A Study on Contact Tracing Apps for Covid-19: Privacy and Security Perspective

Auwal Shehu Ali
School of Computer Sciences, Universiti Sains Malaysia, Malaysia.
Department of Computer Sciences, Faculty of Computer Science and Information Technology, Bayero University Kano, PMB Kano Nigeria, Nigeria.
E-mail: asali.cs@buk.edu.ng

Zarul Fitri Zaaba*
Senior Lecturer, School of Computer Sciences, Universiti Sains Malaysia, Pulau Pinang Malaysia, Malaysia.
E-mail: zarulfitri@usm.my

Received December 24, 2020; Accepted March 05, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V18I1/WEB18093

Abstract

To support the manual contact tracing methods of Covid-19, countries and big companies like Apple and Google are busy developing several contact tracing applications. The purpose of digital contact tracing apps is to accelerate existing traditional face to face interview method which can control the pandemic effectively and rapidly. A major concern is whether consumers will be willing to download, install, and use the contact tracing applications because of the debate it created about its main attribute like security, privacy concern, system framework, data processing, location measurement. In this paper we discuss the contact tracing apps and its different architecture, then we analyze the framework in term of security, privacy concern and privacy policy. We reported 47 contact tracing applications which are from 28 countries worldwide, with several others expected to be roll out later. We found that 23 percent of contact tracing apps currently implemented do not provide privacy policy in their documentation. We believe that these comprehensive evaluation and specific suggestions will lead to creation and implementation of solutions towards Covid-19 and support governments and mobile development industries in creating safe and privacy conserving apps for contact tracing solutions.

Keywords

Privacy, Security, Contact Tracing Apps, Covid-19, Privacy Policy.

Introduction

Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2) known as COVID-19, has recently shocked the world, when the virus started to spread worldwide. On 30th January 2020 WHO (World Health Organization) declare COVID-19 to be a public health emergency of international concern (PHEIC) (Mozur, Zhong, & Krolik, 2020; O'Neill, Ryan-Mosley, & Johnson, 2020), pushing government to enforce lockdowns, changing the lifestyle of people all over the world, promote self-isolation, specify work – from – home measures, develop stringent social distancing requirements, deploy emergency health responses, providing significant new facilities for both the management and mass testing of the general public and straining global healthcare systems (Ahmed et al., 2020). All of these approaches were aim to decrease the speed of coronavirus spread and contribute to the so called 'curve attenuation' until an approved vaccine/procedure has been authorized (O'Neill et al., 2020). Many tracking applications were developed through a fast-tracked development process, mostly paid for with public money, with very minimal socio-economic impact evaluation and respect for fundamental rights and values such as fairness and inclusion (Vinuesa, Theodorou, Battaglini, & Dignum, 2020). Therefore, it is critical to analyze carefully the actual utility, importance and efficacy of both the applications, as well as their effects on the wider social system, including our constitutional rights and freedoms, considering that such applications established a standard for the usage of similar intrusive technology, even after the COVID-19 crisis.

The rest of this paper is structured in the following way. In section two, we give an overview, architecture, and classifications of the contact tracing applications. In section three we discuss the security, privacy and most common attacks and vulnerabilities that could affect contact tracing applications and discuss most widely contact tracing app developed by different countries. In section four we give the general discussion of the paper. Finally, we conclude the paper with some recommendation in section five.

Contact Tracing Application

Contact tracing applications are used to decide when a person has meet people infected with COVID-19. If that happens, the application alert the user, as well as public health authority in some cases, and offers advice or guidance (Kind, 2020). According to Centre for Disease Control and Prevention (CDCP), contact tracing will help ensure the safe, sustainable, and effective quarantine of contacts to prevent additional transmission. The automatic contact tracing protocols operate over the Bluetooth Low Energy (BLE) and a short-range wireless communication system. Instead of using centralized location monitoring system, they detect

proximity between two smartphones, thereby protecting individual's privacy toward unwanted invasion into their location history (Park, Choi, & Ko, 2020).

Architecture of Contact Tracing Apps

Due to several security and privacy issues, the type of architecture implemented for the data collection components of contact tracing apps has become a topic of much debate. We would address 3 different system architectures that are widely used or introduced in building apps for COVID-19 contact tracing apps (T. Li et al., 2020). These are the centralized, decentralized, and hybrid approach which incorporates elements of both centralized and decentralized architecture. The requirements for classification include how the system is being used, and what data it needs (or stores). We are now discussing each one of the 3 architectures outlining their unique characteristics. We will be addressing some different specific contact tracing applications which use each of the three architectures (Meadows, 1986).

- **Centralized Contact Tracing App Architecture**.

This architecture is based on the Bluetrace mechanism (Bay et al., 2020) as shown in figure 1. The app's first prerequisite would be that a person must register first with the central database. For each machine, the database will create a (TempID) temporary ID that will maintains privacy. This TempID is being coded and forward to the device using a secret code (classified only by the centralized database authority). Devices share this TempID once they come in close range (in Bluetooth interaction signals). When a user result return positive, they will voluntarily send to the central database all their recorded contact messages (Maurer, 2005). Within such messages, the database map the TempID to individuals to identify those persons at risk. The database controller plays a very important role in executing core functionalities in the centralized architecture, like keeping encrypted personally identifiable information, creating anonymized TempID, risk assessment, as well as alerting for close contact (Ahmed et al., 2020). Such aggregation of obligations poses concern about privacy (Levy & Stewart, 2020), while the database are believed to be reliable for this framework, with several countries adopting stringent privacy protection legislation to ensure the usage and life cycle of the data collected (Watts, 2020).

