a reference implementation. With the app development, several hurdles are to be crossed when it comes to the design. The Solution however is the best available of all proposed solutions as of now.

5. Possible attacks on Contact Tracing Solutions and their Countermeasures

This section presents a taxonomy of possible attacks on contact tracing solutions as shown in Figure 2. Other than that, a discussion on the possible countermeasures is briefly discussed.

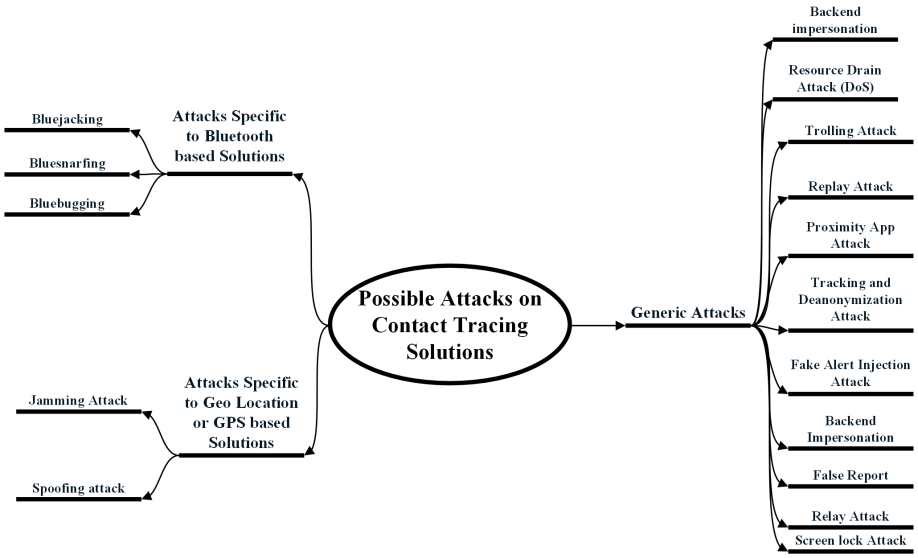

Figure 2: Possible Attacks on Contact Tracing Solutions

5.1. Generic Attacks

This section categorizes attacks based on their generality unlike those that are specific to a certain adoption of a technique like we will discuss in next sub-sections. However, there might be other possible attacks other than the one's we have discussed in this part. The attacks discussed below are the common and does not need any high technical setup.

5.1.1. Resource Drain Attack

Most contact tracing mechanisms face resource drain attacks leading to denial-of-service attacks in them. In a resource drain attack, an attacker sends a huge number of garbage messages from the device, forcing the other devices to drain the energy if the message is invalid or drain the energy and storage if the message is valid [27]. Such attacks do not affect the services provided by contact tracing mechanisms but lead to low performance of phones.

Countermeasures

Various Countermeasures include garbage message filtering, detection of attack and reporting to the phone user that will help to mitigate the attacks caused by resource drain attacks.

5.1.2. Trolling Attacks

In trolling attacks, an adversary spreads a fear of virus exposure by causing a sense of being in close proximity to the diagnosed people [28]. As a consequence, the non-affected people will conduct tests and waste the resources of diagnostic centers, leading to loss of trust in the contact tracing systems.

Countermeasures

The primary Countermeasure includes attack detection by health authorities. Further, a proper security mechanism is required to make sure that the attacker does not compromise a contact tracing application and thereby prevent the spread of false information about a person (trolling) or leaking personal information from such apps while connecting to other devices for contact tracing.

5.1.3. Replay Attacks

In a replay attack, the attacker uses one or two devices at different instances and advertises at the later time a message recorded at the earlier time [29]. In replay attack, the attacker advertises a proximity identifier derived from a diagnosis key before the victim observes the publication of this key[30]. If such attacks continue to happen, it will spread fear and anxiety among the people such that they will believe to have come in touch with the affected person, leading to loss of resources at diagnosis centers.

Countermeasures

The prime countermeasure is attack detection by health authorities.

5.1.4. Proximity App Attack

Any contact tracing application on a phone can leak proximity information about a person. A log of a user's proximity to other users could be used to show who they associate with and infer what they were doing [31]. Fear of disclosure of such proximity information might fear users from participating in expressive activity in public places.

