

Received November 14, 2020, accepted November 20, 2020, date of publication November 24, 2020,
date of current version December 9, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3040198

An Automated Contact Tracing Approach for Controlling Covid-19 Spread Based on Geolocation Data From Mobile Cellular Networks

MD. TANVIR RAHMAN¹, RISALA T. KHAN², (Member, IEEE),
MUHAMMAD R. A. KHANDAKER³, (Senior Member, IEEE),
MATHINI SELLATHURAI³, (Senior Member, IEEE),
AND MD. SIFAT A. SALAN⁴

¹Department of Information and Communication Technology, Mawlana Bhashani Science and Technology University, Tangail 1902, Bangladesh

²Institute of Information Technology, Jahangirnagar University, Dhaka 1342, Bangladesh

³School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, U.K.

⁴Department of Statistics, Mawlana Bhashani Science and Technology University, Tangail 1902, Bangladesh

Corresponding author: Muhammad R. A. Khandaker (m.khandaker@hw.ac.uk)

This work was supported by the EPSRC under Project EP/P009670/1.

ABSTRACT The coronavirus (COVID-19) has appeared as the greatest challenge due to its continuous structural evolution as well as the absence of proper antidotes for this particular virus. The virus mainly spreads and replicates itself among mass people through close contact which unfortunately can happen in many unpredictable ways. Therefore, to slow down the spread of this novel virus, the only relevant initiatives are to maintain social distance, perform contact tracing, use proper safety gears, and impose quarantine measures. But despite being conceptually possible, these approaches are very difficult to uphold in densely populated countries and areas. Therefore, to control the virus spread, researchers and authorities are considering the use of smartphone based mobile applications (apps) to identify the likely infected persons as well as the highly risky zones to maintain isolation and lockdown measures. However, these methods heavily depend on advanced technological features and expose significant privacy loopholes. In this article, we propose a new method for COVID-19 contact tracing based on mobile phone users' geolocation data. The proposed method will help the authorities to identify the number of probable infected persons without using smartphone based mobile applications. In addition, the proposed method can help people take the vital decision of when to seek medical assistance by letting them know whether they are already in the list of exposed persons. Numerical examples demonstrate that the proposed method can significantly outperform the smartphone app-based solutions.

INDEX TERMS Coronavirus, Covid-19, contact tracing, geolocation, pandemic.

I. INTRODUCTION

After World War II, the coronavirus (COVID-19) is being considered to be the most life-threatening event that happened in the history of mankind. It is a new family of coronavirus that changes its RNA structure frequently. As the virus had spread all on a sudden and the spread rate could not be predicted in prior, only a few countries have been able to control the penetration of this virus. The main reason behind

The associate editor coordinating the review of this manuscript and approving it for publication was Derek Abbott¹.

their successful control was the ability to trace the contacts of the infected persons promptly and put them into isolation [1]. To slow down the coronavirus spread, three measures have been proven effective: i) contact tracing, ii) social distancing, and iii) quarantine. In particular, contact tracing plays a leading role in containing the spread when the R-value is below 1.0. Since the outbreak began, different countries adopted different types of contract tracing strategies based on their socio-economic conditions. A vast majority of these methods operate through smartphone-based mobile apps. According to the statistical portal, it has been found that in 2019 almost

5.07 billion people in the world are using mobile phones as a medium of communication and an estimated 67% of the world population has a mobile phone. The statistics also reports that in 2014 the smartphone users were around 38% which increased to 50% by the end of 2018. It has been reported that the number of smartphone users worldwide today surpasses three billion [2]. From this growth, it is expected that the number of smartphone users will grow by one billion in a period of five years [3], [4]. Therefore, contact tracing can be easily done using mobile phone apps but the challenge is how the collected data can be handled securely and what information should be collected [5]. In addition, people's willingness to install the apps as well as the availability of smartphones in all areas of a society is also a major challenge. According to Ferretti *et al.* [6] and Zastrow [7], if 60% of the population of a country install the contact tracing app, the spread rate will automatically slow down. After collecting the data, the next obvious question is how to warn people effectively. Many approaches are now under consideration such as contact tracing, narrowcasting, broadcasting, and so on to alert people regarding the possibility of being infected or tracing the likely infected person's contact trajectory [8]. Accurate contact tracing data is vital for providing timely exposure notices. For that purpose, users' personal information such as mobility, details of the persons the suspected user contacted, etc. has to be disclosed. The app can provide the data with reliable accuracy only if the collected information is sufficient. But more information leads to increased breach of privacy which is a major concern these days. For a clear understanding of the privacy concerns related to smartphone app-based contact tracing, one needs to know how such apps operate in practice. A typical contact tracing app works as follows: the app should be installed on an individual's cell phone and the Bluetooth of the phone must always remain on. When two users, having the same app installed, reach in close proximity, the app exchanges a unique identifier using Bluetooth which is stored either in the phone storage or in a centralized database. If a person is found to be COVID-19 positive, his mobile is taken to collect all the mobile numbers that had so far been stored in this mobile, and then those persons are informed as soon as possible. However, the authors in [9] raised some valid questions regarding the method being used in the Bluetooth-based contact tracing app, such as, how the anonymity of a user be protected from the app provider, how to prevent the snooper to access individual's data through this app, what measure the authority will take in case of contacted persons after knowing their details and so on. Therefore, not only finding the infected or likely infected person is enough but how to inform them or what measures should be taken to confine them is also important in the pandemic situation. In addition, solutions that seem effective for some countries may not be appropriate for other countries due to different social norms.