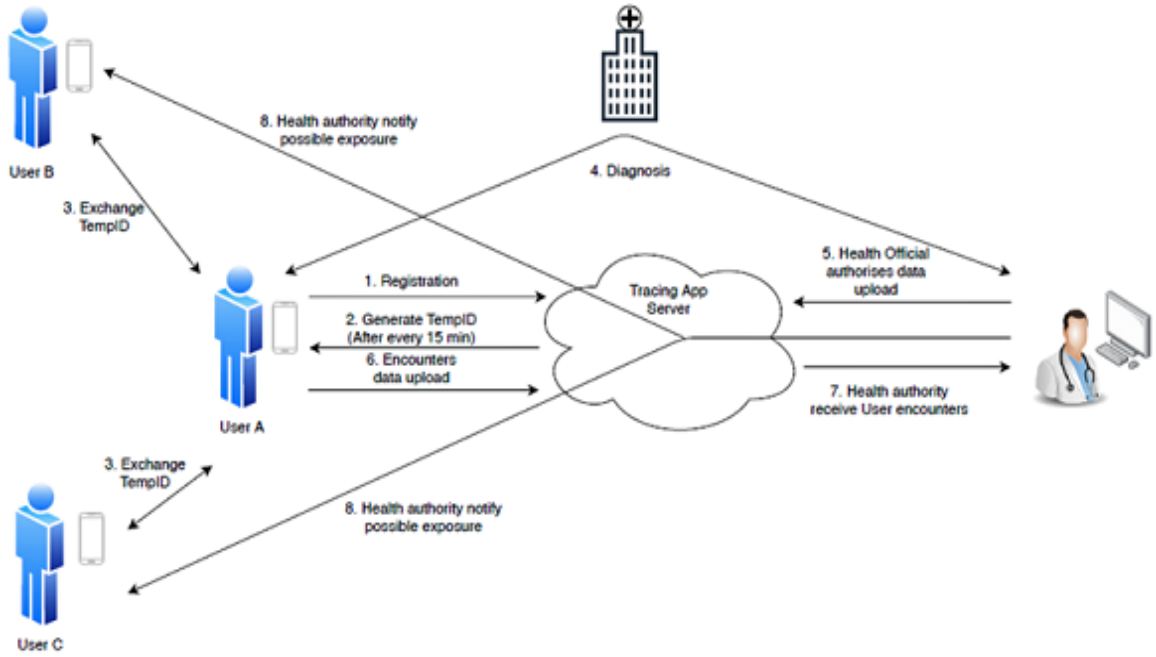

Figure 1 Architecture of Centralised Contact Tracing App (Ahmed et al., 2020)

- **Decentralized Contact Tracing App Architecture**

Unlike centralized architecture, decentralized framework does not require users of the app to pre-register before they can use the app, thereby preventing any personally identifiable information being stored within the database. Decentralized architecture suggests moving core features into consumer devices as shown in figure 2, leaving the database with limited role in the development of contact tracing . Devices produce their random seeds (used as inputs for the pseudorandom function), which are utilized in conjunction with the actual time to produce privacy-conserving pseudonyms or 'chirps' with a limited lifespan of approximately one minute. The intention is to strengthen user privacy by creating secret identities for consumer devices (leaving actual user identities hidden from all other consumers and the database) and executing exposure notifications onto specific devices rather than the centralized database (Zhao, Wen, Lin, Xuan, & Shroff, 2020).

A Private Automated Contact Tracing protocol (PACT) is use as a base to explain decentralized framework (Rivest et al., 2020). Eventually, these chirps are regularly exchanged with many other devices which came in close contact. When a user has been positively identified with Covid-19, they will volunteer to send their seeds to a central repository with associated time information. This compares with the centralized system that uploads the entire list of interaction messages. Rather than all chirps, uploading seeds reduces latency and increases the usage of bandwidth (Ahmed et al., 2020).

The database controller only serves as a meeting spot, similar to a newsletter board advertising the infected user seeds. Such database is referred to as 'honest but curious.' Many users of the app can be able to download such seeds to recreate the chirps (using timestamps) sent by users who were infected . Both the database and other users cannot obtain any identity information merely from recognizing the seeds and chirps. Just the other users of the app can do a risk assessment to verify whether they are exposed for a sufficiently long period of time. This method of downloading seeds through a one-way lookup limits the flexibility of the database and mitigates most of the privacy threats.

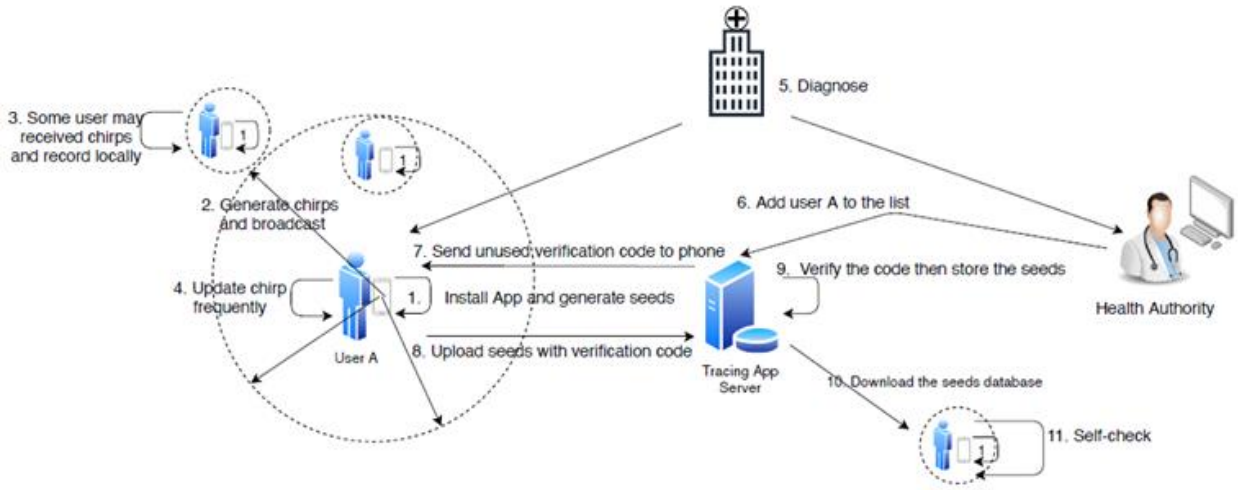

Figure 2 Architecture of Decentralized Contact Tracing App (Ahmed et al., 2020)