Countermeasures

The application should not collect location information and time stamp information, and it should build time limits into their applications themselves, along with regular check-ins with the users as to whether they want to continue broadcasting.

5.1.5. Tracking and Deanonymization Attacks

Tracking and deanonymization attacks are intended to violate privacy leading to harmful impacts such as relying on false alert injections [32]. The attacker is interested in exposing the identity of a person, or several persons in a meeting, whose mobile device advertised messages including particular proximity identifiers. The privacy of the targeted person is violated if his diagnosis key is published.

Countermeasures

The mobile device varies the signal strength in a way that makes it difficult to determine with good accuracy the location of the device from the few samples that the attacker

may collect over a reasonably short period of time. The chances that an attacker will be forced to stalk the targeted person are more and so is his risk of getting discovered.

5.1.6. Screen Lock Attack or Ransomware

In this attack, hackers are using fake contact tracing apps to lock the android phones, therefore misusing the global pandemic to steal bank details, photos, videos and other private information [33]. For example, CovidLock changes the password of the phone and demands a ransom of $100 bitcoins for unlocking; otherwise it threatens to either permanently delete their data or leak their data to social media [34].

Countermeasures

Few countermeasures include installing anti-virus, never installing from a third party application store, never visiting any shady websites, etc.

5.1.7. Backend Impersonation

In backend impersonation, an attack is launched by an attacker device by masquerading as another device and misrepresenting its identity by changing its own identity. It can then advertise the incorrect information to other participating devices leading to the creation of loops in the information routing [35].

Countermeasures

Basic cyber-security mechanisms are required to prevent such attacks.

5.1.8. False Injection or False Report Attack

In this attack, an attacker injects false data and compromises the communication of information among smartphones [36]. False reports can be injected through compromised smartphones, thereby leading to low performance of any contact tracing applications. In COVID detection mechanisms, when an adversary compromises more phones and combines all the obtained secret keys, the adversary can freely forge the event reports.

Countermeasures

Effective filtering schemes such as interleaved hop-by-hop authentication, Statistical en-Route filtering, etc are required to mitigate the impacts of false data injection attacks[37] [38].

5.2. Attacks specific to Bluetooth based Solutions

Since mobile contact tracing leverages the fact that there are billions of devices that are in use today capable of Bluetooth based information exchange, but these devices are also exposed to a lot of security issues that are to be mitigated for better use of these solutions. We have discussed certain Bluetooth based attacks that can possibly be launched with little setup. Though Zeadally et al., in [8] has categorized and further discussed a full taxonomy of attacks on Bluetooth. For brevity, we discuss some attacks that we feel are common to this setting and then we briefly write about its possible countermeasures.

5.2.1. Bluejacking

In this type of attack, Bluetooth technology is exploited by sending unwelcomed messages to those devices that have Bluetooth enabled. The receiver has no knowledge of the sender. The contents it receives is the message along with the name and model of sender's phone. The messages sent does not do any harm to the user but are actually intended to cause the user to counter react in a particular manner or to add a new contact in his device's addressbook[39].

Countermeasures

This attack can be avoided by setting the devices in non-discoverable, hidden or invisible mode. Devices that are set in these modes are not susceptible to this type of attack[39].

5.2.2. Bluesnarfing

This type of attack allows unapproved access to a Bluetooth node. In this attack, the intruder hacks the node so as to access document files, contactbook etc. Here a attacker could even possibly call and forward messages to other devices as well[40].

Countermeasures

Devices that have discovery mode of their devices disabled can avoid this attack. By keeping the device in invisible mode and by leverging tools that restrict the connection of the device to known devices only.

5.2.3. Bluebugging

This attack is of most and serious concern. In this type of attack, the attacker gets unauthorized access to a device, thereby being capable of running commands or make phone calls etc. These result is major problems. This attack exploits a security flaw present in the firmware of some of the older Bluetooth devices (usually with those that are using Bluetooth Classic) in order to gain access to the attacked device [41].

Countermeasures

This type of attack can be avoided by switching off the radio (Bluetooth) capability while it is not being used. The attackers can only make connection when Bluetooth is enabled. The another important practice is to scan all the incoming messages (multimedia) for possible infections (viruses). The attackers usually gain access by transmitting this sort of information to it[42].

