# A Global Contact Tracing Application for Viral Outbreak: Architecture, Design, and Deployment Challenges

**Anas Basalamah**[1†],

Umm Al-Qura University

**Abstract**

A contact tracing application can remedy the rapid infection spike to minimize the massive spread of infectious viruses during an outbreak. During the COVID-19 pandemic, many contact tracing applications based on QR codes, Global Positioning System (GPS), and Bluetooth technologies were launched that helped control the virus's spread. This paper reviews the underlying architecture of those contact tracing applications and presents a global contact tracing application framework for future use. The proposed architecture follows the Bluetooth-based decentralized framework that promises the end-user higher data privacy and security.

***Key words:***

*Contact Tracing, Bluetooth, Covid-19.*

## 1. Introduction

The COVID-19 pandemic caused by Severe Acute Respiratory Syndrome-Coronavirus-2 (SARS-CoV-2) stimulated various researches on the design and development of contact tracing applications. Various contact tracing applications have been deployed in different countries to prevent the rapid spread of the coronavirus that saved many lives. However, the COVID-19 pandemic is not the only viral infection spreading worldwide in the twenty-first century. The world has witnessed several severe viral attacks like-Ebola, Zika, West Nile, pandemic influenza, and severe acute respiratory syndrome (SARS) except the SARS-CoV-2 in the initial two decades of the 21st-century [1]. More such infectious viruses may appear in the coming decade. Therefore, it is necessary to become prepared in advance with the experience of the recent COVID-19 outbreak. Although the COVID-19 pandemic is not finished yet, new mutations of this virus, such as newcov, omicron, B.1.1.7, and B.1.351 exhibited their threats and took many lives. But the progress in vaccination programs shows us hope to overcome this situation as early as possible. However, most vaccines are struggling to prevent the new mutation of COVID. Therefore, countries impose travel bans and go through strict lockdown in Europe, America, Africa, and Asia. Although governments and people are adapting to this new normal situation daily, it is important to search for ways to be an efficient remedy to international travel bans and nationwide lockdown.

In this paper, we propose a globally deployable contact tracing app architecture that can work as a remedy to the rapid spread of current COVID-19 mutation and future infectious viral outbreaks. Many researchers have studied different architectures for contact tracing applications. All these studied architectures can be classified into three main types: centralized architecture, decentralized architecture, and hybrid architecture [2]. Two primary technologies used as the backbone of the architecture are Bluetooth and Global Positioning System (GPS) [3].

In this paper, we propose a decentralized Bluetooth-based application architecture that can be deployed worldwide with the prime supervision of the World Health Organization (WHO). In this architecture, the WHO and local governments will maintain the global (central) and local (country-wise) databases. The proposed architecture follows a decentralized architecture method because of its user data privacy. Decentralized and hybrid architectures rarely involve central or local databases as they store user contact tracing data at the user device. The user only uploads the data to the database if they get infected by the virus. Random seed for each user is allocated during the installation of the application at the user device, which works as the only identifier of the user. Therefore, there is a rare chance of breaking user data privacy and misusing personal information.

---

Manuscript received March 5, 2022
Manuscript revised March 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.3.63

We present a summary of different architectures in section 2 that discusses the mechanism of each architecture, advantages, and disadvantages. The remaining part of the paper is structured as follows: the proposed model's architecture and design are discussed in section 3.1, various deployment challenges for an application to deploy globally is discussed in section 3.2, and the paper concludes in section 4.

## 2. Survey on Contact Tracing Application

The twenty-twenty (2020) started with a few coronavirus cases and ended with millions of infected people and thousands of deaths on the tally. The virus spread rapidly throughout the world, and every country suffered from a long lockdown. People below the poverty line suffered the most during the lockdown in poor and least developed countries. The rapid spread rose exponentially because of asymptotic carrier individuals. It is nearly impossible to find asymptotic carriers as they do not exhibit any symptoms. But it is possible to trace infected patients with symptoms as they usually get tested after suffering from the symptoms. An efficient way to limit the virus's spread is to trace the infected or suspected individual's movement, and their close contacts during their movements [4].