- **Hybrid Contact Tracing App Architecture**

The database handles all the difficult operations in the centralized framework, e.g. TempID analyses, encoding, decoding, risk assessment, and at-risk contact alert notifications. From the other hand, both features are assigned to individual devices in the decentralized framework, maintaining the database for lookup needs and as a notice board. The hybrid framework as shown in figure 3, implies separating certain features between the database and the devices. Most especially, the creation and management of TempID remains decentralized (i.e. controlled by devices) to guarantee privacy and anonymity, while the database controller will be responsible for risk assessment and notifications. According to (Castelluccia et al., 2020) there are 3 key reasons why tracing operation undertake at database point; 1) the database is ignorant of the number of at-risk users in decentralized approach as the devices conduct this risk assessment without looping the database. Therefore, the database has no statistical knowledge and cannot perform any data analytics to classify clusters of exposure. 2) Risk assessment and alerting are regarded as critical mechanism which should be managed by authorities, considering the available

infrastructure components and the pandemic status. 3) Uploaded interaction details from infected users will not be made public to other users but it will only be kept on the database. It is to prevent potential threats on user de-anonymization in the decentralized framework.

The hybrid approach contact series is based on Desire protocol (Bielova et al., 2020; Castelluccia et al., 2020). This protocol ensures that the registration procedure for the user's application assign a unique identifier for the device with no Personally identifiable information recording (Felt et al., 2012). Devices create and share Ephemeral IDs cryptographically with many other devices via BLE. Two un-linkable Private Encounter Tokens (PETs) were created by each to obtained EphID and retained to reflect an experience. A collection of the locally created Private Encounter Tokens is submitted to the database once a user is confirmed positive. Any device now can submit its 2nd created Private Encounter Tokens to database which then carries out risk assessment and alert . The database cannot deduce any Private Encounter Tokens identifiable details, and all database and device communication is transferred via a proxy or anonymization network (Boutet et al., 2020).

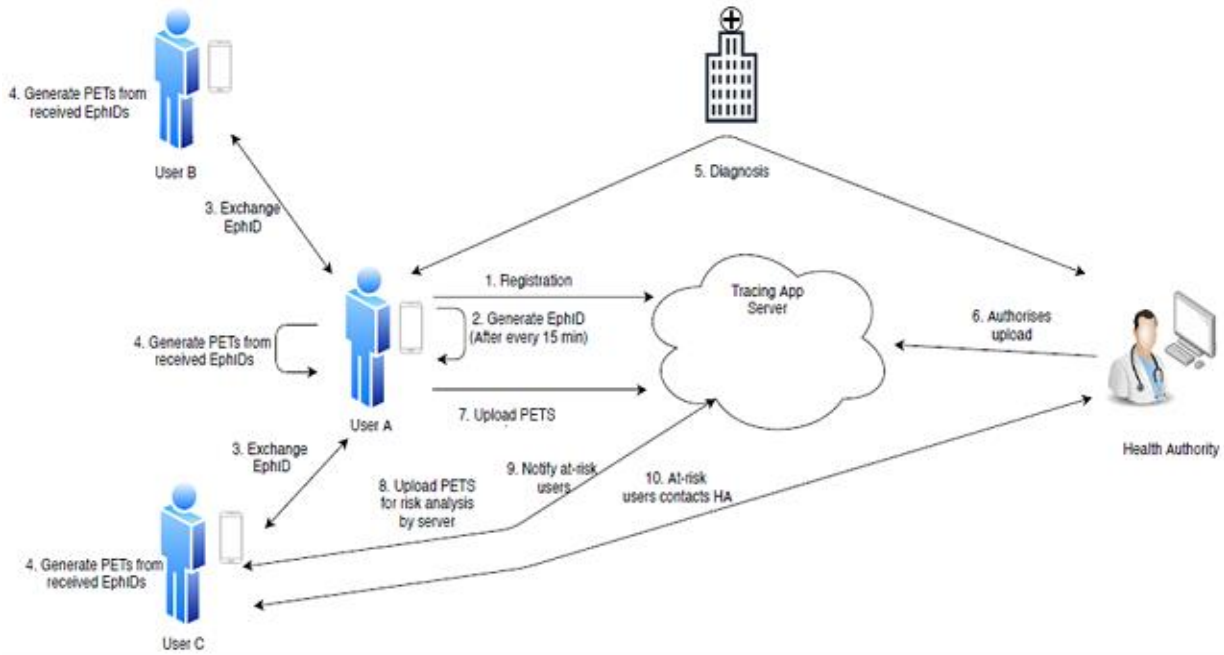

Figure 3 Architecture of Hybrid Contact Tracing App (Ahmed et al., 2020)

Privacy and Security Assessment of Contact Tracing Apps

Innovations can alert people quickly when they have been in contact with anyone infected with Covid-19, which are part of a plan to contain the pandemic. At least there are 47 contact-tracing applications presently released worldwide, which already been used in some

countries like for example, China, India, Australia, South Korea, and Singapore (Woodhams, 2020). While several other governments are evaluating or considering them. Such automated initiatives are coming at a price. The gathering of sensitive personal information could threaten anonymity, fairness, and justice (Zhou et al., 2013). However, though COVID-19 applications are temporary measure, rapidly rolling out tracking applications is running the risk of producing permanent, sensitive records of people's health, activities, and social gathering that they have no influence over. Further legal transparency is imperative. These issues have so far mainly focused on personal privacy (Troncoso et al., 2020). Many governments also agreed to data privacy and security (Guillo, 2020). Nevertheless, certain social and ethical factors in the attempt to thwart the outbreak should not be set aside (Danz et al., 2020).