5.3. Attacks specific to Geo Location or GPS based Solutions

With the advancement in technologies, GPS (Global Positioning System) devices have become more affordable and with the result our lives are becoming increasingly dependent on precise positioning and timing. But there have been a lot of researchers that have proved that GPS is vulnerable to two main attacks viz., jamming and spoofing attacks. In this subsection, we investigate these attacks against GPS and their countermeasures [43].

5.3.1. Jamming Attacks

Jamming is the intentional or unintentional interference of the signal that prevents it from being received, which is relatively simple to do [44]. The aim is to overpower the extremely weak GPS signals so that they cannot be acquired and tracked anymore by the GPS receiver, and majority of GPS receivers do not implement any countermeasures against jamming.

Countermeasures

To countermeasure the jamming attack, we can use a notch filter or adaptive notch filters for GPS attack detection in contact tracing phones.

5.3.2. Spoofing Attacks

In GPS spoofing, an attacker uses radio signals located near the device to interfere with the GPS signals in such a way that it either transmits no data at all or transmits inaccurate coordinates; thereby making the location functionality of smartphones, used for contact tracing apps, vulnerable to spoofing attacks [45].

Countermeasures

Use of encrypted versions of the system in the defense sector, basic cyber-security principles to protect various digital threats in companies, machine learning and other analytics to detect any suspicious attacks, etc.

6. Conclusions

With growing demand for contact tracing solutions it is the need of the hour to have one general solution that takes all the aspects into consideration. From security and privacy aspects to legal and ethical aspects. Though the proposed solutions do not look at all aspects in general but rather focus most on one or the other. In order to frame a strategy to evaluate the solutions in a generic way, our proposed framework takes some important aspects into consideration so as to evaluate a contact tracing solution. Since the notions for evaluation we have used in our framework are generic in a sense that a lot more can be discussed under each section. We did not want to narrow down the scope where we would miss some aspects. Another important thing is that we did not tread in the direction of legal and ethical aspects because we feel once a contact tracing solution passes this assessment criteria, then and only then the legal and ethical aspects are to be taken into consideration. Another reason why we omit the discussion of these parts is due to the varying nature of societal norms for various countries. If a solution works for one country, it does not imply that it will work for other countries as well. We have framed the available solutions in a tabular form and then evaluated some of the proposed solutions in light of our framework. We also conclude that Open-Sourceness is an important parameter in keeping a solution transparent so as to avoid the misuse of a technology for surveillance, inserting backdoors or being used as a Trojan horse. The need of the hour suggests a general solution and its wide adoption i.e. standardization. DP-3T is a promising solution with regard to the support it has received from the scientific community and due to its transparency. Though the reference implementation

is available now, it is important to see how it behaves under a real scenario when the solution is adopted.

References

[1] L.-Y. Hsu, C.-C. Lee, J. A. Green, B. Ang, N. I. Paton, L. Lee, J. S. Villacian, P.-L. Lim, A. Earnest, and Y.-S. Leo, "Severe acute respiratory syndrome (sars) in singapore: clinical features of index patient and initial contacts," *Emerging infectious diseases*, vol. 9, no. 6, p. 713, 2003.

[2] "Report of clustering pneumonia of unknown etiology in wuhan city. wuhan municipal health commission, 2019." [Online]. Available: http://wjw.wuhan.gov.cn/front/web/showDetail/2019123108989

[3] R. Raskar, I. Schunemann, R. Barbar, K. Vilcans, J. Gray, P. Vepakomma, S. Kapa, A. Nuzzo, R. Gupta, A. Berke *et al.*, "Apps gone rogue: Maintaining personal privacy in an epidemic," *arXiv preprint arXiv:2003.08567*, 2020.

[4] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. Parker, D. Bonsall, and C. Fraser, "Quantifying sars-cov-2 transmission suggests epidemic control with digital contact tracing," *Science*, 2020.

[5] T. Altuwaiyan, M. Hadian, and X. Liang, "Epic: Efficient privacy-preserving contact tracing for infection detection," in *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–6.

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

[7] G. Kampf, D. Todt, S. Pfaender, and E. Steinmann, "Persistence of coronaviruses on inanimate surfaces and its inactivation with biocidal agents," *Journal of Hospital Infection*, 2020.