Many contact tracing applications have been deployed to trace the infected or suspected individuals and notify others who have been exposed to COVID-19 confirmed patients, thus facilitating the government, public, and social organizations to control the pandemic [5]. Different technologies are used to develop these applications at the regional level [6]; for example- Asian countries such as China, Singapore, South Korea are among the first to develop and deploy contact tracing applications in their respective land. China developed a QR code-based Epidemic Prevention and Health Information Code (EPHIC) after the surge of COVID-19 in February 2020 [7]. The EPHIC has a specific QR code, which the user scans to provide their current health status, information of the last contact with a COVID positive or suspected patient with contact location within the past 14 days, and residential address. Besides, Australia and New Zealand are among the first countries to develop a national contact tracing application to trace contacted persons with COVID-19 patients [8]. Later, Canada, the USA, more than 20 countries of Europe developed contact tracing applications to restrict the infection rate [9,10,11]. Among these countries, One-third states of the USA, Germany, Netherlands, and Switzerland used the Google-Apple API to develop their contact tracing application. This Google-Apple API was launched jointly in May 2020 by the two tech giant Google, and Apple [12,13].

All developed contact tracing applications are based on the mobile platform, and there is many debates on the underlying architectures and used technologies of these applications, such as decentralized versus centralized, Global Positioning System (GPS) versus QR code scanning, big data analysis versus Bluetooth devices, etc. The government controls the personal data of the user in the centralized app architecture, and it uses Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) protocol for data privacy [14]. The centralized architecture is considered an academic framework, which is imperfect for practical implementation by the technical advisors.

In contrast, the decentralized framework stores personal data of the user at the user device that follows the DP-3T (Decentralised Privacy-Preserving Proximity Tracing) protocol for data protection and privacy [15]. However, this architecture is considered partially decentralized compared to the Google-Apple contact tracing API. GPS-based contact tracing architecture is based on crowd mapping for tracking the COVID-19 spread, whereas the QR code-based approach is equipped with the combination of physical, thermal imaging, or temperature testing along with user data collection. The following subsections discuss these architectures in detail with their embedded data privacy settings and protocols.

### 2.1. GPS based contact tracing

The global positioning-based contact tracing application CovTracer [16,17] was developed and deployed in Cyprus. This application works by tracking the GPS location of the user device, and contact is considered when two devices share the exact location for a long time. Since each smartphone has the GPS feature embedded by default, this way of tracing seems very promising. However, the technology faces two significant issues that question the application of this framework. Firstly, it breaks user data privacy protocol by tracking the user's location simultaneously, which causes significant concern for the individuals' personal information, such as frequent co-locators, daily routine, and activities. Secondly, it fails to classify close contacts for indoor and outdoor places with higher accuracy as the false positive and false negative cases are very high. For example- the GPS has a positioning error of around 30 feet [18] when the user stays in indoor places. GPS technology usually considers close contact if the distance is approximately 6 feet. Since a user persists in indoor areas most of the day, the rate of miss-classifying close contacts becomes very high. As a result, it loses its effectiveness to be considered a promising framework in the contact tracing domain.

## 2.2. GPS based contact tracing

The Bluetooth-based method works similarly to GPS by detecting close devices within a specific distance range for a certain amount of time. Different architectures store these contact data in different ways. Centralized architecture stores the data in a central server whereas decentralized framework stores contact information locally in the user device. Researchers prefer a decentralized approach over the centralised approach because of the user data protection technique of DP-3T protocol. However, all the Bluetooth-based methods are discussed in the following subsections with good examples.

### 2.2.1 Centralized

The centralized architecture described here is based on the Bluetrace protocol [19]. The first requirement for the app is that the user must pre-register with the central server. The server will generate a temporary ID (TempID) for each device to protect user privacy. This TempID is then encrypted with a private key and sent to the device. When the devices come into close contact with each other, they exchange these TempIDs (with a Bluetooth encounter message). If the user tests positive, they can voluntarily upload all stored encounter messages to the central server. Afterward, the the TempID is mapped by the server with these messages to individuals to identify risky contacts.

### 2.2.2 Decentralized

The decentralized architecture transfers core functionalities of the contact tracing process to the user device so that the server requires minimal involvement during the trace. The idea is to generate an anonymous ID on the user device (keeping the actual user ID confidential to the server and other users) and process contact notifications on individual devices rather than on a centralized server for user privacy.

This is in contrast to a centralized architecture that employs a fully private automated contact tracing protocol (PACT) [20] as a basis for describing a distributed architecture. The decentralized approach does not require app users to "pre-register" before using, so storing the PII on the server is unnecessary. The device generates a random seed (used as an input for a pseudo-random function). It is used in combination with the current time and produces a pseudonym or "chirp" that protects privacy with a very short lifespan of about 1 minute. These chirps are then regularly replaced with other devices in close contact. Once a user is diagnosed with COVID-19, they can volunteer to upload seed and associated time information to a central server. A list of encounter messages will be uploaded. Uploading seeds on behalf of all used chirps will improve latency and bandwidth utilization.