To address the aforementioned challenges in smartphone app-based contact tracing of COVID-19, we propose the idea

of using mobile phone users' geolocation data, as opposed to Bluetooth low energy (BLE) based smartphone apps, for contact tracing. The proposed framework facilitates contact tracing without necessitating smartphones. Since in many countries especially in developing countries smartphone penetration rate is significantly low, BLE based technology may not be very effective in those countries. In the geolocation based approach proposed in this article, any type of mobile phone with an active SIM card will work and thus the proposed approach can be equally effective in developing countries as well as in countries where smartphone penetration rate is significantly higher. The proposed approach can be considered as a technology aided concept that can minimize the spread of the deadly Coronavirus yet preserving the privacy of the users. In this work, we have also demonstrated practical benefits of using cellphone networks as a medium of contact tracing. The procedure is detailed in the following sections.

Meanwhile, the rest of this article is organized as follows: Section II presents an extensive review of existing systems, Section III focuses on the details the proposed model, Section IV compares the proposed model with existing systems from different viewpoints, then, experimental results are presented in section V. Finally, conclusions are drawn in section VI.

II. REVIEW OF EXISTING SYSTEMS

After the declaration of WHO as COVID-19 outbreak a public health emergency of international concern (PHEIC) on 30th January 2020 [10], [11] and a pandemic on 11th March 2020 [12], many countries developed different contact tracing apps to monitor and control the spread in the country. According to a CNN report, the Health Code app [13] that is being used in many parts of China works as follows: the app asks people about their symptom as well as their travel history, the possibility of being in contact with a COVID-19 positive patient, their workplaces, residential addresses, phone numbers, passport numbers, national identity number, etc. will be verified. After verification, a color code will be sent to the person's mobile phone named as "QR Code" whose color can be either red, green or amber. Users with red code will have to go under government quarantine or self-quarantine for 14 days, users with amber code will go to quarantine for 7 days but users with green code are considered to be risk-free. The major problem in this app is if a person intentionally provides wrong information regarding his travel information or symptom or being in close contact with a COVID-19 positive patient, then he will get a green code and will likely affect more people before being identified.

South Korea was among the first few countries that were affected by the novel coronavirus after China. Hence, in South Korea, the first confirmed cases were reported on 20th January 2020 [14]. Even though in the initial stage the number of affected people in South Korea was quite high but they didn't go for any lockdown or roadblock or aggressive immigration control strategy. Rather they used a trace, test,

and treat strategy which proved very effective as within a short period the curve of newly confirmed cases, as well as deaths, had been flattened at around mid-March [15]. To control the spreading, the Government of South Korea sent all the travelers who came from abroad into self-quarantine. During the quarantine state, the travelers forcefully used a self-diagnosis app and updated their health status regularly so that the Government can trace whether there are any suspected symptoms [16]. At the same time, the government also sent all of the individuals who had direct contact with those travelers to self-quarantine as well and followed the same monitoring scheme. But the main problem in this tracing process arose when the collected data was shared among many authorities such as police, health insurance, central government agencies, health care professionals, health care associations, and others. Hence, it is a direct violation of data privacy law in South Korea [15]. But during the pandemic situation, such law can be relaxed and that was what South Korea did at that time. Besides, it was suggested that if such a situation happens again, aggregated data rather than an individual's can be shared to all the concerned sectors to control the misuse of data [15].