[8] S. Zeadally, F. Siddiqui, and Z. Baig, "25 years of bluetooth technology," *Future Internet*, vol. 11, no. 9, p. 194, 2019.

[9] "Security and privacy issues with gps tracking /navigation," accessed: 23-04-2020. [Online]. Available: https://cmu95752.wordpress.com/2011/12/14/security-and-privacy-issues-with-gps-tracking-navigation/$_ftn1$

[10] J. S. Warner and R. G. Johnston, "A simple demonstration that the global positioning system (gps) is vulnerable to spoofing," *Journal of security administration*, vol. 25, no. 2, pp. 19–27, 2002.

[11] "J. tidy, "coronavirus: Israel enables emergency spy powers," bbc news, march 2020." accessed: 23-04-2020. [Online]. Available: https://www:bbc:com/news/technology-51930681

[12] "M. j. kim and s. denyer, "a travel log of the times in south korea: Mapping the movements of coronavirus carriers ," the washington post, march 2020." accessed: 23-04-2020. [Online]. Available: https://www:washingtonpost:com/world/asiapacific/coronavirus-south-koreatracking-apps/2020/03/13/2bed568e-5fac-11eaac50-18701e14e06d story:html

[13] "Tracetogether," accessed: 23-04-2020. [Online]. Available: https://www.tracetogether.gov.sg/

[14] "S. vaudenay. analysis of dp3t." accessed: 23.04.2020. [Online]. Available: https://eprint.iacr.org/2020/399, 2020.

[15] Q. Tang, "Privacy-preserving contact tracing: current solutions and open questions," *arXiv preprint arXiv:2004.06818*, 2020.

[16] "Hamilton, isobel asher, "11 countries are now using people's phones to track the coronavirus pandemic, and it heralds a massive increase in surveillance," accessed: 26.03.2020. [Online]. Available: www.businessinsider.com/countries-tracking-citizensphones-coronavirus-2020-3?r=DEIR=

[17] H. Cho, D. Ippolito, and Y. W. Yu, "Contact tracing mobile apps for covid-19: Privacy considerations and related trade-offs," *arXiv preprint arXiv:2003.11511*, 2020.

[18] O. Goldreich, S. Micali, and A. Wigderson, "How to solve any protocol problem," in *Proc. of STOC*, 1987.

[19] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.

[20] L. Reichert, S. Brack, and B. Scheuermann, "Privacy-preserving contact tracing of covid-19 patients," 2020.

[21] S. Brack, L. Reichert, and B. Scheuermann, "Decentralized contact tracing using a dht and blind signatures," 2020.

[22] "Argenox technologies llc., "ble advertising primer"," accessed: 05.04.2020. [Online]. Available: www.argenox.com/library/bluetoothlow- energy/ble-advertising-primer

[23] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," Naval Research Lab Washington DC, Tech. Rep., 2004.

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

[25] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[26] "Decentralized privacy-preserving proximity tracing. version: 3rd april 2020. pepp-pt." accessed: 26.03.2020. [Online]. Available: https://github.com/DP-3T/documents

[27] M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*. IEEE, 2005, pp. 356–364.

[28] A. Gaus, "Trolling attacks and the need for new approaches to privacy torts," *USFL Rev.*, vol. 47, p. 353, 2012.

[29] Z. Feng, J. Ning, I. Broustis, K. Pelechrinis, S. V. Krishnamurthy, and M. Faloutsos, "Coping with packet replay attacks in wireless networks," in *2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*. IEEE, 2011, pp. 368–376.

[30] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Eidgenössische Technische Hochschule Zürich, Department of Computer Science, 2011.

[31] T. Halevi, D. Ma, N. Saxena, and T. Xiang, "Secure proximity detection for nfc devices based on ambient sensor data," in *European Symposium on Research in Computer Security*. Springer, 2012, pp. 379–396.

[32] J. Su, A. Shukla, S. Goel, and A. Narayanan, "De-anonymizing web browsing data with social networks," in *Proceedings of the 26th international conference on world wide web*, 2017, pp. 1261–1269.

[33] N. Andronio, S. Zanero, and F. Maggi, "Heldroid: Dissecting and detecting mobile ransomware," in *International Symposium on Recent Advances in Intrusion Detection*. Springer, 2015, pp. 382–404.

