Computers, Materials & Continua
DOI:10.32604/cmc.2022.018736
Article

Tech Science Press

Real-time Privacy Preserving Framework for Covid-19 Contact Tracing

Akashdeep Bhardwaj[1], Ahmed A. Mohamed[2,3,*], Manoj Kumar[1], Mohammed Alshehri[4] and Ahed Abugabah[5]

[1]School of Computer Science, University of Petroleum & Energy Studies (UPES), Dehradun, 248007, India
[2]Department of Computer Science, College of Computer and Information Sciences, Majmaah University, Majmaah, 11952, Saudi Arabia
[3]Department of Information Technology, Faculty of Computer and Information, Assiut University, Assiut, 71515, Egypt
[4]Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Majmaah, 11952, Saudi Arabia
[5]Department of Information System, College of Technological Innovation, Zayed University, Abu Dhabi, United Arab Emirates
[*]Corresponding Author: Ahmed A. Mohamed. Email: amohamed@mu.edu.sa

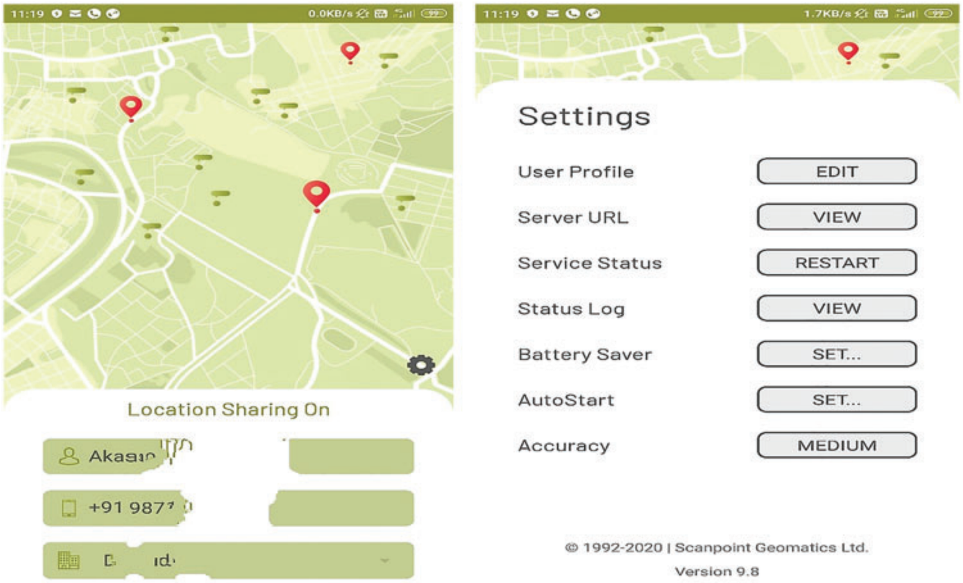
Received: 19 March 2021; Accepted: 14 May 2021

Abstract: The recent unprecedented threat from COVID-19 and past epidemics, such as SARS, AIDS, and Ebola, has affected millions of people in multiple countries. Countries have shut their borders, and their nationals have been advised to self-quarantine. The variety of responses to the pandemic has given rise to data privacy concerns. Infection prevention and control strategies as well as disease control measures, especially real-time contact tracing for COVID-19, require the identification of people exposed to COVID-19. Such tracing frameworks use mobile apps and geolocations to trace individuals. However, while the motive may be well intended, the limitations and security issues associated with using such a technology are a serious cause of concern. There are growing concerns regarding the privacy of an individual's location and personal identifiable information (PII) being shared with governments and/or health agencies. This study presents a real-time, trust-based contact-tracing framework that operates without the use of an individual's PII, location sensing, or gathering GPS logs. The focus of the proposed contact tracing framework is to ensure real-time privacy using the Bluetooth range of individuals to determine others within the range. The research validates the trust-based framework using Bluetooth as practical and privacy-aware. Using our proposed methodology, personal information, health logs, and location data will be secure and not abused. This research analyzes 100,000 tracing dataset records from 150 mobile devices to identify infected users and active users.

Keywords: Privacy; contact tracing; mobile apps; Bluetooth; Covid; epidemic

1 Introduction

Epidemics such as H1N1, SARS, Ebola, and the recent coronavirus have impacted millions of people worldwide, resulting in a large death toll. The World Health Organization (WHO) has issued several advisories and courses for action to limit the spread of COVID-19 [1] infection by tracing infected individuals. The tracing process requires infected individuals to share information with governments and local medical agencies, which are tasked with tracking and quarantining individuals who may have been in close contact with infected victims, and the subsequent collection of further information about the infected victims. Tracking involves acquiring the personal information of each infected individual, including their travel history, locations visited, recent contacts, and their health details [2]. While most individuals may be comfortable with sharing this information for their own and the nation's benefit, privacy-aware individuals may not be so willing. This can hinder the contact tracing process, even as the virus continues to spread at alarming rates [3]. Secure and privacy-aware contact tracing methods can inspire everyone, infected or not, of all ages to join the contact tracing, with an assurance of the data being processed confidentially and with no malicious intent. Globally, various contact tracing applications, such as mobile apps and global positioning systems (GPS), are being used. The infected individual is expected to self-test and self-report health details using mobile applications and location data [4]. However, the sharing of data depends on local infrastructure and networks, which rely on unsecured external technologies such as wireless access points, GPS, data networks, or even those involved in the deployment and maintenance of the application itself. The government of Singapore has launched a contact tracing app called "Trace Together." The Indian government's contact tracing app, which is called Aarogya Setu, performs real-time tracking, as illustrated in Fig. 1.