For example, contact-tracing applications must be flexible and accessible to everyone, regardless of the technology or perhaps the degree of digital literacy they need. However, a lot of applications function only with some certain devices. For instance, Australia will have no plans to develop its application that will work on any device uses operating system older than Apple's iOS 10 or Android 6.0. About one-fifth of adults in the UK do not use a smartphone, and thus may be exempted from a mobile contact-tracing project. Trying to roll out an application before taking its broad ethical and legal ramifications into account can be risky, expensive, and pointless. For instance, Bluetooth signals indicating the proximity of the cell phones of two persons are not a definite indication of the risk of infection — two persons may be in the same area yet physically separated, for instance, by a fence. A high degree of false - positive by such an application (because of self-reporting, for example) may result in unjustified anxiety. And inadequate safeguards toward false negatives (people who do not report being unwell using the application) may cause a negative sense of safety towards others and maximize the risk of infection (Chowdhury, Ferdous, Biswas, Chowdhury, & Muthukkumarasamy, 2020).

People will reject applications that violate privacy, equality, and justice principles. This would infuriate the initiatives and waste the capitals committed in the production and implementation of such software. Lack of concern in privacy (Ali, Zaaba, Singh, & Hussain, 2020), security and ethics could weaken confidence in government and public health services — as happened in the Norwegian Data Protection Authority when they accused the Norwegian Institute of Public Health of failing to perform a thorough risk analysis of its Smittestopp, a contact tracing application.

Privacy

The performance of contact tracing application heavenly rely on many factors such as: how secure and private their data are. Another factor in using the application is how quickly and reliably it can identify near contacts. According to (Rivest et al., 2020) A naive method for contact tracing may be to create a privacy-agnostic program which displays and shares the contact information of the individuals and regularly reports their locations with a centralized database. Such an app would pose significant questions about privacy, and the users would probably not embrace it. And all the frameworks provide built-in privacy and security. Since privacy is the core of the approaches to contact tracing (Alsdurf et al., 2020).

The 1st step in developing contact tracing technologies is to protect privacy. Personal privacy was not an issue in many of the recommendations for contact tracing. Many countries have also embraced the concept of government surveillance to monitor individuals in the context of contact tracing (Hamilton, 2020). The data to be processed is divided into 3 groups: 1) Personally Identifiable Information of individuals (e.g., name, mobile ID, status of users checked, and so forth.) 2) User advertising notifications (pseudonyms shared among phones) 3) Social / similarity map, an indicator of connection among people who came in frequent proximity with each other. Each type of information may have different consequences for privacy. According to (Cho, Ippolito, & Yu, 2020).

While there is no specific definition of privacy which can assure the privacy and security requirements in a contact tracing apps, solution requires with confidence, we should seek to develop those concepts of privacy in addition to making privacy protection a good issue in reality. To this end, we apply the ideas used by (Cho et al., 2020) since these notions tend to always be a common to every techniques and applicable to development of methods for contact tracing (Spensky et al., 2016). Here in their proposed model, they classified privacy notion of contact tracing apps into three level: i) first level embraces the very first notion i.e. snooper's privacy. ii) The level of privacy notion is a privacy of users. iii) And the third level which is the privacy from authorities (Utz et al., 2020).

We discuss the consequences of privacy first from the mobile viewpoint, which is usually least protected than a database. Throughout this situation, threats such as stealing or intimidation (an individual is compelled or convinced) would lead in exposure of the information stored on the device. Some of this danger exists in all the frameworks. But what is contained on devices is the significant difference between the average frameworks as shown in Table 1.

Table 1 Summary of Contact Tracing App Architecture for Data Storage

Architecture	Storage	Stage of Registration	Stage of Operation	Positive case identification phase
Centralized	Server	Name, Mobile Number, Zip Code, Age range	Generate and stores TempIDs for each user	List and contact details of all 1) positive cases 2) close contacts of each positive case
	Devices	--	Own TempID and Smartphone model Encounter messages received from contacts (TempIDs of contacts, time stamp, RSSI TxPower, Phone model)	--
Decentralized	Server	--		Seeds (and validity period) received from all positive cases
	Devices		Generate own seeds and chirps Chirps received from contacts, time stamp, RSSI	Seeds for all positive cases received from the server Generates chirps based on seeds/validity period of positive cases
Hybrid	Server	Device ID	Device ID	Stores PETs (and validity period) received from all positive cases Stores metadata about positive cases Store query PETs from other users
	Devices	Device ID, Encryption key	Generate and store own EphID Maintain two tables of PETs Stores timestamp, duration, and signal strength for PETs	--

Security

Even though, the level of security offered differs heavily on the types of attack, the assumptions of confidence and the safeguards they provide (AISEC, 2020). The concept of security includes reducing the capabilities of an attacker to launch (false positives and false negatives) into the system, as well as guaranteeing system availability and integrity. The purpose for an intrusion according to (Ahmed et al., 2020) is differs and therefore can vary from political, religious, to monetary. An intruder can attempt to inflict incorrect entries in the sense of contact tracing or trigger a denial-of-service conditions.

Because all the 3 frameworks mentioned above include a centralized database, the different security vulnerability to each framework will be explore. The possible security vulnerability rely on what data is being collected and processed from a database, what data is being exchanged and available to a database and under what format (e.g., pseudonymous, encrypted, unencrypted). This also relies mostly on server's method of operation, notably whether it will be 1) trustworthy server, 2) an honest yet suspicious server, 3) a compromised / misleading server, or 4) a colluding server. In all the frameworks, a suspicious / hacked server can obstruct all forms of communication or inflict fake exposure alerts. Likewise, a collaborating server can collaborate with many other malicious entities to de-anonymize users.