In March 2020, Singapore Ministry of Health first released a contact tracing app called "TraceTogether" and its BLE-based protocol BlueTrace [17] where the tracing will be done through mobile phones' Bluetooth technology. For tracking purpose, a person has to install the app, and Bluetooth must be turned on always. A unique token is generated in the person's mobile during installation. Whenever two persons are in close proximity their phone will exchange that token through Bluetooth and preserve that token number in the phone storage [18].

The Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) [19], a joint project between Germany, France and Italy, proposed a centralized data center based on Bluetooth low energy (BLE)-based tracing technique where any traveler travelling within EU countries can use the same app to let the government know his contacted persons' list without needing any additional contact tracing app.

There are several major problems in the BLE-based tracing systems following both centralized and decentralized approaches. First, if the person does not use a smartphone featuring Bluetooth connectivity, then there is no way he or she can be traced. We acknowledge that in a first world country like Singapore or Germany, most of the people use smartphones but not necessarily everyone keeps the Bluetooth connectivity enabled in his/her device at all time. Second, although Bluetooth technology is considered as a cheap, reliable, and low power consuming option, any malicious user may access the information stored in the mobile devices through the Bluetooth link [20]–[22]. In [21], Naveed *et al.* explained the security issues of using mobile Bluetooth technology for android devices and in [23] the authors showed the security issues in the iOS platform. Data privacy is thus a major concern in Bluetooth based apps. For any contact tracing app, the main goal is to inform the person that he or she

has been exposed to the virus. However, with Bluetooth-based apps, even if the person has not been in touch with any infected person but within the Bluetooth range of the person, the user of the phone will be flagged as a suspected one and may be subject to social bullying. It may also create a mass confusion if the number of such false alarm increases significantly. On the other hand, if we consider the scenario of a developing country like Bangladesh, Nigeria etc., where coronavirus is creating phobia among people as medical facilities to support the massive number of patients are not adequate and many hospitals are not even treating patients with other problems due to the suspicion of coronavirus, this type of contract tracing app will create mass panic rather than mass awareness and people will face social harassment.

In general, two types of data can be collected by using these apps, one is "proximity" which will show with whom the user has been in contact and "location" which will show in which area the user has roamed [8]. Both may cause false positive alarms and false-negative alarms [8]. A false-positive alarm will happen if the person who is identified being in contact either by location information or contact information may just pass the area at that time and didn't even come in direct contact with the infected person. A false-negative alarm means the app is failing to identify any suspected person which may happen due to many reasons as we have discussed earlier.

Interestingly, many existing works suggest decentralized solutions because less sensitive data can then be shared with central authorities and thus the end user's privacy can be preserved [24], [25]. However, the risk of the decentralized solution compared to the centralized solution is still a trade-off and beyond the scope of this work.

While most of the contact tracing apps are now using the BLE-based tracing technique, some researchers are also thinking about storing user's mobility information and only hand over this information only when found COVID-19 positive [26]. In terms of data security and privacy, this is more secure as logging the location without the contact's stored information is less private.

In [27], the authors proposed a Bluetooth based contact tracing app "CONTAIN" where they showed that the identity of the user will be completely anonymous and at the same time, they experimented different timing of turning the Bluetooth on (random, decentralized, centralized) of the mobile to compare the results. They found in their experimental results that even if the Bluetooth is turned on, only when the user goes to any public gathering, the performance of the app is better than if it is turned on randomly during different times of the day.

Most of the COVID-19 contact tracing apps released so far are based on location/ proximity-based contact tracing, location-based hotspot reporting, and self-reported symptom tracking [17], [19], [24]–[36]. On the other hand, if the location data can be obtained from cellular mobile phone networks, then the issues related to the BLE-based tracing technique can be eliminated as well as the technological

requirements (e.g. phones with Bluetooth and smart features) can be waived. The authors of [37] have proposed an outdoor location tracking technique of mobile devices in a cellular network. They have shown that the proposed technique is nearly 88% accurate. In urban areas, the tracking performance is the best with median accuracies of up to 112m. It is also found that the cellular systems show promising positioning performance in indoor environments as well [38]. The authors of [39] have presented field test results in different scenarios e.g., cell phone network location system, gps location system and Google location services for measuring the accuracy of mobile device based location services. They have found the highest accuracy of 3.20 meter with the gps based location services. A more recent study in [40] suggests that achievable positional accuracies of mobile geolocation data range from 1.90 to 2.26m (median 2.11m) in urban open areas. So, it can be concluded based on practical experimental data that geolocation measurement using mobile networks coupled with the GPS sensors of mobile phones can be accurate, reliable and efficient for COVID-19 contact tracing.

