Vol 4 No 1 (2022) *e*-ISSN: 2682-8383

Journal of Engineering Technology and Applied Physics

Security and Privacy of Contact Tracing Protocols for COVID-19

Zhen Ang Soh and Swee Huay Heng*
Faculty of Information Science and Technology, Multimedia University, Melaka, Malaysia.
**Corresponding author:* shheng@mmu.edu.my

https://doi.org/10.33093/jetap.2022.4.1.5
Manuscript Received: 10 January 2022, Accepted: 13 February 2022, Published: 15 March 2022

** The Abstract of this paper has been presented in CITIC 2021.*

Abstract **- Contact tracing is a way to track people who have been in contact with infected patients of COVID-19 and thereby effective control is achieved. Various countries have developed their own contact tracing applications which deploy the same or different protocol. It is of utmost importance to improve public awareness on the potential hidden risks of the respective protocols and applications and instill user confidence. The purpose of this research is to study the security and privacy of the existing contact tracing protocols to ensure that the security and privacy of users can be guaranteed. The protocols used by the applications include DP-3T protocol, TCN protocol, PEPP-PT protocol and BlueTrace protocol. The architecture of the protocols can be classified into centralised and decentralised architectures. In addition, the contact tracing applications in seven selected countries will be briefly analysed and compared. Some common user concerns are also outlined.**

Keywords—Contact tracing, COVID-19, privacy, protocol, security

I. Introduction

The new coronavirus COVID-19 was discovered at the end of 2019 and spread rapidly around the world. Protective measures have been taken against this deadly virus. As the number of COVID-19 cases around the world has risen sharply, protective measures have been taken against the virus around the world, such as isolation, prohibition of entry and exit, and contact tracing. Contact tracing is a way to track people who have been in contact with patients and where they went. Of course, contact tracing is also different in each country in terms of the architecture of protocols and policy. If the contact tracing method is handled well, the spread of the virus can be well controlled. This can eventually reduce the risk of infection greatly.

There are many types of contact tracing protocols and applications in use. In addition, each country has its own protocols and applications. However, how to protect the security and privacy of user or patient information in these applications and protocols is the main concern of the public. If the user's security and privacy cannot be guaranteed, the user's trust will be lost. This will usher in unimaginable consequences. Therefore, these applications and protocols will be discussed and analysed in-depth to understand how they work so that they can be trusted by users. The emphasis of this study is on how to avoid potential leakage of user data and to increase security awareness among users so that more users may utilise the security functions of these protocols and applications in order to minimise the risk of infection and to restore to normal life.

In [1], the authors evaluated the degree of privacy protection in the existing contact tracing system. The goal is to enable individuals to control their information and become a global standard. Although contact tracing can effectively control the spread of the virus, it also contains some hidden risks especially on user data security and privacy. If these risks are not being addressed properly, users may lose trust and the use will be abandoned.

In this paper, we first highlight the two architectures and the protocol methodologies commonly adopted. We then provide a quick review on several popular contact tracing protocols and the contact tracing applications in seven selected

Published by MMU PRESS. URL: https://journals.mmupress.com/index.php/jetap/index

countries. The contact tracing application in each country in terms of storage method and security are evaluated and its potential limitation is pointed out. Some common user concerns on user information privacy and protection, device storage capacity problem and location issue are outlined.

II. Differences between Centralised and Decentralised Architectures

Table I highlights the main differences between centralised and decentralised architectures before further discussions are presented. The centralised architecture centrally stores all data on a central server, where the data will be calculated and processed. In short, all data processing is operated and done by a central server. Meanwhile, in the decentralised architecture, the data is stored separately on the user's mobile phone, so all data calculations and operations will be completed on the user's mobile phone. This however will also cause a certain burden on the user's mobile phone.

Table I. Differences between centralised and decentralised architectures.