Centralized Security Architecture

The server is deemed trusted in the centralized architecture. This is ideal for keeping Personally identifiable information of user and administering encryption keys that are used for encryption / decryption of TempIDs. If the database gets hacked, this raises the possibility of security breaches, a common concern to any centralized system. The server program must execute in a secure environment in this case and use acceptable encryption with access control mechanisms.

Every data transferred between the database and the device of the person or between database and the healthcare officers must be approved and protected. Therefore, centralized frameworks only include malicious activity in their threat designs and seek to maintain every users' data secured so that it can avoid the destruction of privacy of users as stated in It means no unauthorized 3rd party can obtain any data that is being sent / received or exfiltrated. Nonetheless, unauthorized attacker in centralized environments may compromise the unsecured BLE contact details shared among devices through conveying or replaying wrong contact details. Such types of threat will contribute to false positives causing users to be wrongly informed as near contacts mostly during contact tracing phase.

Decentralized Security Architecture

From the other end, decentralized and hybrid framework presume an honest yet suspicious server which executes most of the work allocated to and collects confidential data indirectly, where possible. The method of intrusion regards the government as well as the database as dishonest and only exposes the details of the user to just the health officials. The main user worry, as previously stated, is about government using information for the reasons other than contact tracing apps. Hence, such frameworks are intended to mask user IDs and create encrypted device IDs, thereby eliminating the system capabilities to relate IDs to user details.

The decentralized framework assigns information management to a device of individuals, making the whole system more resilient against a specific fault / attack, including the remote database. Nevertheless, a moderately functional central database also needs the decentralized approach. This would also be prone to a much smaller proportion of server-based threats. Untraceable IDs were submitted to the database in decentralized systems, which will then be possibly available to interact with by other devices. Yet a sincere-but curious database would not fail to understand any Personally Identifiable Information, connect the secret IDs or create social graphs until it has links to certain side channel information.

There is going to be a little effect in the event of a security incident because the perpetrators can only access the seeds / tokens of compromised individuals, which are available. At some point, an unauthorized attacker can also trigger false positives by conveying the chirps then launching DoS attacks by transmitting fraudulent, but properly formatted, ads.

Hybrid Security Architecture

At the database point, the hybrid approach performs a communication risk assessment and verification processes. This is to avoids any threats of re-identification / de-anonymization, Furthermore, the hybrid approach offers various techniques to mask the individual's IDs from the server thereby allowing centralized communication matching. This suggests the creation of abstract IDs at the computers, related to the decentralized frameworks. The justification is that computers maintain complete ownership of their hidden keys, rendering them less vulnerable to database violations.

Table 2 Summary of COVID-19 Contact Tracing Apps Currently Developed and Implemented by Many Countries

Name of App	Number of Download	Operating System	Framework	Privacy Policy	Technology
COVIDS safe	500K+	Android/iOS	Decentralized	Yes	Bluetooth
Stop p Corona	100K+	Android/iOS	Decentralized	Yes	Bluetooth
Bahrain	100K+	Android/iOS	Centralized	No	Bluetooth, GPS
Viru Safe	10K+	Android/iOS	Centralized	Yes	Bluetooth
ABTrace Together	10K+	Android/iOS	Decentralized	Yes	Data
Detector	NULL	Alipay, QQ, WeChat	Centralized	N/A	Bluetooth, GPS
Cov Tracer	500+	Android	Centralized	Yes	GPS
Mapy.cz	1M+	Android/iOS	Centralized	Yes	GPS
eFacemask	100K+	Android	Decentralized	Yes	Bluetooth, GPS
Tracker App	NULL	Android/iOS	Unknown	No	Bluetooth, GPS
Rakning C-19	50K+	Android/iOS	Decentralized	Yes	GPS
Track & Trace	50+	Android	Centralized	Yes	Bluetooth, GPS
Aarogya Setu	50M+	Android/iOS	Centralized	Yes	Bluetooth, GPS
COVID CARE	1K+	Android	N/A	No	GPS
Covid Locator	10K+	Android	N/A	No	GPS
Corona Watch	100K+	Android	Centralized	Yes	GPS
Maha Kavac	10K+	Android	Centralized	Yes	GPS
COVID-19 Odisha	1K+	Android	N/A	No	Bluetooth, GPS
SMC COVID-19 Tracker	50K+	Android	Centralized	No	GPS
COVID-19 Quarantine Monitor Tamil Nadu	100K+	Android	N/A	No	GPS
UP Self-Quarantine App	10K+	Android	N/A	No	GPS
Uttarakhand CV 19 Tracking System	5K+	Android	Centralized	Yes	GPS
Peduli Lindungi (Care Protect)	1M+	Android	Decentralized	No	Bluetooth, GPS
The Shield	1M+	Android/iOS	Decentralized	Yes	GPS