In this article, we propose a contact tracing approach using cellular sim card geolocation data as opposed to the BLE-based tracing techniques. In the proposed model, a confirmed COVID19 patient's mobile number will be passed to the corresponding mobile operator to find its mobility information for the past 7 days. The operator will use the geolocation information to trace the mobility as shown in Fig.1.

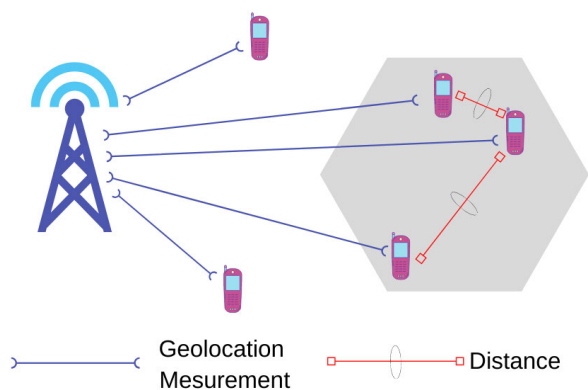


FIGURE 1. Contact tracing through cell phone network using geolocation data.

In the proposed model, no Bluetooth/ Wi-Fi/ NFC enabled cell phone is needed as the operator will use the geolocation-based tracing approach by getting the location data directly from the base station to identify the likely infected persons. This method can avoid panic spread among people as it does not require continuous warning about their possibility of getting infected. The responsible authority can then identify the riskiest persons based on the intensity of contact with Covid-19 positive patients and instruct them to go for isolation/test if necessary. In addition, if a person feels to have developed any symptoms of COVID-19, the proposed method can also perform an initial screening by

checking whether the cell phone number is enlisted in the list of victims.

III. PROPOSED CONTACT TRACING MODEL

In this section, we present the proposed cell phone geolocation-based contact tracing model. We structure the overall framework in three operational phases. Each phase has specific activities. The phases and their operations are discussed below. Note that there are some basic requirements for the proposed method. First of all, the patient has to carry a cell phone of any type with an active sim card and the sim card must belong to the patient. Secondly, the phone must be kept on.

A. PHASE-I : DATA COLLECTION

In this phase, the primary data for the COVID-19 patients will be collected from the designated test centers. Then the infected areas will be shown using any map services (e.g. Google map). The activities to be performed at this stage are described below and the process is depicted in Fig. 2.

1) STEP 01

Whenever a person visits a COVID-19 test center, two basic information, such as the current address and the active mobile phone number(s) must be recorded in the local register of the test center.

2) STEP 02

If the person is found to be COVID-19 positive, then the previously recorded information (i.e. address and phone numbers) must be reported to the central database.

3) STEP 03

At this point, the number of infected persons in an individual area (e.g. Division, District, City, Road, etc.) will be calculated.

4) STEP 04

An application will be in place (e.g. iOS or Android App, or Web Application, etc.) where anyone can do a simple registration with the mobile number. The registered user can search for a particular location and get the number of infected persons around it via any map services (e.g. Google map).

B. PHASE-II: IDENTIFYING PROBABLE OCCURRENCES

In the second phase, we focus on how the Government can identify the likely infected persons. The cell phone number of the Covid-19 positive patients can be traced to find out the possible occurrences as shown in Fig. 3. Here, any other cell phone user who came in near proximity (e.g. 2 meters) to the infected person during the last 7 days lies in the suspected list. But the mass people do not need to install any kind of application as the location data (latitude and longitude) will be collected from the cell phone network. Therefore, this process is not limited to the use of smart phones, rather we can get the data for any type of cell phone (e.g. feature phone) users. While collecting the location data, we have considered two cases. Firstly, when the infected persons travel within the

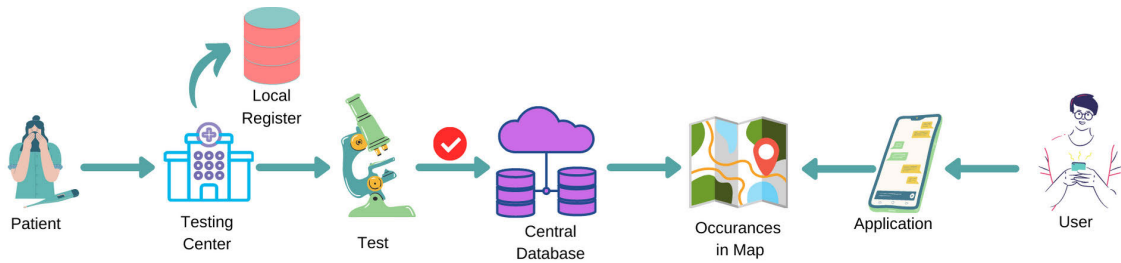


FIGURE 2. Flow diagram of Phase - I.