Centralised	Decentralised
The anonymous data will be uploaded to the remote server.	Users can control their information. Matches were made there with infected people.
Authorities can better understand the operating status.	Users can get more privacy. The infected people data will be uploaded to the server. Otherwise, the data be stored on the user's mobile phone.
The data of each mobile phone will be uploaded to the central server.	The data will be compared with the stored place visited or the Bluetooth identifier received from other mobile phones.
Analysis by public health agency.	The diagnosed patients' data will be shared.
GPS location data is collected and aggregated centrally.	

A. Centralised Architecture

If someone starts to show COVID-19 symptoms, the collected anonymous data will be uploaded to the remote server and matched with other contacts. If the collected data is stored on the server, authorities can better understand the operating status of applications and the spread of viruses. Data from mobile phones will be uploaded to the central server to be analysed by public health agencies. GPS location data is collected and aggregated centrally by mobile phones [2-5].

It is worth noting that due to the existence of the central server, once the server is attacked or compromised by hackers, a large amount of sensitive information will be stolen, causing social panic. However, users do not need to worry too much about this because all data will be encrypted into incomprehensible words or symbols called ciphertext. From this point of view, all calculations and matching work will also be taken care of by the server, so users do not need to perform too many operations.

B. Decentralised Architecture

Users can better control their information in decentralised architecture and matches were made with people who might be infected with virus. Moreover, users can get a higher level of privacy so as not to expose their social connections by criminals or their own country. Note that, when the user is diagnosed with COVID-19, the data will be uploaded to the server. Otherwise, the data will continue to be stored on the user's mobile phone. The COVID-19 operator's shared data will be compared with the locally stored place visited or the Bluetooth identifier received from other mobile phones earlier and the data of diagnosed patients will be shared among the populations [2-5].

Since only the user data that has been diagnosed will be uploaded to the server, even if the server is attacked, it will not cause a large amount of data loss and leakage. This architecture also needs to always turn on Bluetooth or similar functions, thus this will cause a large amount of power consumption of the mobile phone. Once the battery of phone is exhausted, the application will not function properly which may lead to ineffective tracing of the contacts. Therefore, users need to ensure that their phone battery is sufficient.

III. Protocol Methodologies

A. Bluetooth Proximity Tracing [6-8]

Bluetooth is a method to trace the encounter between two mobile phones. In general, the anonymous time-shift identifier will be transmitted to nearby devices via Bluetooth. These identifiers will then be submitted to the locally stored contact history record of the receiving device.

Due to Bluetooth has an encryption function, there are fewer privacy issues and lower battery usage. In addition, this protocol does not record the user's location information, so hidden dangers related to location information data will not affect this protocol. However, the possible inaccuracy of Bluetooth in detecting contact events is a problem and shortcoming of this protocol.

B. Location Tracking [9, 10]

GPS and cell phone tower network can achieve location tracking. The biggest advantage of the cell phone tower network is that users do not need to download applications. Israel is the first country to use this protocol. However, the accuracy is often insufficient for meaningful contact tracking. Smart phones can record GPS values so that smart phone GPS logging solution is more private. In addition, the unencrypted tracking information which is uploaded to the central system is also one of the privacy issue concerns.

C. QR Code Tagging

Assigning QR code to a place or venue is another method of tracing. This method allows people to scan the QR code with their mobile phone so that the user's visit can be tagged. In this way, people can voluntarily check in and check out from certain location. At the same time, users can also control their privacy. This method is used by the Malaysian government.

D. Ultrasound [11]

Another method is to use ultrasound to trace contacts. The smartphone will detect the ultrasonic signals emitted by other ultrasonic mobile phones. So far, a contact tracing application called NOVID is the only digital contact tracking with sub-meter contact tracking accuracy, mainly using Ultrasound.

E. CCTV with Facial Recognition [12, 13]

Confirmed cases and those who undermine control measures can be detected using closed-circuit television with facial recognition. It is worth noting that some systems that use this method will use a central database or store identification data, while some systems that use this method will not.

IV. CONTACT TRACING PROTOCOLS

Following are some existing protocols used in contact tracing applications or systems. These protocols help users preserve their privacy and security to avoid potential leakage of user data to third parties.