Track Virus	100K+	Android/iOS	Decentralized	No	Bluetooth, GPS
SM Covid19	10K+	Android	Centralized	Yes	Bluetooth, GPS
Stop COVID-19 KG	10K+	Android	Centralized	Yes	GPS
Plan Jalisco Covid-19	5K+	Android/iOS	Centralized	Yes	GPS
StopKorona!	10K+	Android/iOS	Decentralized	Yes	Bluetooth
Smittestopp (Infection Stop)	100K+	Android/iOS	Centralized	Yes	Bluetooth, GPS
WeTrace	5K+	Android/iOS	Decentralized	No	GPS
Home Quarentine (Kwarantanna domowa)	100K+	Android/iOS	N/A	Yes	GPS
ProteGo Safe	1K+	Android	Decentralized	Yes	Bluetooth
TraceTogether	500K+	Android/iOS	Centralized	Yes	Bluetooth
Contact Tracer	5+	Android	Centralized	Yes	GPS
Zostan Zdravy	100K+	Android	N/A	Yes	GPS
Corona100m	1M+	Android	N/A	No	GPS
Shincheonji Location Notification	100K+	Android/iOS	N/A	Yes	GPS
COVID-19.eus	50K+	Android/iOS	Centralized	Yes	Geo-Data Submitted by User
MorChana	50K+	Android/iOS	N/A	No	Bluetooth, GPS
SafePaths	10K+	Android/iOS	Decentralized	No	GPS
Contact Tracer	10K+	Android	N/A	Yes	Bluetooth, GPS
HEALTHLYNKED COVID-19 Tracker	5K+	Android/iOS	N/A	Yes	GPS
Contact Tracing	50K+	Android/iOS	Centralized	Yes	Bluetooth, GPS
Care19	10K+	Android/iOS	Centralized	Yes	GPS
Action at Home	10K+	Android/iOS	Centralized	Yes	GPS
NHS Covid-19	5K+	Android	Centralized	Yes	Bluetooth

Discussion

After studying various contact tracing apps architecture particularly in term of their security and privacy, we assume that perhaps the issue at this point is little complex. There is indeed a race to formulate new innovative technologies by researchers and for the developers to

lunch new applications, almost every day. Such initiatives may help in tackling the pandemic, at least by raising awareness and support to begin conversations. Fortunately, several approaches are mainly focus on theories that are impractical and impede their efficacy and widespread adoption. We first discuss our key findings in this section, mainly based on the review in section 3, and then offer a proposal that envisage an interdisciplinary future research.

The first key observation is that many of the approaches only highlighted the privacy and security issues in contact tracing apps while not looking at the aspect of authenticity (elaborated in section 3.1). This means that a particular application user can probably fake location information for himself as well as for anyone. Subsequently, contact tracing app data could have been largely exploited, allowing fraudulent users and advisories to compromise the system and execute different fraud operations. Another significant observation is that the lack of authenticity, as shown by Vaudenay (2020), may also contribute to the violation of privacy. The major challenge in developing a privacy preserving and efficient contact tracing system is how to reconcile authenticity and privacy.

The second key observation is that several approaches centered only on the personal contact situation and pay less concern to the quality of location information and accuracy proximity measurement precision (for instance, those relying on the intensity of the Bluetooth sensor). Furthermore, it has not taken into consideration a variety of extraordinary circumstances. For example, an affected and quarantined victim's neighbors may be very similar in proximity and labelled as high risk, when the fact is that they are in separate apartments or homes such that the risk of infection is minimal. Incorrect measurement of distance and misleading risk warnings can trigger needless population fear and consume a lot of resources to resolve the false suspects in the public health system. In addition, many of the time, the situation of indirect contact was overlooked. Since Covid-19 can also be transmitted by means of indirect communication. Disregarding this situation makes current solutions for contact tracing less realistic and functional than anticipated.

The third key finding is that in current approaches, the context of contact tracing is quite small. Its more about a person assessing his risk of being infected depending on his contact record with the infected persons. Nevertheless, contact tracing is intended to allow health authorities and medical staff not to only analyze the disease at the global scale, but to also assist the person at the individual level. This poses an open question about how the medical team and health authority can gather and conduct their usual duties with the appropriate details. In order to satisfy the goals of robust contact tracing apps, new privacy preserving technologies must eventually be planned and introduced, thus minimizing the disclosure of

information. One core issue confronting both current and new approaches, is that there is no evidence about the relationship of confidence between the various players in the context of contact tracing. More potential issues can occur when an application is deployed.

The final observation is that not all the technical specifics have been presented by most theoretical solutions to promote an adoption. An untrusted database is needed in many solutions. In practice, it is unclear how this database is selected and how to enable it to function in the same way as what has been specified. In addition, to conduct certain cryptographic operations, a health authority is often involved and needed. In certain nations, this may be impossible condition for governmental authority. This will not be achieved in a short span of time.

Our study from table 2 show that currently, there are forty-seven contact tracing applications available worldwide (Woodhams, 2020), India's Aarogya Setu app is the most common with more than 50m downloads, 53 percent use GPS technology, 15 percent use Bluetooth technology and 28 percent use the combination of GPS and Bluetooth technology, twenty-four applications (51 percent) contain Google and Facebook tracking, eleven applications (23 percent) do not provide a privacy policy, twenty-five applications (53 percent) do not reveal how long they can retain users' data. Twenty-eight applications (60 percent) do not provide publicly reported confidentiality mechanisms (Woodhams, 2020).

In addition to that, we can see that from table 1 the study shows that data storage through different stages of centralized, decentralized and hybrid architecture has been review. In the operation stage, the centralized tracing framework stores user identities (like name, phone number, age, zip code) on the server side, but do not store the information on user’s device, in the case of decentralized, neither server nor user device store anything during the registration, in the hybrid architecture, both the server and user device store device ID with addition of encryption key from the user device . In the operation stage, centralized architecture generates and store a TempID for each user at a server side, while the user device has TempID and phone model, time stamp and RSSI. In decentralized operation stage, a user device will generate its own seeds and chirps but no operation for server at this stage. In hybrid architecture, the server will have the device ID while the user device will generate and store own EphID, store timestamp, duration, and signal strength for PETs. On handling positive cases identification, centralized architecture keeps list and details of all positive cases, also close contacts of each positive case in server side only. In decentralized architecture, the server receives the seeds with valid time from all positive cases, while at user’s device seeds for all the positive cases will receive from server. Finally, hybrid

architecture, the server generates chirps based on seeds with validity period of all the positive cases, it stores metadata about all positive cases and store query PETs from other users.