The central server only acts as a rendezvous point, similar to a bulletin board that advertises the seeds of infected users. This server is considered "honest but curious." Other app users can download these seeds and rebuild the chirps (using timestamps) sent by the infected user. Servers and other users cannot derive identification details simply by knowing the seeds and chirps. Only other app users can perform a risk analysis to see if it has been published long enough. This one-way lookup for downloaded seeds limits server functionality and reduces some privacy risks.

### 2.2.3 Hybrid

The server performs complex tasks such as TempID calculation, encryption, decryption, risk analysis, and alerting at-risk contacts in a centralized architecture. In contrast, these features are delegated to devices with a distributed architecture, and the server is kept only as a bulletin board for lookup purposes. The

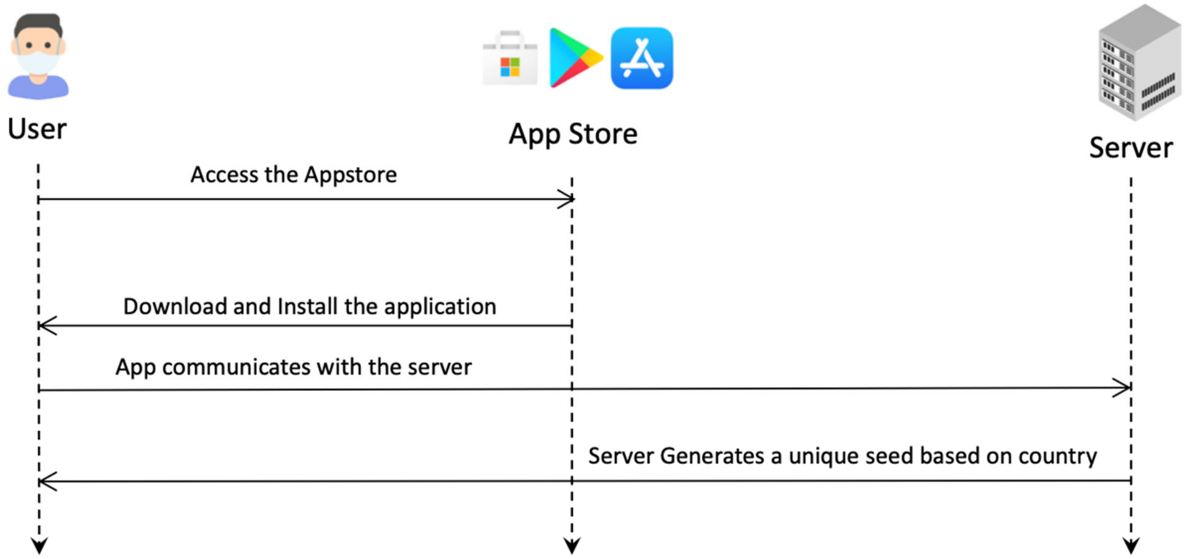

Figure 1: Installation process of the global contact tracing application.

hybrid architecture proposes to split these features between the server and the device. More specifically, TempID generation and management remain decentralized (that is, processed by the device), ensuring privacy and anonymity. Still, risk analysis and notification must be the responsibility of the centralized server.

There are three main reasons to run the tracing process on the server. i) In a distributed architecture, the server does this risk analysis without considering the server, so the server is unaware of the number of users at risk. Therefore, the server has no statistics and cannot perform data analysis to identify exposed clusters. ii) Risk analysis and notification is considered a sensitive process that must be handled by the authorities, keeping in mind existing infrastructure resources and pandemic conditions. iii) Encounter information uploaded by an infected user will not be available to other users and will only be retained on the server. This is to avoid user anonymization attacks that can occur in distributed architectures. To describe the hybrid architecture in this context, we will use the Desire protocol [21]. This protocol requires the user's app registration process to assign a unique device ID without recording the PII. The device then cryptographically generates a temporary ID and exchanges it with another device via BLE. For each EphID received, two non-linkable private encounter tokens (PETs) are generated and stored to represent the encounter. If the user tests positive, a locally generated list of PET will be uploaded to the server. Now any device can send the second generated PET token to the server, which will perform risk analysis and notifications. The server cannot infer identification information from PET, and all communication between the server and the device is routed through a proxy or anonymized network.

## 3. Global Contact Tracing Application

The proposed global contact tracing application is based on a decentralized architecture. The designed framework modifies the decentralized architecture a little for generating and maintaining the seed and also during notifying the contacted users if they get encountered any positive patient in the last 14 days. The application installation and working architecture are discussed in the following subsections.