A. DP-3T Protocol [14]

The DP-3T protocol [14] is an open and decentralised protocol, which is also a COVID-19 proximity tracing using the Bluetooth Low Energy function on mobile devices. The protocol can store all calculations and personal data on the phone. This protocol was produced by a team of more than 25 scientists and academic researchers from all over Europe. In addition, the protocol has also been reviewed and improved by the wider community.

The use of the DP-3T protocol [15] is very important. This is because the purpose of this protocol is to optimise and speed up the identification of those who have close contact with the diagnosed person. In this way, some basic technologies can be provided to prevent the virus from spreading too fast. DP-3T can provide a great reduction of the security risk or privacy of communities or individuals. It can also ensure that the data can be protected at the highest level.

B. TCN Protocol [16]

The TCN protocol is a privacy-first contact tracing protocol, a decentralised protocol developed by the TCN Coalition. This protocol is extensible, and its main purpose is to provide some interoperability between exposure notification applications. The "Contact Tracing Bill of Rights" has been taken into consideration when designing the TCN protocol and its related work.

The TCN protocol allows users' mobile devices to transmit short-range broadcasts to nearby devices. This transmission is carried out via Bluetooth. In this way, if some users have been confirmed as ill, they can report the confirmed status to other people who have been in contact, and privacy issues can be largely guaranteed. On the contrary, if users do not send any related reports, no information will be displayed. If different applications use the same TCN protocol, these applications can interoperate.

C. PEPP-PT Protocol [17]

PEPP-PT protocol uses a centralised reporting server and is to make a management system works better by providing a common foundation. In countries with COVID-19 pandemic, this management system can be integrated with the country's public health response measures. European multinational company team is establishing PEPP-PT approach. In addition, the protocol is fully complying with the General Data Protection Regulation (GDPR) requirements, and is also a privacy-protected digital proximity tracing approach. When traveling across countries, it can also be used through an anonymous multi-country federation mechanism. Please note that neither location data nor personal identification information will be collected in this process.

D. BlueTrace Protocol [18]

This protocol was designed by the Singapore Government Technology Bureau. Applications using the BlueTrace protocol can mix decentralised and centralised contact tracing models. The collection and recording of the data between user devices that implement BlueTrace protocol is conducted in a peer-to-peer and decentralised manner to protect privacy. Trusted public health agencies will focus on the analysis of epidemic control guidelines so that the usage rate of the application can be increased.

E. Protocol Review

The above-mentioned protocols are very good tools against the spread of the virus and provide effective tracing. More importantly, all user data are stored locally in their mobile phone or device or central server that data is encrypted, meaning that user privacy is protected. In addition, the central server does not store personal information belonging to the users, which means that even if the server is maliciously attacked, the user information will not be leaked.

The DP-3T protocol is a decentralised architecture protocol such that all data will only be stored locally in the user's mobile phone. It only requires necessary data such as temporary ID to be uploaded for comparison and matching purpose. The protocol is mature enough to effectively protect users' sensitive information and privacy. The protocol can effectively trace contacts and resist the spread of viruses. The DP-3T protocol can also reduce the burden and cost of the server.

TCN and DP-3T are very similar protocols as they have similar functions and both can help track contacts. We can see that TCN can be used in different applications but the protocols used are all TCN protocols. This greatly improves the efficiency of tracing contacts and reduces the probability of exposure to danger. Furthermore, the user's identity information will not be recognised.

Although PEPP-PT and BlueTrace protocols are similar to DP-3T and TCN, there could be potential security risk as compared to DP-3T and TCN. This is because PEPP-PT has a central server where user privacy is likely to be leaked or observed if the central server is malicious. Also, the existence of a central server means that a huge database exists at the same time which may also be the main target of attackers.

V. REVIEW ON CONTACT TRACING APPS IN SELECTED COUNTRIES

Due to space limitation, the contact tracing applications from seven selected countries only are reviewed and evaluated in terms of their advantages and disadvantages, and information collected from the users.

Different countries developed their own country-specific contact tracing application, and these applications are designed to better prevent the spread of COVID-9. Although each application has its own advantages and disadvantages, the ultimate goal is to protect the people of its own country. People of all countries should also abide by national laws to reduce the spread of COVID-19. These applications are also developed and continuously improved with the aim of providing a more secure, efficient and user friendly platform to users.