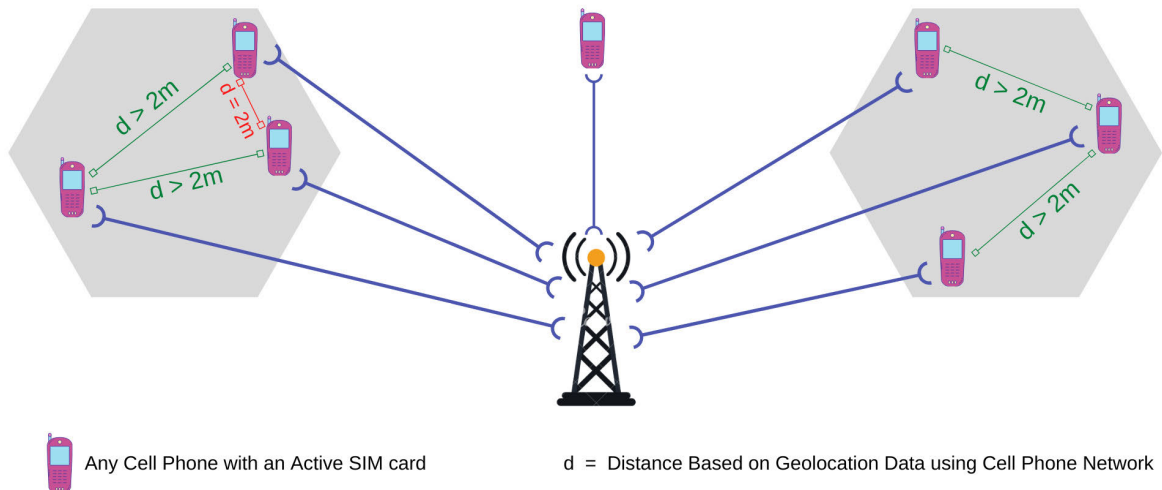


FIGURE 3. Finding possible occurrences using geolocation data from mobile phone operators.

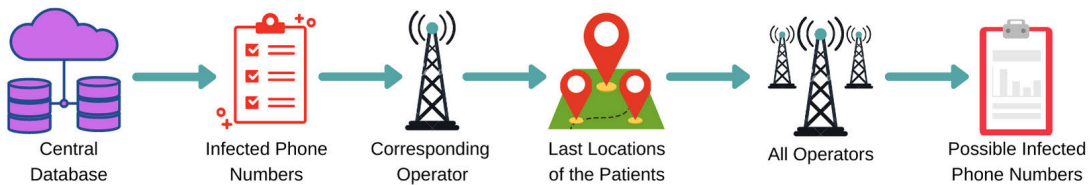


FIGURE 4. Flow diagram of Phase-II.

coverage of multiple BSCs (Base Station Controller) under the home MSC (Mobile Switching Centre), then authorities need to collect the data only from a single MSC owner. Secondly, when the infected persons travel between multiple different MSCs (Mobile Switching Center) owned by multiple service providers, the authorities may need to collect the complete travel data from all the relevant service providers. The step-by-step process is illustrated below, and the process is depicted in Fig. 4.

1) STEP 01

After getting the data (i.e. the list of infected persons) from the central database, each mobile number will be sent to the corresponding mobile operator to get the mobility information (latitude and longitude) of the respective cell phone users during the prior 7 days. At the same time, the operator will also be asked to provide the mobile numbers of the active cell phone users within those infected persons' mobility zones within a given distance.

2) STEP 02

The mobility zone information, acquired from the previous step, will then be sent to all other operators to identify all of the active cell phone users inside the zone at that time.

3) STEP 03

All the cell phone numbers (obtained from step 1 and 2) will be stored in the central database marked as "possible infected cell phone numbers".

4) STEP 04

If a particular number is found to appear multiple times in the "possible infected cell phone numbers" list, then those cell phone users will be instructed to go for isolation/ COVID-19 test as appropriate.