### 3.1 Design and Architecture

Figure [1] depicts the installation process of the contact tracing application. When the application gets

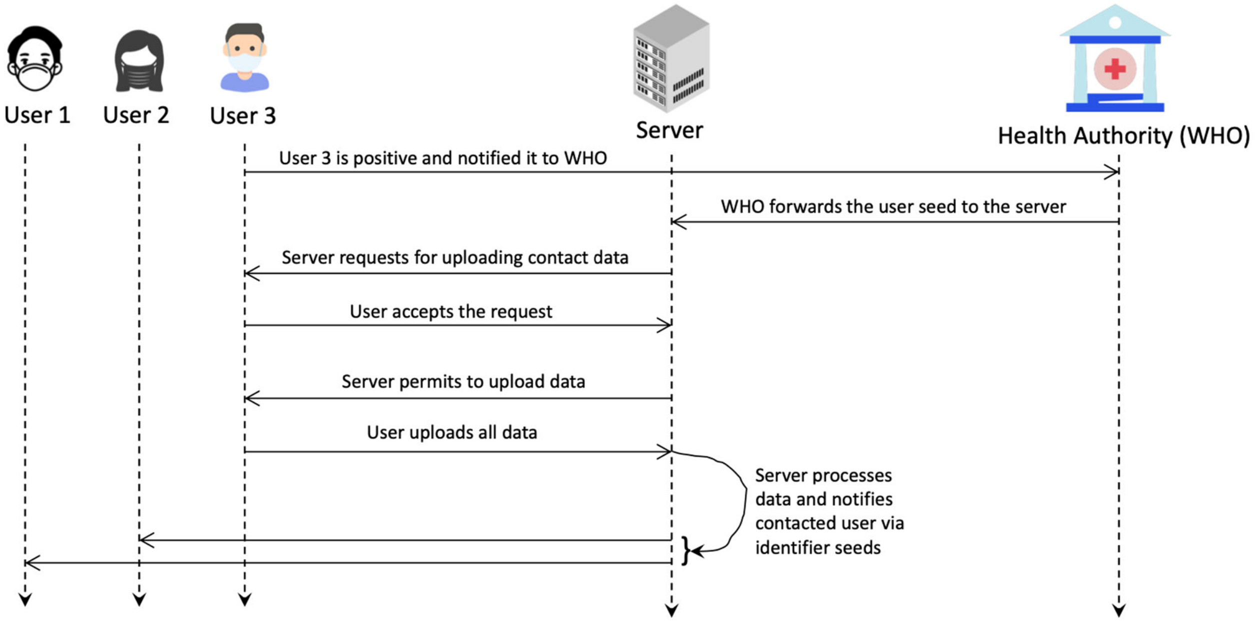

Figure 2: Architecture of the proposed global contact tracing application.

installed in a user device, it immediately contacts the main server for an identification seed. In the conventional decentralized method, the seed is automatically generated at the user device to add more security layers for the user data. As the app only gathers contact data with timestamps against a particular seed, there is no specific identification process for the user. The data collection method is secure enough and does not contain personal information. Therefore, we transfer the seed generation process on the server to maintain a country-wise unique seed range and count the number of confirmed cases for each country on each day. The total number of confirmed and suspected cases throughout the world can also be generated simply from the server.

### 3.2 Deployment Challenges

The architecture used for the proposed global contact tracing application is depicted in Figure 2. The architecture follows all the key points of the decentralized method except the user data processing on the server and notification method for isolating the contacted user with the positive patient. In the conventional decentralized method, the application of the user device automatically downloads all the uploaded data and processes them to find its contact involvement with a confirmed patient.

In contrast, the proposed method analyzed the data to find out all contacted seeds in the last 14 days with the confirmed patient when a patient uploads their data. The seed generated for each user is permanent and remains the same for that device until the user uninstalls and reinstalls the application in their device. The proposed method is easier to manage, simple for notifying the users in threat, facilitate the counting of confirmed patient country-wise and worldwide in a simple way, and satisfies user data privacy conditions. The proposed architecture uses the DP-3T protocol for maintaining all communication between the user device and the server.

## 4. Conclusion

The recent COVID-19 pandemic inspired the research community to launch efficient technologies for preventing viral outbreaks. This research adds a new dimension to the contact tracing application development. Hopefully, it will inspire more researchers to think about such techniques that are efficient for tracing positive patients. Contact tracing applications can help the world avoid lockdown situations in the future on a large scale if new variants of the COVID come or any new viral infection spreads. Therefore, more research is required on this particular technology to make it better with features like user data protection, positive case counts, automated notification methods, etc.

## References

[1] K. Payne, P. Kenny, J. M. Scovell, K. Khodamoradi, and R. Ramasamy, “Twenty-first century viral pandemics: a literature review of sexual transmission and fertility implications in men,” *Sexual medicine reviews*, vol. 8, no. 4, pp. 518–530, 2020.