Location Sharing On

Akas [redacted]

+91 987 [redacted]

[redacted]

Settings

User Profile EDIT

Server URL VIEW

Service Status RESTART

Status Log VIEW

Battery Saver SET...

AutoStart SET...

Accuracy MEDIUM

© 1992-2020 | Scanpoint Geomatics Ltd.
Version 9.8

Figure 1: Interface of Aarogya Setu contact tracing app

This study proposes the use of a mobile application with Bluetooth connectivity to perform real-time contact tracing. The authors propose the use of mobile devices to send anonymous beacons of encrypted random code messages via Bluetooth. This allows for foolproof data privacy, and individuals remain anonymous. No collection of privacy-sensitive data is involved or dependent on external third-party IT infrastructure. The major highlights of this research are privacy-aware contact-tracing mobile applications with the following features.

- The proposed contact tracing application does not involve any public wireless or network infrastructure.
- No personally identifiable sensitive information, geolocation, or logs is shared or gathered.
- Real-time tracking enables the rapid identification of locations corresponding to new infected cases.
- Focuses on complete privacy and the use of an individual's Bluetooth connection to determine others within a specific range.
- Around 100,000 contact tracing datasets were used, which involves 150 individual mobiles.

This technology process helps to monitor infected individuals as well as reduce the medical costs involved during quarantine measures. The focus is on testing a framework that ensures complete privacy. To evaluate the contact-tracing framework, T-test and regression analysis were used to validate datasets from real scenarios.

The remainder of this paper is organized as follows: Section 1 describes in detail contact tracing and privacy issues, and Section 2 presents the literature survey regarding the different contact-tracing methods employed by various researchers. The proposed Contact Tracking Framework (CTF) algorithm is illustrated in Section 3. Section 4 discusses the experimental results obtained and presents the T-test validation of the dataset reviewed.

1.1 Contact Tracing and Privacy Issues

Contact tracing involves the identification, assessment, and management of persons exposed to diseases to prevent any onward transmission. If scientifically applied, this can help break the transmission chain of infectious diseases and can be an effective health tool for managing outbreaks. With respect to COVID-19, contact tracing requires the identification of individuals who may have been exposed. Steps such as the quarantining of contacts and the isolation of cases need to be performed. The design and development involved in the contact tracing application system needed to consider various threat vectors in terms of privacy, as presented in Tab. 1.

Table 1: Privacy threat vectors and their malicious activities

Threat vectors	Unauthorized & malicious privacy activities
Software development team	• Perform malicious activities such as accessing and uploading the data of individuals and other users in proximity and selling them on the dark web. • Snoop on data from other mobile apps running on the mobile device. • Request additional app permissions for accessing storage, camera, SMS, emails, location etc., without the user's permission. • Analyzing the app data for generating further insights, which were not parts of the privacy or service.
Nation states	• Selectively analyze individuals or the community and retaining personal, health, or discriminative user data even after the outbreak has ended or the app has been uninstalled. • Perform mass surveillance. • Analyze data for generating insights, which were not part of the service.

(Continued)

Table 1: Continued

Threat vectors	Unauthorized & malicious privacy activities
Internet service provider	• Can perform all the malicious activities listed above if the design involves the use of mobile data or IT infrastructure during communication between application and server.
Privilege/Apps dependency	• Read locally stored data and monitor network activities. • Paired devices within Bluetooth range can leak data if not properly encrypted.
Hackers	• Can perform penetration testing to discover zero-day exploits. Release the vulnerability worldwide to cause chaos. • Access the user's device without their consent or proper authorization.

Gathering personal mobility details for health application purposes presents challenges, even if privacy ethics and issues are upheld. The analysis of any individual's mobility and health data can only be justified if the benefits are related to public health. Most existing contact-tracing solutions rely on wireless infrastructure for contact tracing to preserve privacy.

2 Literature Survey

During the 2014 EBOLA outbreak, the WHO expounded on the significance of contact tracing and even proposed protocols for tracing infected individuals. However, no mobile application or data-gathering technologies were deployed. The WHO has proposed recommendations for medical staff and those on the front line to improve the safety of using contact tracing applications. With COVID-19, several countries have mandated the use of mobile-based contact tracing, thus gathering data and making use of data obtained from mobile applications. Monitoring and regulating interactions are vital for preventing the spread of this disease. Internet-and mobile-based technologies have aided in terms of surveillance, modeling of infection, remote sensing, etc., to predict and control the disease spread [5]. This tactic of using new-age technology to deal with global epidemics is classified as digital epidemiology under a new domain, as described by Chancay-García et al. [6]. Recently, several researchers have assessed the categorization of mobile call data records. Dede et al. [7] and Christak et al. [8] tracked user mobility patterns to model and evaluate epidemic sickness. Tizooni et al. [9] explored the use of proxy systems for individual users. The authors evaluated the mobility flow to predict the spread of epidemics. The accuracy of the predictive analysis, which was performed using mobility data sources, varied with the epidemic rate of propagation and timing of data results gathered.

Salathe et al. [10] discussed the use of wireless technologies, such as the ZigBee protocol and Bluetooth, to detect and trace infected people. The authors obtained detailed data on the social contacts of infected persons during the infection period. Then, the authors recreated the social networks of potentially infected users. To evaluate the spread, diffusion, and impact, the authors also proposed the SEIR model based on features such as susceptible, exposed, infectious, and recovered. Mastrandrea et al. [11] presented a prototype of wearable sensors for determining contacts amongst individuals and students. The authors matched the results with contacts from personal records, and associated the spread of an epidemic using sensors and diaries with a notable difference in dynamics. Interest in contact-tracing strategies has increased in recent times, and different methods have been used to estimate the impact and rate of spread before and during the plagues, as well as the efficiency of measures against contiguous epidemics. In many outbreaks, contact tracing is the only feasible option to identify infected individuals, as presented by Lima et al. [12], Rubrichi et al. [13], and Fraser et al. [14], who also tested reasons that aid in controlling an outbreak.