C. PHASE-III: USER'S QUERY

At this phase, if a person feels physically uncomfortable and wants to go for a test, the application can help to make the

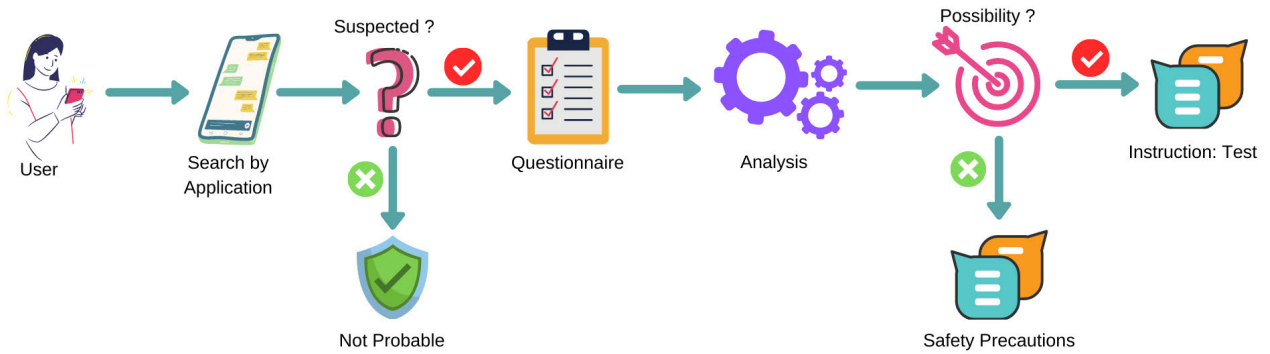


FIGURE 5. Flow diagram of Phase-III.

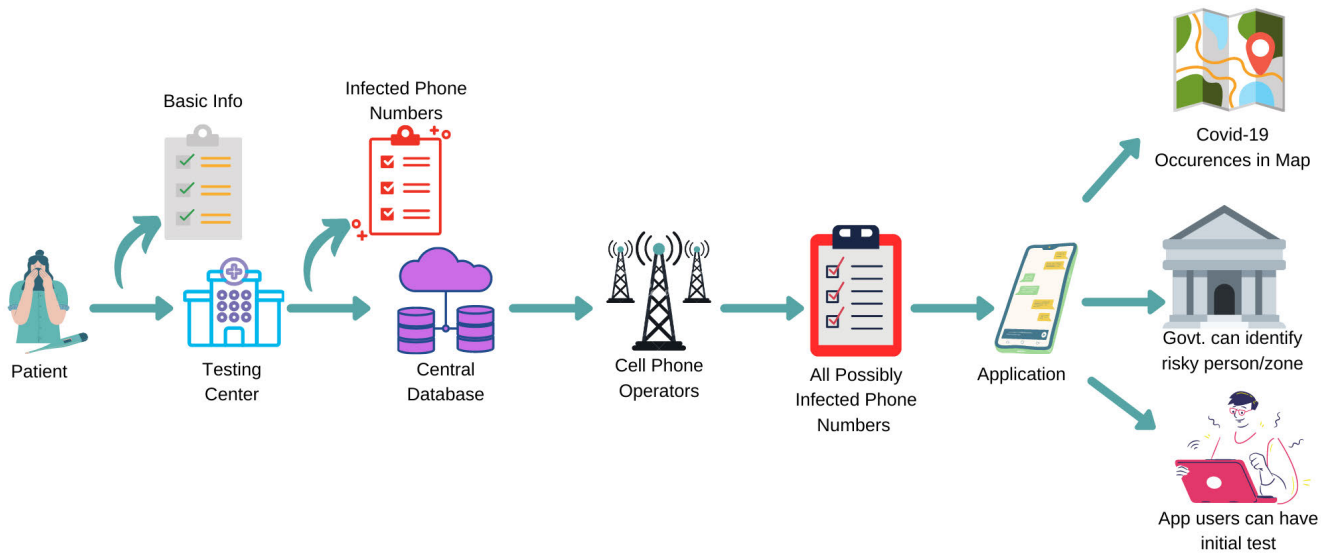


FIGURE 6. Overall flow diagram of the proposed system.

decision and predict the intensity. For this purpose, we propose activities as follows in stepwise and the process is depicted in Fig. 5.

1) STEP 01

Through the application, any person can search whether the corresponding cell phone number is enlisted in the suspected list.

2) STEP 02

If the cell phone user is already suspected by the application, the person will be instructed to answer some questionnaires which can be taken from [36], [37], [38]. The sample question set is shown in Table 1.