[34] "Coronavirus stimulus scams are here. how to identify these new online and text attacks," accessed: 23.04.2020. [Online]. Available: [12] https://www.cnet.com/how-to/coronavirus-stimulus-scams-are-here-how-to-identify-these-new-online-and-text-attacks/

[35] P. Wood, "Web application hacking: Exposing your backend," accessed: 23-04-2020. [Online]. Available: https://www.helpnetsecurity.com/2003/11/11/web-application-hacking-exposing-your-backend/

[36] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," in *Proceedings of the 3rd international conference on Embedded networked sensor systems*, 2005, pp. 294–295.

[37] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004*. IEEE, 2004, pp. 259–271.

[38] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 4, pp. 839–850, 2005.

[39] "Bluejacking technology: A review. int. j. trend res. dev. 2016, 3." accessed: 23-04-2020. [Online]. Available: $https://www.researchgate.net/publication/314233155_Bluejacking_Technology_A_Review?channel=doi&linkId=58bc1599a6fdcc2d14e574d1&showFulltext=true$

[40] S. S. Hassan, S. D. Bibon, M. S. Hossain, and M. Atiquzzaman, "Security threats in bluetooth technology," *Computers & Security*, vol. 74, pp. 308–322, 2018.

[41] J. Padgette, J. Bahr, M. Batra, M. Holtmann, R. Smithbey, L. Chen *et al.*, "Guide to bluetooth security (nist special publication 800-121 revision 2)," 2017.

[42] S. Dhuri, "Bluetooth attack and security," *Int. J. Curr. Trends Eng. Res*, vol. 3, pp. 76–81, 2017.

[43] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "Gps software attacks," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 450–461.

[44] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," *International Journal of Production Economics*, vol. 172, pp. 76–94, 2016.

[45] J. Warner and R. Johnston, "Gps spoofing countermeasures, homeland secur," *J*, vol. 25, no. 2, pp. 19–27, 2003.

[46] "Pan-european privacy-preserving proximity tracing," accessed: 23-04-2020. [Online]. Available: https://www.pepp-pt.org/

[47] "Private tracer," accessed: 23-04-2020. [Online]. Available: https://gitlab.com/PrivateTracer/coordination

[48] "Meet the stop corona," accessed: 23-04-2020. [Online]. Available: https://www.roteskreuz.at/site/meet-the-stopp-corona-app/

[49] "The private way of tracing contacts," accessed: 23-04-2020. [Online]. Available: https://www.novid20.org/en

[50] "How close were you and for how long - were you exposed? this is how the official corona app works, which may soon be on your phone as well," accessed: 23-04-2020. [Online]. Available: https://yle.fi/uutiset/3-11299573

[51] "Corona data donation," accessed: 23-04-2020. [Online]. Available: https://corona-datenspende.de/

[52] "Tracking app may assist iceland with coronavirus contact tracing," accessed: 23-04-2020. [Online]. Available: https://www.icelandreview.com/sci-tech/tracking-app-may-assist-iceland-with-coronavirus-contact-tracing/

[53] "Aarogya setu mobile app," accessed: 23-04-2020. [Online]. Available: https://www.mygov.in/aarogya-setu-app/

[54] "Coronavirus: Smartphone app to facilitate contact tracing to be rolled out, hse says," accessed: 23-04-2020. [Online]. Available: https://www.irishtimes.com/news/ireland/irish-news/coronavirus-smartphone-app-to-facilitate-contact-tracing-to-be-rolled-out-hse-says-1.4215036

[55] "Health ministry launches phone app to help prevent spread of coronavirus," accessed: 23-04-2020. [Online]. Available: https://www.timesofisrael.com/health-ministry-launches-phone-app-to-help-prevent-spread-of-coronavirus/

[56] "Rilevatore terremoto," accessed: 23-04-2020. [Online]. Available: https://web.archive.org/web/20200403104132/https://sismo.app/it/covid/

[57] "The fhi app will store info about your movements for 30 days," accessed: 23-04-2020. [Online]. Available: https://www.nrk.no/norge/fhi-app-skal-lagre-info-om-dine-bevegelser-i-30-dager-1.14963187