Contact tracing methods adopt two primary models, namely, population-based and agent-based approaches. Klinkenberget et al. [15] proposed a population-based top-down approach for analyzing system research data from a macroscopic perspective. Then, Kwok et al. [16] and Müller et al. [17] presented an agent-based bottom-up approach, considering every individual as a self-regulating agent entity. Each agent is responsible for its own infection state, movement, and location to estimate unrelated and adaptive activities. The stochastic model introduced by Farrahiet et al. [18] and Keelinget et al. [19] involves grouping the associated measures and fundamental dynamics of epidemics using a deterministic approach. In previous years, contact-tracing models have focused on a generic network of contacts. To improve the precision of such network contact models, Huerta et al. [20] presented a similar model as part of the epidemic regulation tactics. This method helped to estimate the impact of contact tracing and the random tracing of complex contact networks. Yang et al. [21] proved that by tracing the contacts at a low additional cost, the spread of an outbreak may be considerably reduced, and even eradicated. The FluPhone project developed at Cambridge University [22] was one of the first attempts to use mobile apps to determine contacts. Using wireless Bluetooth as a proxy, the application was able to estimate physical contacts. The application promoted users to report symptoms to determine the rate and risk of infection. Similar contact tracing schemes focus on privacy issues, such as the pan-European privacy-preserving proximity tracing (PEPP-PT) [23] and the MIT project Safe Paths [24]. Corporate enterprises such as Apple, Facebook, and Google teamed up to integrate their web portals with handheld and sensor devices to provide similar solutions for Android and iOS mobiles. Isella et al. [25] claimed that the practice of contact tracing and isolation did not prevent the COVID-19 epidemic. The decreasing infection count is primarily due to asymptomatic infected individuals who are undetected, and who it is believed contribute to the spread of the COVID-19 outbreak. Using mobile apps to find previous contacts, we mathematically proved that such epidemic diseases can be checked even when no one uses the mobile application.

3 Proposed Framework: CTF

A real-time contact tracking framework (CTF) was designed and developed as a secure mobile application using the Android platform, SDK tools, and Java. Instead of using a data network or IT infrastructure such as wireless or office networks, the lightweight application uses Bluetooth with the need for limited computing resources of the individual's mobile. However, there are unauthorized and malicious privacy impacts from threat vectors. The CTF process is trust-based; individuals own the process, and it is his/her prerogative to join or exit, and further perform regular 15 days self-assessment to determine any infection. The generated logs comprise a unique ID (user's Bluetooth), timestamp (date and time), and health status code (random salted number) for each application user. The contract tracking framework follows five phases, as shown in Tab. 2.

Entities involved in the CTF process require privacy protection. These include individuals (mobile IMEI and number), location (IP address and geolocation), health data, and command server communication. The proposed CTF application ensures that the data collected is never shared with any of these entities, and keeps the individuals anonymous. The proposed workflow is shown in Fig. 2.

Table 2: Phases of contract tracing framework

Phase	Description
Installation	Interested individuals are required to opt-in to join and install the secure contact tracing application. Only users of Android operating systems can currently install and use this application.
Operation	Each installed app enables Bluetooth, records the individual information, and encrypts the log on the mobile SD card locally.
Report generation	Opt-in individuals are provided with two types of reports–detailed and basic. The basic level report is uploaded to the command server and is encrypted with a public key with their consent, while the detailed report is encrypted with the private key.
Handling self infection	Infected individuals can use the detailed report to contact medical teams and anonymously receive support. No location or mobile details are shredded by the app.
Handling other's infection	App scans and checks others Bluetooth beacons and checks the other's basic report using their public keys. This indicates the presence of another infected individual in the physical vicinity of 8 to 10 m, and proximity alerts are generated. The basic report presents only the status code, and no personal information is shared. The process ensures that an infected individual stays anonymous.
Analytic option	Depending on the individual's consent, the detailed report and data generated are provided to medical analytics teams for further research.
Graceful removal	Individuals opting out or who are not COVID-19 positive need to just click and select the option, the app would gracefully uninstall and remove all logs and encryption keys.