A. Malaysia – MySejahtera [19]

No data will be recorded in this application without the user's permission. In this app, the location data is obtained from check-in procedures by scanning a QR code, and the health risk status is generated by answering a health assessment survey. All relevant data will only be stored for 90 days and will be permanently deleted. The application performs security functions that comply with global standards, which means that all data is encrypted and protected during transmission.

B. Australia – COVIDSafe [20]

COVIDSafe is a contact tracing application built on the BlueTrace protocol. All data about this application is stored by the international cloud service provider AWS. However, this application may have the possibility of canceling anonymity, which means that the real name will be used. This app may also interfere with other apps designed for diabetes monitoring systems. In order to ensure the security and stability of the application, some updates will process to improve the application. It is worth discussing whether the US government has the right to subpoena these data.

C. China – Chinese Health Code System [20]

This app will assign a color code, namely, green, yellow or red, based on the user health status and travel history assessment. This app uses various digital technologies to solve contact tracing issues, not just the app. The applications and technologies used may possess potential privacy violations. This app uses Global System for Mobile Communications (GSM) cell positioning to estimate close contact which may not always be accurate and thus accuracy could be a concern.

D. India – AarogyaSetu [20]

AarogyaSetu is built on Aarogya Setu Protocol [21]. This app collects absolute location information so the user location will be known. Due to the collection of absolute location information, there is a risk of potential cyber hacking or national surveillance of citizens. In addition, there is no clear indication of how long the data will be retained and who can access the information stored in the data center.

E. Singapore - Trace Together [20]

Trace Together is an application built on the BlueTrace protocol. Unlike the Indian contact tracing app, this application does not collect personal geographic location. It is however vulnerable to certain types of cyber-attacks due to its centralised architecture.

F. South Korea - Corona 100m [20]

The country's prolific CCTV, mobile phone location data and credit card transaction records are used by South Korea to trace people. This application has very serious privacy issues and committed personal privacy. All users will be strictly controlled and their data will be collected by completely ignoring their privacy.

G. UK - NHS COVID-19 App [20]

This application uses Bluetooth handshakes to register contacts between smartphone users or proximity events. All data about the user location will be provided to the authorities and this data may be misused and stored. However, this application does not use the location of the phone to trace contacts and instead requires users to provide the first half of their zip code.

VI. MAIN CONCERNS

If users are doubtful about certain information, it is likely that they may give up using the application. We outline some common user concerns below:

A. User Information Privacy and Protection

The privacy, usage, and protection methods of the collected and uploaded data are common issues that users are concerned about especially for centralised servers. Data protection by way of encryption and the access control to the data is equally important.

B. Storage Capacity Problem

As far as data storage in the mobile phone is concerned, users may worry about whether there will be a large amount of irrelevant data being stored as this will result in insufficient phone capacity. The capacity of the central server is also a concern as data could be lost or ignored if not careful.

C. Location Issue

Collecting user's location information in order to track contacts is one of the hidden risks. Users may worry about whether their whereabouts and daily activities will be disclosed to malicious people. Some users may provide wrong information in order not to disclose their location information which may indirectly lead to information errors.

VII. CONCLUSION

We provided a quick review on some popular contact tracing protocols and applications with the emphasis on the security and privacy aspect. It is hoped that this brief review is able to serve as a quick guide for users and to improve security awareness among users. This study is by no means exhaustive as it takes into account protocols and applications that are well-known and widely used only.

ACKNOWLEDGEMENT

This work was supported by the Ministry of Higher Education of Malaysia's Fundamental Research Grant Scheme (FRGS/1/2018/ICT04/MMU/01/01).

REFERENCES

[1] R. Abrich and S. C. Gary, "Privacy Preserving Contact Tracing," *Info. Sys. Secur. Assoc.*, November, pp. 12-18, 2020.