[2] N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, and S. K. Jha, “A survey of covid-19 contact tracing apps,” *IEEE access*, vol. 8, pp. 134 577–134 601, 2020..

[3] L. Du, V. L. Raposo, M. Wang *et al.*, “Covid-19 contact tracing apps: A technologic tower of babel and the gap for international pandemic control,” *JMIR mHealth and uHealth*, vol. 8, no. 11, p. e23194, 2020.

[4] S. Chen, J. Yang, W. Yang, C. Wang, and T. Ba ̈rnighausen, “Covid-19 control in china during mass population movements at new year,” *The Lancet*, vol. 395, no. 10226, pp. 764–766, 2020.

[5] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Do ̈rner, M. Parker, D. Bonsall, and C. Fraser, “Quantifying sars-cov-2 transmission suggests epidemic control with digital contact tracing,” *Science*, vol. 368, no. 6491, p. eabb6936, 2020.

[6] N. Oliver, B. Lepri, H. Sterly, R. Lambiotte, S. Deletaille, M. De Nadai, E. Letouze ́, A. A. Salah, R. Benjamins, C. Cattuto *et al.*, “Mobile phone data for informing public health actions across the covid-19 pandemic life cycle,” p. eabc0764, 2020.

[7] Z. Li, Q. Chen, L. Feng, L. Rodewald, Y. Xia, H. Yu, R. Zhang, Z. An, W. Yin, W. Chen *et al.*, “Active case finding with case management: the key to tackling the covid-19 pandemic,” *The Lancet*, vol. 396, no. 10243, pp. 63–70, 2020..

[8] D. Watts, “Covidsafe, australia’s digital contact tracing app: the legal issues,” *Australia’s Digital Contact Tracing App: The Legal Issues (May 2, 2020)*, 2020.

[9] E. Fernandez, “Privacy and contact tracing apps—google and apple debate with world governments,” 2020.

[10] J. Leith and S. Farrell, “Measurement-based evaluation of google/apple exposure notification api for proximity detection in a light-rail tram,” *Plos one*, vol. 15, no. 9, p. e0239943, 2020.

[11] A. Blasimme, A. Ferretti, and E. Vayena, “Digital contact tracing against covid-19 in europe: Current features and ongoing developments,” *Frontiers in Digital Health*, vol. 3, p. 61, 2021.

[12] C. Dwork, A. Karr, K. Nissim, and L. Vilhuber, “On privacy in the age of covid-19,” *Journal of Privacy and Confidentiality*, vol. 10, no. 2, 2020.

[13] S. Chidambaram, S. Erridge, J. Kinross, and S. Purkayastha, “Observational study of uk mobile health apps for covid-19,” *The Lancet Digital Health*, vol. 2, no. 8, pp. e388–e390, 2020..

[14] N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, and S. K. Jha, “A survey of covid-19 contact tracing apps,” *IEEE access*, vol. 8, pp. 134 577–134 601, 2020.

[15] C. Troncoso, M. Payer, J.-P. Hubaux, M. Salathe ́, J. Larus, E. Bugnion, W. Lueks, T. Stadler, A. Pyrgelis, D. Antonioli et al., “Decentralized privacy-preserving proximity tracing,” *arXiv preprint arXiv:2005.12273*, 2020.

[16] P. Isaia, C. Laoudias, A. Kamilaris, and C. G. Panayiotou, “Covtracer-en: The journey of covid-19 digital contact tracing in cyprus,” in *2021 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. IEEE, 2021, pp. 1–8.

[17] A. Trivedi and D. Vasisht, “Digital contact tracing: technologies, shortcomings, and the path forward,” *ACM SIGCOMM Computer Communication Review*, vol. 50, no. 4, pp. 75–81, 2020.

[18] M. B. Kjærgaard, H. Blunck, T. Godsk, T. Toftkjær, D. L. Christensen, and K. Grønbæk, “Indoor positioning using gps revisited,” in *International conference on pervasive computing*. Springer, 2010, pp. 38–56.

[19] 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, Tech. Rep*, vol. 18, 2020.

[20] R.L.Rivest, D.Weitzner, L.Ivers, I.Soibelman, and M.Zissman, “Pact: Private automated contact tracing,”*Retrieved December*, vol. 2, p. 2020, 2020..

..

[21] A. Boutet, C. Castelluccia, M. Cunche, C. Lauradoux, V. Roca, A. Baud, and P.-G. Raverdy, “Desire: Leveraging the best of centralized and decentralized contact tracing systems,” *Digital Threats: Research and Practice*, 2021.