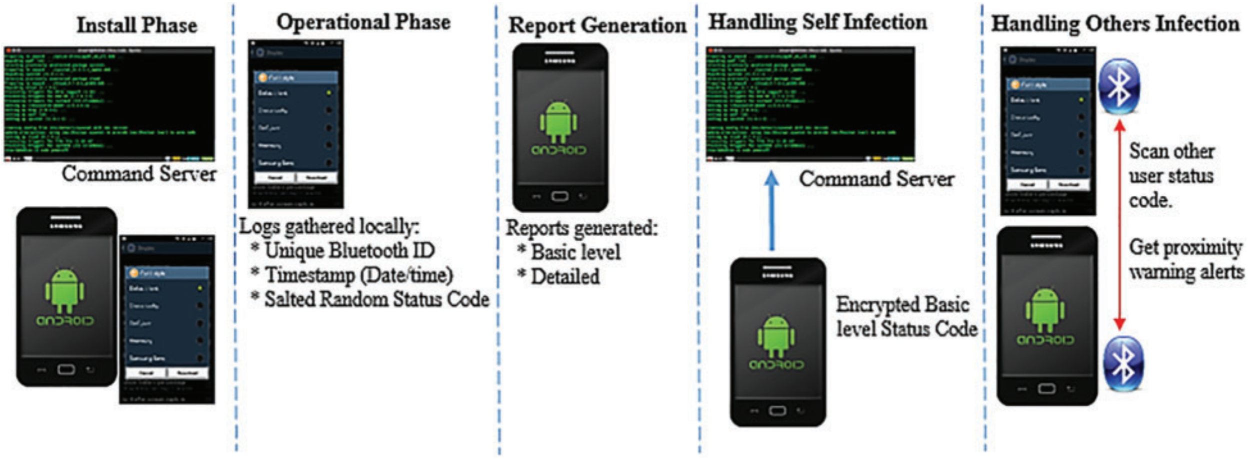


Figure 2: Process flow for secure contact tracing framework

This application was designed for Android mobile devices. The reports are saved locally on the mobile, and are encrypted with a private key in the form of two reports. The first report is a detailed description accessible only to individuals. If the individual is infected, he can share with the medical teams all of the details in full confidence using a private key in order to determine the treatment. The second report is a basic-level code encrypted with a public key and uploaded to the command server. Whenever an individual goes outside, the application scans other mobile devices using Bluetooth. This sends and receives anonymous encrypted beacons to and from other mobile devices. If the application can decrypt the basic report of other individuals, Bluetooth alerts are generated immediately.

3.1 *Bluetooth Beacons*

- Should not reveal any personal information, location, reports, or other individual information.
- While scanning, any personally identifying information should not be revealed to other users.
- Should be arranged, encrypted with a symmetric key to prevent any log being revealed to any other user.
- Should be randomly generated every 24 h to prevent the identification of transmitted information.

3.2 *Uninfected Individuals*

These are individuals who were or are infected, and who are never:

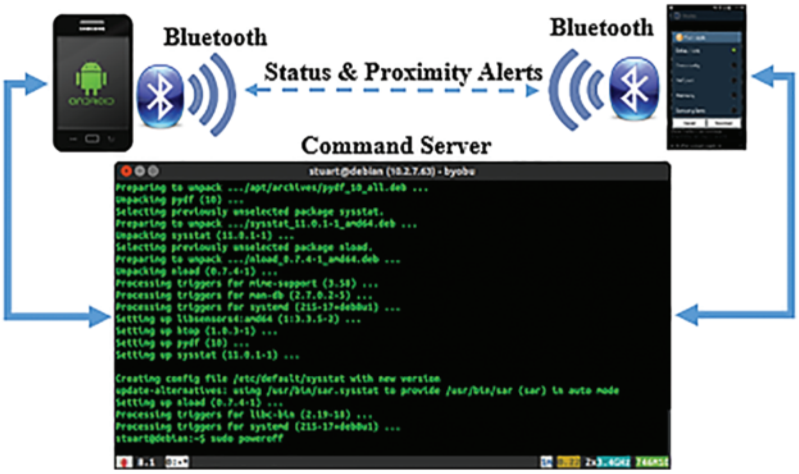
- Mandated to upload their details on the command server.
- Notified by the command server to verify potential contact with other non-infected.
- Receive medical certificate encrypted with medical teams' public key.

3.3 *Infected Individuals*

These are individuals who are infected:

- Are given the option to opt-in so that others can determine if they are near to any infected user.
- Can check if they are close to others or those who opted to join.
- Can stay anonymous even from the admin teams of the command server.
- Can find an infected user and determine when or where the actual contact happened.
- Should be assured of their IMEI number or MAC address.
- Can use the TOR browser to upload or download their logs and reports, thus remaining anonymous.

These alerts warn about an infected person in an individual's proximity. This indicates the presence of an infected individual within a range of 8–10 m. The flow of the secure contact tracing process is shown in Fig. 3. In this case, the user should then proceed to be tested. This process is anonymous, and no information about the individual is shared with the command server or other individuals. Individuals can opt-in or opt out as the process is trust-based. Only those who shared the reports on the command server and individual infections were verified using Bluetooth. The authors formally prove that the application guaranteed privacy-sensitive features and trust verification for the individuals observed correctly. The following features were considered when designing the framework.



```
Preparing to unpack .../apt/archives/pydf_10_all.deb ...
Unpacking pydf (10) ...
Selecting previously unselected package sysstat.
Preparing to unpack .../sysstat_11.0.1-1_amd64.deb ...
Unpacking sysstat (11.0.1-1) ...
Selecting previously unselected package sload.
Preparing to unpack .../sload_0.7.4-1_amd64.deb ...
Unpacking sload (0.7.4-1) ...
Processing triggers for mime-support (3.58) ...
Processing triggers for man-db (2.7.0.2-5) ...
Processing triggers for systemd (215-17+deb8u1) ...
Setting up libsensors4:amd64 (1:3.3.5-2) ...
Setting up htop (1.0.3-1) ...
Setting up pydf (10) ...
Setting up sysstat (11.0.1-1) ...

Creating config file /etc/default/sysstat with new version
update-alternatives: using /usr/bin/sar.sysstat to provide /usr/bin/sar (sar) in auto mode
Setting up sload (0.7.4-1) ...
Processing triggers for libc-bin (2.19-18) ...
Processing triggers for systemd (215-17+deb8u1) ...
stuart@debian:~$ sudo poweroff
```

Figure 3: Bluetooth and command server communication

3.4 Proposed Algorithm: CTF

Algorithm 1 presents the proposed secure application workflow and the CTF process. Tab. 3 lists the notations used in the proposed algorithm.