3) STEP 03

The answers will be verified and analyzed in real-time with a predefined answer set.

4) STEP 04

Finally, after the analysis, if the person is found to be possibly infected then the person will be instructed to go for a COVID-19 test.

TABLE 1. Sample questionnaire.

Sample Questions	Option-1	Option-2
1. New or worsening cough	Yes	No
2. Shortness of breath	Yes	No
3. Sore throat	Yes	No
4. Runny nose, Sneezing or nasal congestion	Yes	No
5. Hoarse Voice	Yes	No
6. Difficulty Swelling	Yes	No
7. Nausea/ Vomiting/ Diarrhea/ Abdominal pain	Yes	No
8. Unexpected Fatigue	Yes	No
9. Fever	Yes	No

These three phases are combined to form the proposed contact tracing method and the overall flow is depicted in Fig. 6. Note that relying on a centralised database may pose several security issues such as man in the middle (MITM), distributed denial of service (DDoS), SQL injection and so on. However, these threats are common for many centralized databases. We suggest the use of state-of-the-art defence mechanisms against any potential attacks. The authors of [41] have proposed a security model assessment prototype for databases, a prototype of security management architecture using blockchain for a database, a database security algorithm

and a prototype to mitigate cyberattacks. The authors have shown that the use of a hybrid blockchain model provides the system with the optimal security such that public organizations in relation to test results performed with a 99.50% security effectiveness. This model can be considered as a defence strategy for the proposed approach.

IV. COMPARISON WITH OTHER SOLUTIONS

The strongest aspect of the proposed contact tracing method is that it is not limited by advanced technological requirements (e.g. Smartphone, Bluetooth, Wi-Fi, NFC, and so on). The only requirement is that every individual has to carry the cell phone with an active sim card. With 5.112 billion unique mobile users, 67% penetration globally (even higher in urban areas where COVID-19 has the worst effect), mobile phone geolocation data seems to be the most viable means of contact tracing. Recently, a few articles have summarized different approaches proposed in the literature for minimizing the spread during this outbreak of COVID-19 [42], [43]. Most of the approaches are modern technology facilitated. The common approaches are broadcasting, selective broadcasting, unicasting, participatory sharing, private kit: safe paths, etc. Each of these approaches has its strengths and limitations. Raskar *et al.* have provided a detailed summary of the approaches named above [42]. We have reviewed the detailed comparison presented in [42] and analyzed different aspects of each method. The comparison of strengths and limitations of existing and the proposed methods is outlined in Table 2. The comparison factors are illustrated below as per the proposed model

A. ACCURACY

As the mobility information will be collected from the mobile operators, it is obvious that the data will be accurate. In the proposed model, we will not collect the locations verbally. As a result, we can say that the data will be precise and accurate.

B. ADOPTION

There will be no adaptability issue as the person does not need to carry out any predefined activity. People will continue their day-to-day activities, and what everybody does most of the time, they will carry their cell phones.

C. PRIVACY

The privacy issues are considered in the viewpoints of carriers, local businesses, users of the proposed model, and the non-users. These issues are discussed below:

1) PRIVACY RISK FOR CARRIERS

There will be no privacy risks for the carriers as the personal information will not be publicized. Only the infected count will be made public via any map services (e.g. Google map). While identifying the adjacent persons of a particular cell phone user, the location information will not be made public also because the proposed model works in a centralized

TABLE 2. Strength and limitation analysis with other proposed methods.

Model	Major Strengths	Major Limitations
Broadcast	<ul style="list-style-type: none"> No public adoption issues User’s privacy is protected Mostly accessible by all 	<ul style="list-style-type: none"> Significant privacy risk for Covid-19 carriers Data accuracy issue High risk of misinformation and mass panic
Selective Broadcast	<ul style="list-style-type: none"> Moderate privacy risk for COVID-19 carriers Mass panic may be limited 	<ul style="list-style-type: none"> Data accuracy issue Risk of misinformation Limited by technological requirements
Unicast	<ul style="list-style-type: none"> Low risk of mass panic Data accuracy is high 	<ul style="list-style-type: none"> No privacy for the user Not helpful for the mass people
Participatory	<ul style="list-style-type: none"> User’s privacy is protected from mass people 	<ul style="list-style-type: none"> There can be fraudulent activity Mass user adoption is low Full consent is needed from the COVID-19 carrier
Private Kit: Safe Path	<ul style="list-style-type: none"> Overall accuracy is high Moderate to low privacy risk for the COVID-19 carrier. 	<ul style="list-style-type: none"> Limited by technological requirements Full consent is required from the COVID-19 carrier
Proposed Solution	<ul style="list-style-type: none"> High accuracy of location data Users’ cell phones must not be smartphones rather any phone with an active sim card. To collect the data, no user application is needed Less false negative issue 	<ul style="list-style-type: none"> The user has to carry the cell phone

manner. The location data will be used only for predicting infection probability of the respective user.