[58] "Wetrace," accessed: 23-04-2020. [Online]. Available: https://wetrace.ch/

[59] "Using a mobile app for contact tracing can stop the epidemic," accessed: 23-04-2020. [Online]. Available: https://045.medsci.ox.ac.uk/mobile-app

[60] "Reduce the spread of covid-19 without increasing the spread of surveillance." accessed: 23-04-2020. [Online]. Available: https://covid-watch.org/

[61] "Coepi," accessed: 23-04-2020. [Online]. Available: https://github.com/Co-Epi

[62] "open-coronavirus," accessed: 23-04-2020. [Online]. Available: https://github.com/open-coronavirus/open-coronavirus

[63] "Privacy-preserving cross-border contact tracing," accessed: 23-04-2020. [Online]. Available: https://bluetrace.io/

[64] "How south korea flattened the curve," accessed: 23-04-2020. [Online]. Available: https://www.nytimes.com/2020/03/23/world/asia/coronavirus-south-korea-flatten-curve.html

Appendix A. Summary of Available Contact Tracing Solutions

Table A.1: Summary of available Contact Tracing solutions

Available Solution	**Centralized/Decentralized**	**Type of Project**	**Type of Tracking**	**Status of the project/work**	**Medium of information sharing**
Decentralized Privacy Preserving Proximity Tracing (DP-3T) [26]	Decentralized	Public(Open-Source)	Proximity Tracking	Proposed with Reference implementation	Broadcasting
Pan European Privacy Preserving Proximity Tracing (PEPP-PT) [46]	Decentralized	Private	Proximity Tracing	Under Development	*
Netherlands: Private Tracer [47]	Decentralized	Public (Open Source)	Proximity Tracing	Under Development	*
Austria: "Stopp Corona" app [48]	Decentralized	Red Cross	Proximity Tracing	Developed and Published	Selective Broadcasting
Austria: NOVID20 [49]	Decentralized	Private (Open Source)	Location & Proximity Tracing	Developed	*
Finland: Ketju project [50]	Decentralized	Private & Public	Proximity Tracing	Under Development	Selective Broadcasting
Germany: "Corona-Datenspende" (Robert Koch Institut) [51]	Decentralized	Government	Data Tracking	Developed	Broadcasting
Iceland: Government app project [52]	Decentralized	Government	Data Tracking	*	*
India: Aarogya Setu mobile app [53]	Decentralized	Government	Proximity and Location Tracing	Developed	Selective Broadcasting
Ireland: HSE App [54]	Decentralized	Government	Proximity Tracing	Under Development	*
Israel: "Hamagen" app [55]	Decentralized	Government (Open Source)	Location Tracing	Developed	Unicasting
Italy: Rilevatore terremoto [56]	Decentralized	Government	Location Tracing	Developed	*
Norway: App by the Institute of Public Health [57]	Decentralized	Government	Location & Proximity Tracing	Developed	Selective Broadcasting
Singapore: "TraceTogether" app [13]	Decentralized	Government	Proximity Tracing	Developed	Broadcasting
Switzerland: "WeTrace" app [58]	Decentralized	Private (Open Source)	Proximity Tracing	Under development	Selective Broadcasting
United Kingdom: NHSX/University of Oxford tracking app [59]	Decentralized	Government	Proximity Tracing	Under Development	Selective Broadcasting
United States: Covid Watch (Stanford University) [60]	Decentralized	Public (Open Source)	Proximity Tracing	Under Development	Selective Broadcasting
United States: CoEpi [61]	Decentralized	Private (Open Source)	Proximity Tracing	Developed	Selective Broadcasting
Spain: "Open Coronavirus" app [62]	Decentralized	Private (Open Source)	Location and Proximity Tracing	Developed	*
Bluetrace [63]	Decentralized	Private	Proximity Tracing	Proposed with Reference implementation	Selective Broadcasting
CAUDHT [21]	Decentralized	Private	Proximity Tracing	Proposed	Selective Broadcasting
South Korea: Multi-Source Contact Tracing[64]	Centralized	Government	Security Footage, GPS data	In practice	Broadcasting
Assessing Disease Exposure Risk with Location Data: A Proposal for Cryptographic Preservation of Privacy [24]	Centralized	Private	Location Tracing	Proposed	Selective Broadcasting

* Not Enough information