Table 3: Notations in proposed algorithm

U	Exposed individuals to hotspots, infected victims or have travel history
X	Individual under contact tracing
T	Individuals with travel history
I (App)	Install proposed contact tracing application
S (Mon)	Individuals who are self-monitoring for 15 days
L	Application log generated (User ID, Timestamp, Code)
U	Unique Bluetooth ID → generated from user's Bluetooth
T	15-min timestamp → date/time of log from mobile device
C	Code → Sorted random number for individual status
R1	Individual's detailed private report
R2	Basic level public report (Infected or not)

Algorithm 1: Contact Tracing Framework (CTF)

```
1. Start
2. Assuming U(i) = Exposed individual with exposure to corona hotspots, infected victims, or travel history
3. $U(i)^n = \sum_{k=0}^{n} \binom{n}{k} X^k T^{n-k}$
4. I(App) = Install proposed contact tracing application & S(Mon) = perform self-monitoring for 15 days
```

(Continued)

```
$|\mathrm{I(App)}| = \begin{cases} \mathrm{True,} & \mathrm{X(i)} \\ \mathrm{False,} & X(i) \end{cases}$ and $|\mathrm{S\,(Mon)}| = \begin{cases} \mathrm{True} \to \mathrm{X\,(i)} \le 15\ \mathrm{days} \\ \mathrm{False} \to X\,\mathrm{(i)} < 15 days \end{cases}$
L = Application log generated (User ID, Timestamp, Code)
$\mathrm{L\,(i)} = \sum \{\mathrm{U^n} + \mathrm{T^n} + \mathrm{C^n}\}$
E = Encrypted Log {L} stored locally on user's mobile SD Card, encrypted with symmetric private Key
if Symptoms Detected = False
    Confirm no symptoms
    No follow-up or review required
    U(i) = User can opt-out & uninstall application
Else
    Consider case = Suspected
    Isolate and use personal protection equipment
    Provide user option to open-in or opt-out
Endif
if U(i) = opt-out
    Exit
Else
U(i) = opt-in
    Receives Private Key from Command Server
    Encrypts and Upload logs to Command Server
    Encrypted info available on Server Portal
Endif
U(i) receives two reports → R1(i) & R2(i)
U(j) are other individuals reporting infection also receive similar decryption keys & reports
App on U(i, j) constantly check for decryption of other's basic report, duration (15 min/24 h)
if U(j) → Decrypt R1(i) = Success
    if U(i) within range
        U(i) Bluetooth → Generate Proximity Alert
        U(i) and U(j) →in vicinity of infected user or maybe infected
        Recommend Lab Testing
        Access Lab Results
    Endif
Endif
if Results R(i) = Negative
    Download Covid19 free certificate
    Stop Contact Tracing
    Exit
Else
    if R(i) = Positive
        Confirmed Case
        Isolation for 15 days
        Recheck Lab Testing
    Endif
Endif
if U(I, j) = exit and opt-out
    U(i)opt-out & Delete L(i) ± Exit_App = Graceful Uninstall
Endif
End
```

The proposed contact detection runs as a service utilizing Bluetooth beaconing. This confirms the proximity detection of data exchange with nearby phones, even as the advertisements are non-connectable and undirected. Fig. 4 illustrates the flow of advertisements between the application and remote Bluetooth devices. Contact detection and advertisement services are run on devices with a Bluetooth 16-bit UUID 0 x FA5F to enable proximity sensing between devices. Devices advertise and scan using a 128-bit proximity identifier that is periodically modified. Each advertisement scan is timestamped, and the discoverable bit is initially set to 1 and captured. The scan interval window is 5 min, which is sufficient to provide the discovery of advertisers and coverage. The advertiser address and proximity are changed so that they cannot be linked in any way. The advertising intervals are changed every few hundred milliseconds. The scanning internal window performs periodic sampling for every few minutes.

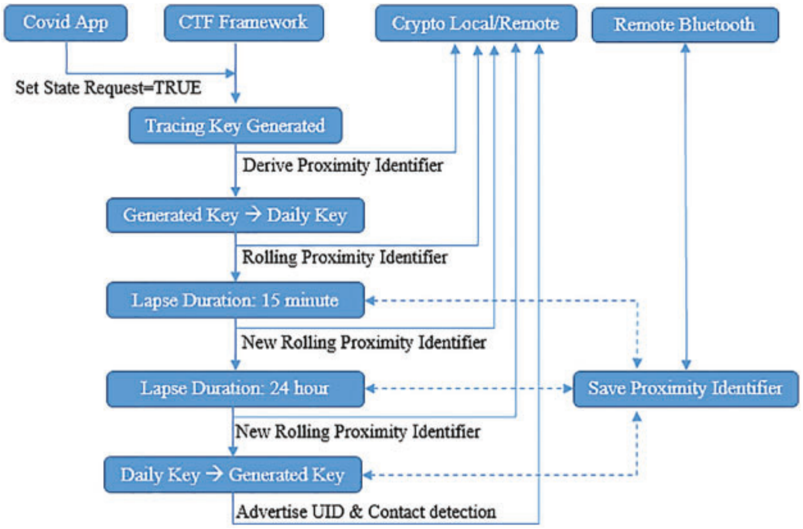

Covid App
CTF Framework
Crypto Local/Remote
Remote Bluetooth
Set State Request=TRUE
Tracing Key Generated
Derive Proximity Identifier
Generated Key → Daily Key
Rolling Proximity Identifier
Lapse Duration: 15 minute
New Rolling Proximity Identifier
Lapse Duration: 24 hour
Save Proximity Identifier
New Rolling Proximity Identifier
Daily Key → Generated Key
Advertise UID & Contact detection