There is no technological solution that will ensure privacy is complete. Exploration and supervision would be essential for probable weaknesses to be realistically assessed. Certain applications installed on a phone, for instance, might attempt to listen to a tracking app then transmit the information to a 3rd party, or someone might infer who infected them to a virus because they had limited external communication and made notes to identify different access points. our expectation is that an app would be built with less privacy vulnerabilities than conventional manual touch monitoring and more security and privacy than GPS location-based monitoring, allowing users to opt-in depending on a reasonable knowledge of the consequences.

It is really important that technology will protects privacy, so that users will be safe against unnecessary data gathering and possible agency damages, especially in the foreseeable future. Privacy regulations which include complete voluntary adoption, comprehensive information security, de-identification, verifiable preservation, and many more are needed to depend society and encourage trustworthy acceptance. When government policies are set in force for citizen monitoring, rolling back such steps is hard. Therefore, a great deal of consideration must be made to ensure that data gathering is comparable, completely justified and it has a fixed end gate with all use is opt-in, without any repercussions if the new application is not used (Gostin, Hodge, & Wiley, 2020).

Traditionally, physical contact tracing approaches already have concerns with privacy due to the lack of sensitive data protection, which has caused serious damage mostly to vulnerable people. There has been a serious concern that a massive scale mobile contact tracing technology can inflict equal damage. Nonetheless, despite going through this process, we assume a friendly framework with strong protection and straightforward privacy, and effective data processing will allow smart testing to be implemented efficiently.

Conclusion

Technology design decisions must be informed through privacy-by-design and availability tools and characterized by non - expert steps to counter digital exclusion. Technological steps may include the preservation of individual privacy by decentralized privacy-conserving digital contact tracking, and the privacy-conserving protocols should underline this, also the security of the application should be usable to non-technical expert, since it is

expected that many individuals will use the contact tracing app in future. There is need for government and developers to see the possibility of making sure that privacy policies are put in place, which can reduce the concern users have in using the contact tracing apps.

Analyze and project the threats to privacy and security, this will need to explain the confidence and relationships between the members and lead to a set of safety criteria that a solution can fulfill. The responsibility and liability arrangement among the players should be reflected. Different consideration between privacy, effectiveness, utility, and other elements could be unavoidable. The rapid implementation of technological solutions without reliable evidence backing and impartial scrutiny that weaken public confidence and hinder the efficacy of the innovations in helping disaster preparedness. Good technological approaches need to be focused on reliable data on the health. Technology companies and programmers will interact extensively alongside professionals in healthcare during development and implementation of the system.

The amount of contact tracing applications available across the globe has seen a significant increase in the past few months. The applications are intended to help counter the virus spread through tracking people as well as those with whom they interacted. When a person is infected with the disease, all the individuals who have been in interaction with him lately will be told and, in certain instances, will be required to self-quarantine. We argue that implementing a weak framework will open substantial opportunities for systematic abuse and not adequately prevent work from creeping or building the confidence which is key to widespread acceptance, protection, and reputation. We believe that these comprehensive evaluation and specific suggestions will lead to creation and implementation of solutions towards Covid-19 and support governments and mobile development industries in creating safe and privacy-conserving apps for contact tracing solutions.

References

Ahmed, N., Michelin, R.A., Xue, W., Ruj, S., Malaney, R., Kanhere, S.S., & Jha, S.K. (2020). A survey of covid-19 contact tracing apps. *IEEE Access*, *8*, 134577-134601.

AISEC, F. (2020). Pandemic Contact Tracing Apps: DP-3T, PEPP-PT NTK, and ROBERT from a Privacy Perspective. *IACR Cryptol. ePrint Arch.*, *2020*, 489.

Ali, A.S., Zaaba, Z.F., Singh, M.M., & Hussain, A. (2020). Readability of Websites Security Privacy Policies: A Survey on Text Content and Readers. *International Journal of Advanced Science and Technology*, *29*(6s), 1661-1672.

Alsdurf, H., Bengio, Y., Deleu, T., Gupta, P., Ippolito, D., Janda, R., Maharaj, T. (2020). COVI White Paper. *arXiv preprint arXiv:2005.08502*.

Bay, J., Kek, J., Tan, A., Hau, C.S., Yongquan, L., Tan, J., & Quy, T.A. (2020). BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders. *Government Technology Agency-Singapore, Tech. Rep*.

Castelluccia, C., Bielova, N., Boutet, A., Cunche, M., Lauradoux, C., Métayer, D. L., & Roca, V. (2020). DESIRE: A Third Way for a European Exposure Notification System Leveraging the best of centralized and decentralized systems. *arXiv preprint arXiv:2008.01621*.

Boudreaux, B., DeNardo, M.A., Denton, S.W., Sanchez, R., & Feistel, K. (2020). *Data Privacy During Pandemics: A Scorecard Approach for Evaluating the Privacy Implications of COVID-19 Mobile Phone Surveillance Programs*. Rand Corporation.

Boutet, A., Bielova, N., Castelluccia, C., Cunche, M., Lauradoux, C., Le Métayer, D., & Roca, V. (2020). *Proximity Tracing Approaches-Comparative Impact Analysis*. INRIA Grenoble-Rhone-Alpes,

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

Chowdhury, M.J.M., Ferdous, M.S., Biswas, K., Chowdhury, N., & Muthukkumarasamy, V. (2020). COVID-19 Contact Tracing: Challenges and Future Directions. *IEEE Access*.

Danz, N., Derwisch, O., Lehmann, A., Puenter, W., Stolle, M., & Ziemann, J. (2020). *Security and privacy of decentralized cryptographic contact tracing*. Cryptology ePrint Archive, Report 2020/1309.

Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. *In Proceedings of the eighth symposium on usable privacy and security*, 1-14.