[2] C. Criddle and L. Kelion, "Coronavirus Contact-Tracing: World Split between Two Types of App," *BBC News*, [Online] *https://www.bbc.com/news/technology-52355028*, 2020.

[3] E. Pullicino, "Coronavirus and Contact Tracing Apps," *Bristows*, [Online] *https://www.bristows.com/news/coronavirus-and-contact-tracing-apps/*, 2020.

[4] J. Sanchez and. M. Feeney, "Protect Privacy When Contact Tracing," CATO Institute, [Online] *https://www.cato.org/publications/pandemics-policy/protect-privacy-when-contact-tracing#data-storage,* 2020.

[5] D. Pahwa and R. Beaudry, "The Architecture of Trust in Contact Tracing," [Online] *https://covidsafepaths.org/*, 2020.

[6] J. Bay, J. Kek. A. Tan, C. S. Hau, L. Yongquan, J. Tan and T. A. Quy, "BlueTrace: A Privacy-Preserving Protocol for Community-Driven Contact Tracing Across Borders," *Government Technology Agency*, Singapore, pp. 1-9, 2020.

[7] K. Servick, "COVID-19 Contact Tracing Apps Are Coming to a Phone Near You. How Will We Know Whether They Work?" *ScienceInSider,* [Online] *https://doi.org/10.1126/science.abc9379*, 2020.

[8] A. Vaughan, "Bluetooth May not Work Well Enough to Trace Coronavirus Contacts," *New Scientist*, [Online] *https://www.newscientist.com/article/2243137-bluetooth-may-not-work-well-enough-to-trace-coronavirus-contacts/*, 2020.

[9] O. Hoimes, "Israel to Track Mobile Phones of Suspected Coronavirus Cases," *The Guardian*, [Online] *https://www.theguardian.com/world/2020/mar/17/israel-to-track-mobile-phones-of-suspected-coronavirus-cases*, 2020.

[10] B. J Stanley and J. S. Granick, "The Limits of Location Tracking in An Epidemic," *American Civil Liberties Union*, pp. 1–9, 2020.

[11] "A New Approach to Pandemics," *NOVID*, [Online] Retrieved May 24, 2021, from *https://www.novid.org/.*

[12] K. Carter, G. Berman, M. García-herranz, and V. Sekara, "Digital Contact Tracing and Surveillance During COVID-19 General and Child-specific Ethical Issues," *Unicef Office of Research*, pp. 1-25, June, 2020.

[13] "Coronavirus France: Cameras to Monitor Masks and Social Distancing," *BBC News* (4 May 2020), [Online] *https://www.bbc.com/news/world-europe-52529981.*

[14] S. Rosch, "DP3T Android Demo App," [Online] *https://github.com/DP-3T/dp3t-app-android-demo/blob/develop/README.md*, 2020.

[15] Veale, "DP3T - Decentralized Privacy-Preserving Proximity Tracing," [Online] *https://github.com/DP-3T/documents/blob/master/README.md*, 2020.

[16] H. Valence, "TCN Protocol," [Online] *https://github.com/TCNCoalition/TCN/blob/main/README.md*, 2020.

[17] "Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) Documentation," [Online] *https://github.com/pepp-pt/pepp-pt-documentation/blob/master/README.md*, 2020.

[18] "What is BlueTrace? – TraceTogether FAQs," [Online] *https://support.tracetogether.gov.sg/hc/en-sg/articles/360044883814-What-is-BlueTrace-*, 2020.

[19] "MySejahtera Privacy Policy," [Online] *Retrieved March 20, 2021, from https://mysejahtera.malaysia.gov.my/privasi_en/.*

[20] M. J. M. Chowdhury, M. S. Ferdous, K. Biswas, N. Chowdhury and V. Muthukkumarasamy, "COVID-19 Contact Tracing: Challenges and Future Directions," *IEEE Access*, vol. 8, 225703–225729, 2020.

[21] "Aarogya Setu's Data Access and Knowledge Sharing Protocol, 2020," [Online] Retrieved May 17, 2021, from *https://vidhilegalpolicy.in/blog/aarogya-setus-data-access-and-knowledge-sharing-protocol-2020/.*