Figure 4: Dataflow for advertisement between mobiles

Fig. 5 illustrates the dataflow process and behavior for the device scans, which ensure that privacy is maintained as the most critical specification while designing the application. This is utilized with the Bluetooth protocol, which is location independent, yet it uses the Bluetooth beacon to detect the device proximity. The user proximity ID correlates and obtains IDs of other devices every 15 min. This reset window reduces the loss from privacy advertisements and is processed exclusively on the local device. If any user is detected to have COVID-19 symptoms, the user can consent to the sharing of the diagnosis keys with the main server. Thus, users have control and transparency regarding their participation for contact tracing. These precautions are implemented in the framework design to ensure user privacy.

4 Experimental Results

The results varied between randomly selected individuals and those infected. Moreover, this research considered different time slots during which users turn ON their Bluetooth to evaluate the effectiveness of our protocols in different scenarios. The validations were repeated to capture the randomness of the simulations for 150 devices.

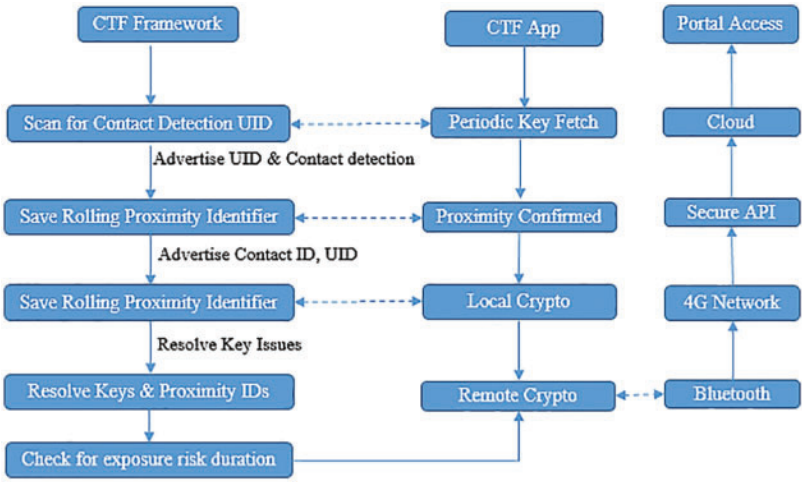

CTF Framework
Scan for Contact Detection UID
Advertise UID & Contact detection
Save Rolling Proximity Identifier
Advertise Contact ID, UID
Save Rolling Proximity Identifier
Resolve Key Issues
Resolve Keys & Proximity IDs
Check for exposure risk duration
CTF App
Periodic Key Fetch
Proximity Confirmed
Local Crypto
Remote Crypto
Portal Access
Cloud
Secure API
4G Network
Bluetooth

Figure 5: Dataflow and behavior of device scan process

Initial research focused on the infection rate among individuals depending on the initial infection and contagiousness probability. These datasets were obtained from infections reported by individuals who had installed the contact tracing application, and who were using it.

Subsequent research focused on three scenarios (i1–i3) as follows:

- i1: Individuals who randomly turn ON/OFF their Bluetooth anytime
- i2: Individuals who turn ON Bluetooth when outside their homes, in a market, or in crowded places
- i3: Individuals who turn ON their Bluetooth only at specific hours and for set durations.

The authors conducted a parametric statistical t-test and regression analysis to ensure that the datasets had no violations of the information presented in random samples from 100,000 records. The use of regression validated the prediction of continuous dependent variables from independent variables in the datasets. The deviations from the linear point line are the errors. The distribution of the sample mean is normal, and the variances of the different parameters are similar. The null hypothesis assumes that if the data violate these assumptions, then it can be safely assumed that the results obtained have committed a Type I error, which is more or less than the alpha probability, and the T-Test validation parameters are interpreted as presented in Tab. 4.

Table 4: Test validation parameters

T	T-Test
DF(x)	Degree of freedom from samples
x.xx	Calculated value as ‘T-Static’
$p \leq 0.05$	$A \neq B$ → Not likely to be result by chance which implies → Difference is significant → Null hypothesis is incorrect Null is rejected → relationship between A and B
$p \geq 0.05$	$A = B$ → Likely chance which implies no significant difference → Null hypothesis is correct Fail to reject the null → no relationship between A and B

The requirement for performing the T-Test is the use of two independent samples with normally distributed data and samples with the same variance. The authors take the null hypothesis, H0: H1 − H2 = 0, where H1 and H2 are the means for the two datasets. The null hypothesis is that there is no difference between the means of the two datasets, or more formally, that the difference is zero. Tab. 5 presents the T-test validation of the CTF dataset sample.

Table 5: Infection count (in thousands) for three options

Probability percentage (%)	Infection count observed on individuals		
	Randomly turn ON bluetooth (i1)	Only when outside homes, market place (i2)	Only at certain specific hours and duration (i3)
0	5	11	18
10	11	17	31
20	13	26	39
30	19	34	47
40	21	43	55
50	24	49	66
60	28	53	73
70	31	57	79
80	34	65	83
90	37	74	88
100	39	79	91

Considering the datasets for i1 and i2, the authors used a significance level of 0.05 with a two-tailed hypothesis. The difference scores that were calculated are presented in Tabs. 6 and 7 below.