Gostin, L.O., Hodge, J.G., & Wiley, L.F. (2020). Presidential powers and response to COVID-19. *JAMA*, *323*(16), 1547-1548.

Grace, M.C., Zhou, W., Jiang, X., & Sadeghi, A.R. (2012). Unsafe exposure analysis of mobile in-app advertisements. *In Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, 101-112.

Guillo, J.D. (2020). *Covid-19 tracing apps*: Ensuring privacy and data protection. https://www.europarl.europa.eu/news/en/headlines/society/20200429STO78174/covid-19-tracing-apps-ensuring-privacy-and-data-protection

Gupta, S., Kaur, M., Lakra, S., & Dixit, Y. (2020). A Comparative Theoretical and Empirical Analysis of Machine Learning Algorithms. *Webology*, *17*(1).

Hamilton, I.A. (2020). 11 countries are now using people's phones to track the coronavirus pandemic, and it heralds a massive increase in surveillance, www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3?r=DE\&IR=T, accessed: 13.07.2020

Huberman, B.A., Franklin, M., & Hogg, T. (1999). Enhancing privacy and trust in electronic communities. *In Proceedings of the 1st ACM conference on Electronic commerce*, 78-86.

Kind, C. (2020). Exit through the App Store? *Patterns*, *1*(3), 100054.

Klinkenberg, D., Fraser, C., & Heesterbeek, H. (2006). The effectiveness of contact tracing in emerging epidemics. *PloS one*, *1*(1), e12.

Krithiga, R., & Ilavarasan, E. (2020). A Novel Hybrid Algorithm to Classify Spam Profiles in Twitter. *Webology*, *17*(1), 260-279.

Levy, B., & Stewart, M.A. (2020). Systematic Review of The Ethics And Efficacy of Digital Contact Tracing Applications. *Harvard Data Science Review, 1-18.*

Li, T., Faklaris, C., King, J., Agarwal, Y., Dabbish, L., & Hong, J.I. (2020). Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing apps. *arXiv preprint arXiv:2005.11957*.

Li, T.C. (2020). Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis.

Maurer, U. (2005). Abstract models of computation in cryptography. *In IMA International Conference on Cryptography and Coding*, Springer, Berlin, Heidelberg 1-12.

Meadows, C. (1986). A more efficient cryptographic matchmaking protocol for use in the absence of a continuously available third party. *In IEEE Symposium on Security and Privacy*, 134-134.

Minami, K., & Borisov, N. (2010). Protecting location privacy against inference attacks. *In Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, 123-126.

Mozur, P., Zhong, R., & Krolik, A. (2020). In coronavirus fight, China gives citizens a color code, with red flags. *New York Times*, *1*.

Narain, S., Vo-Huu, T.D., Block, K., & Noubir, G. (2016). Inferring user routes and locations using zero-permission mobile sensors. *In IEEE Symposium on Security and Privacy (SP)*, 397-413.

O'Neill, P., Ryan-Mosley, T., & Johnson, B. (2020). *A flood of coronavirus apps are tracking us. Now it's time to keep track of them.* In: MIT Technology Review.

Park, S., Choi, G.J., & Ko, H. (2020). Information technology–based tracing strategy in response to COVID-19 in South Korea_privacy controversies. *Jama*, *323*(21), 2129-2130.

Ram, N., & Gray, D. (2020). Mass surveillance in the age of COVID-19. *Journal of Law and the Biosciences*, *7*(1), lsaa023.

Rivest, R.L., Callas, J., Canetti, R., Esvelt, K., Gillmor, D.K., Kalai, Y.T., & Shamir, A. (2020). *The PACT protocol specification*. In: Technical report, Vol. 0.1.

Spensky, C., Stewart, J., Yerukhimovich, A., Shay, R., Trachtenberg, A., Housley, R., & Cunningham, R.K. (2016). Sok: Privacy on mobile devices–it's complicated. *Proceedings on Privacy Enhancing Technologies*, *2016*(3), 96-116.

Tiwari, T., Klausner, A., Andreev, M., Trachtenberg, A., & Yerukhimovich, A. (2019). Location leakage from network access patterns. *In IEEE Conference on Communications and Network Security (CNS)*, 214-222.

Troncoso, C., Payer, M., Hubaux, J.P., Salathé, M., Larus, J., Bugnion, E.,. & Antonioli, D. (2020). Decentralized privacy-preserving proximity tracing. *arXiv preprint arXiv:2005.12273*.

Utz, C., Becker, S., Schnitzler, T., Farke, F. M., Herbert, F., Schaewitz, L., & Dürmuth, M. (2020). Apps Against the Spread: Privacy Implications and User Acceptance of COVID-19-Related Smartphone Apps on Three Continents. *arXiv preprint arXiv:2010.14245*.

Vaudenay, S. (2020). Analysis of DP3T. *IACR Cryptol. ePrint Arch., 2020*, 399.

Vinuesa, R., Theodorou, A., Battaglini, M., & Dignum, V. (2020). A socio-technical framework for digital contact tracing. *Results in Engineering*, *8*, 100163.

Watts, D. (2020). COVID Safe, Australia's Digital Contact Tracing App: The Legal Issues. *Australia's Digital Contact Tracing App: The Legal Issues*.

Woodhams, S. (2020). COVID-19 Digital Rights Tracker. In: TOPVPN. https://www. top10vpn. com/research/investigations/covid-19-digital

Zhao, Q., Wen, H., Lin, Z., Xuan, D., & Shroff, N. (2020). On the accuracy of measured proximity of bluetooth-based contact tracing apps. *In International Conference on Security and Privacy in Communication Systems* Springer, Cham, 49-60.

Zhou, X., Demetriou, S., He, D., Naveed, M., Pan, X., Wang, X., & Nahrstedt, K. (2013). Identity, location, disease and more: Inferring your secrets from android public resources. *In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 1017-1028.