Table 6: Difference scores for i1 dataset

i1	*Diff* $(X - M)$	Sq. Diff $(X - M)^2$
5	−18.82	354.12
11	−12.82	164.31
13	−10.82	117.03
19	−4.82	23.21
21	−2.82	7.94
24	0.18	0.03
28	4.18	17.49
31	7.18	51.58
34	10.18	103.67
37	13.18	173.76
39	15.18	230.49
	M: 23.82	**SS: 1243.64**

Table 7: Difference scores for i2 dataset

i2	*Diff* $(X - M)$	Sq. Diff $(X - M)^2$
11	−35.18	1237.76
17	−29.18	851.58
26	−20.18	407.31
34	−12.18	148.4
43	−3.18	10.12
49	2.82	7.94
53	6.82	46.49
57	10.82	117.03
65	18.82	354.12
74	27.82	773.85
79	32.82	1077.03
	46.18	**SS: 5031.64**

T-Test calculations are performed for validation on datasets, and are presented in Tabs. 8 and 9.

Table 8: Test calculation for i1 dataset

N_1: 11
$df_1 = N - 1 = 11 - 1 = 10$
M_1: 23.82
SS_1: 1243.64
$s_1^2 = SS_1/(N - 1) = 1243.64/(11 - 1) = 124.36$

Table 9: Test calculation for i2 dataset

N_2: 11
$df_2 = N - 1 = 11 - 1 = 10$
M_2: 46.18
SS_2: 5031.64
$s_2^2 = SS_2/(N - 1) = 5031.64/(11 - 1) = 503.16$

For T-Value Calculation:

$s_p^2 = ((df_1/(df_1 + df_2)) * s_1^2) + ((df_2/(df_2 + df_2)) * s_2^2) = ((10/20) * 124.36) + ((10/20) * 503.16) = 313.76$
$s_{M1}^2 = s_p^2/N_1 = 313.76/11 = 28.52$
$s_{M2}^2 = s_p^2/N_2 = 313.76/11 = 28.52$
$T = (M_1 - M_2)/\sqrt{}(s_{M1}^2 + s_{M2}^2) = -22.36/\sqrt{}57.05 = -2.96$

T-value is -2.96089 and the P-value is 0.007726 → Result is significant at $p < 0.05$.

Because the P-value is less than the significance level, alpha 0.05 → Null Hypo (H0) is rejected and the Alternative Hypo (Ha) is accepted.

Further, validating with regression analysis:

Sum of $X = 262$
Sum of $Y = 508$
Mean $X = 23.8182$
Mean $Y = 46.1818$
Sum of squares $(SS_X) = 1243.6364$
Sum of products $(SP) = 2485.3636$

Regression Equation = $\hat{y} = bX + a$

where $b = SP/SS_X = 2485.36/1243.64 = 1.99846$, and $a = M_Y - bM_X = 46.18 - (2{*}23.82) = -1.41798$
$\hat{\mathbf{y}} = \mathbf{1.99846}\ X - \mathbf{1.41798}$

From the graph shown in Fig. 6 below, individuals who randomly turn on their Bluetooth when going out or in crowded places display better performance and contagiousness probability than those who turn on Bluetooth only when outside their homes or only at certain specific hours of for a set duration.

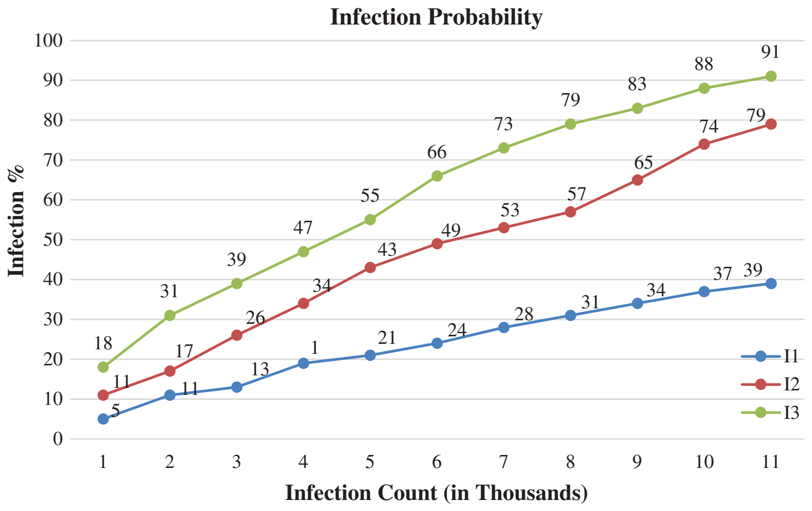


Figure 6: Infected users *vs*. contagiousness probability

5 Conclusion

The presented research work successfully demonstrates the real-time, trust-based contact tracing framework (CTF) as a feasible privacy-aware solution. Nation-states need not use methods or applications that pose privacy-related risks or face issues when an individual's personal information or health logs can be misused. This study considers the features and entities that are related to protecting the privacy of an individual. The focus is to build a trust-based framework with a lightweight Bluetooth-based mobile application. Using sample datasets, the authors have shown how contact tracing with three options can mitigate the spread of COVID-19. Existing contact tracing applications do not provide open-source software for research or experimentation purposes. In the future, the authors plan to release this research as an open-source software implementation for both Android and iOS devices.

Funding Statement: The author would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project No. R-2021-131.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] E. K. Jeong, O. Park and Y. J. Park, "COVID-19 national emergency response center, epidemiology and case management team, Korea centers for disease control and prevention. Coronavirus disease-19: The first 7,755 cases in the Republic of Korea," *Osong Public Health and Research Perspectives*, vol. 11, pp. 85–90, 2020.

[2] R. Li, S. Pei, B. Chen, Y. Song, T. Zhang *et al.,* "Substantial undocumented infection facilitates the rapid dissemination of novel coronavirus (SARS-CoV-2)," *Science*, vol. 368, no. 6490, pp. 489–493, 2020.

[3] B. C. de Jong, B. M. Gaye, J. Luyten, B. van Buitenen, E. André, *et al.,* "Ethical considerations for movement mapping to identify disease transmission hotspots," *Emerging Infectious Diseases*, vol. 25, no. 7, 2019. https://doi.org/10.3201/eid2507.181421.

[4] B. C. de Jong, B. M. Gaye, J. Luyten, B. van Buitenen, E. André *et al.,* "Ethical considerations for movement mapping to identify disease transmission hotspots," *Emerging Infectious Diseases*, vol. 25, no. 7, pp. E1–E6, 2019.

[5] A. L. Barabási, "Network science," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 371, no. 1987, pp. 20120375, 2013.

[6] L. Chancay-Garcia, E. Hernandez-Orallo, P. Manzoni, C. T. Calafate and J. C. Cano, "Evaluating and enhancing information dissemination in urban areas of interest using opportunistic networks," *IEEE Access*, vol. 6, pp. 32514–32531, 2018.

[7] J. Dede, A. Förster, E. Hernández-Orallo, J. Herrera-Tapia, K. Kuladinithi *et al.,* "Simulating opportunistic networks: Survey and future directions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1547–1573, 2018.

[8] E. Christaki, "New technologies in predicting, preventing and controlling emerging infectious diseases," *Virulence*, vol. 6, no. 6, pp. 558–565, 2015.

[9] M. Tizzoni, P. Bajardi, A. Decuyper, G. K. K. King, C. M. Schneider *et al.,* "On the use of human mobility proxies for modeling epidemics," *PLOS Computational Biology*, vol. 10, no. 7, pp. e1003716, 2014.

[10] M. Salathé, M. Kazandjieva, J. W. Lee, P. Levis, M. W. Feldman *et al.,* "A high-resolution human contact network for infectious disease transmission," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 107, no. 51, pp. 22020–22025, 2010.

[11] R. Mastrandrea and A. Barrat, "How to estimate epidemic risk from incomplete contact diaries data?," *PLOS Computational Biology*, vol. 12, no. 6, pp. e1005002, 2016.

[12] A. Lima, V. Pejovic, L. Rossi, M. Musolesi and M. Gonzalez, "Progmosis: Evaluating risky individual behavior during epidemics using mobile network data," arxiv.org, 2015.

[13] S. Rubrichi, Z. Smoreda and M. Musolesi, "A comparison of spatial-based targeted disease mitigation strategies using mobile phone data," *EPJ Data Science*, vol. 7, no. 1, pp. 17, 2018.

[14] C. Fraser, S. Riley, R. M. Anderson and N. M. Ferguson, "Factors that make an infectious disease outbreak controllable," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 101, no. 16, pp. 6146–6151, 2004.

[15] D. Klinkenberg, C. Fraser and H. Heesterbeek, "The effectiveness of contact tracing in emerging epidemics," *PLOS One*, vol. 1, no. 1, pp. e12, 2006.

[16] K. O. Kwok, A. Tang, V. W. I. Wei, W. H. Park, E. K. Yeoh *et al.,* "Epidemic models of contact tracing: Systematic review of transmission studies of severe acute respiratory syndrome and middle east respiratory syndrome," *Computational and Structural Biotechnology Journal*, vol. 17, no. 1, pp. 186–194, 2019.

[17] J. Müller, M. Kretzschmar and K. Dietz, "Contact tracing in stochastic and deterministic epidemic models," *Mathematical Biosciences*, vol. 164, no. 1, pp. 39–64, 2000.

[18] K. Farrahi, R. Emonet and M. Cebrian, "Epidemic contact tracing via communication traces," *PLOS One*, vol. 9, no. 5, pp. e95133, 2014.

[19] M. J. Keeling, P. Rohani and B. Pourbohloul, "Modeling infectious diseases in humans and animals: Modeling infectious diseases in humans and animals," *Clinical Infectious Diseases*, vol. 47, no. 6, pp. 864–865, 2008.

[20] R. Huerta and L. S. Tsimring, "Contact tracing and epidemics control in social networks," *Physical Review E*, vol. 66, no. 5, pp. 4, 2002.

[21] H. X. Yang, W. X. Wang, Y. C. Lai and B. H. Wang, "Traffic-driven epidemic spreading on networks of mobile agents," *Europhysics Letters*, vol. 98, no. 6, pp. 68003, 2012.

[22] R. Raskar, "Apps gone rogue: Maintaining personal privacy in an epidemic," [Online]. Available: https://montrealethics.ai/research-summary-apps-gone-rogue-maintaining-personal-privacy-in-an-epidemic/, Retrieved January 12, 2021.

[23] E. Yoneki, Computer Laboratory Systems Research Group, 2019. [Online]. Available: https://www.cl.cam.ac.uk/research/srg/netos/projects/archive/fluphone2/, Retrieved January 4, 2021.

[24] PEPP-PT, "Pan-european privacy-preserving proximity tracing," Pepp-Pt, 2020. [Online]. Available: https://scholar.google.com/scholar?hl=en&as_sdt= 0%2C5&q=Pan-European+Privacy-Preserving+Proximity+Tracing&btnG=.

[25] R. Raskar and K. Esvelt, "Private kit: Safe paths; privacy-by-design," 2020. [Online]. Available: https://safepaths.mit.edu/, Retrieved February 16, 2021.