2) PRIVACY RISK FOR LOCAL BUSINESSES

There will be very low privacy risks for the local businesses as the locations where the carrier visited will not be made public.

3) PRIVACY RISK FOR USERS

First of all, in every country, mobile service providers are regulated according to the privacy policies of the corresponding government. In the proposed method, when a patient is found Covid-19 positive, the system will only store the phone number of the patient which is accessible to the authorities for many other reasons. The proposed system does not require any other personal information (e.g. Name, Father’s Name, Mother’s Name, Bank Account, National ID Card (NID)

number etc.). After getting appropriate approval from the authorities, the system will then collect only the location points of the user during the last 7 days from the mobile phone operators. Thus, it is apparent that the privacy of the users will not be compromised as no personal information will be collected from the mobile service provider or from the mobile phone itself. On the other hand, in BLE based schemes, intruders may intercept sensitive private information through the Bluetooth connectivity.

4) PRIVACY RISK FOR NON-USERS

There may be privacy violations for the non-users as the users and non-users are somehow connected via social relationships, but this is common for other contact tracing methods as well. When a person is diagnosed as COVID-19 positive, the family members or friends may endure the same unintended consequences of the event.

D. CONSENT

The consent issues are considered in terms of the carriers, businesses and users of the proposed model. These issues are illustrated below:

1) CONSENT OF CARRIERS

The proposed model is considered to operate in such a way where the information about the patients will be recorded before the test of COVID-19. As a result, there will be no way to hide the details of the carrier afterward. Therefore, no consent will be needed as it is a casual and normal practice.

2) CONSENT OF LOCAL BUSINESSES

The consent of local businesses in the proposed model mainly depends on the Government policies.

3) CONSENT OF USERS

The consent of the users is required for the proposed model. During the registration, the user will be asked to provide the cell phone number. Even when the user wants to check if he/she made any contact with any COVID-19 patient, the cell phone number needs to be sent to the operator for a cross-check.

E. SYSTEMATIC CHALLENGES

The systematic challenges are considered in terms of carriers, businesses, and users of the proposed model. The issues are described below:

1) MISINFORMATION

There is a very low risk of misinformation as the location data will not be taken from any user input. Rather the data will be collected from the sim card operator.

2) PANIC

The proposed model can reduce panic to some extent as the users of the model can check the initial status and also the intensity while staying at home.

3) FRAUD AND ABUSE

It is expected that there will be no fraudulent activities as the application will not require any open connection (e.g. Bluetooth, NFC, etc.).

4) SECURITY OF INFORMATION

The proposed model is designed with a view in mind about the security concerns of the carrier's as well as the user's important information. As only the cell phone number, which is already a public entity, is needed to operate the proposed method, there is a very low chance of security holes.

5) EQUAL ACCESS

Equal access is the main strength of the proposed model as it is not limited by any technological requirement (e.g. smartphones, battery, certain OS, etc.) rather only a cell phone is needed.

6) SOCIO-ECONOMIC FACTORS

There are almost no bad impacts on the socioeconomic factors for the proposed model. Sometimes it is dependent on the government's practice if there is any.

Finally, the overall comparison of existing contact tracing approaches with the proposed approach is provided in Table 2 in terms of major strengths and limitations.

V. EXPERIMENTAL RESULTS

In this section, we compare the proposed contact tracing method with existing technologies through numerical examples. To understand the real impact of our proposed system and to make a realistic comparison with the existing solutions based on BLE technology, we have generated the mimic of an actual contact tracing scenario based on some real statistical measures. In the scenario, we have used the Poisson Point Process (PPP) for a circular area of radius 1. We have scaled a distance of 100 meters to unity for ease of presentation. The percentages of smartphone users and any type of mobile phone users are considered as the density parameters of PPP for generating two separate sets of data. We consider Bangladesh as a typical example of developing countries to show the practical effectiveness of the proposed approach. According to the Bangladesh Bureau of Statistics (BBS) and Bangladesh Statistics 2018, the total population of Bangladesh is 162.7 Million [44]. According to the Bangladesh Telecommunication Regulatory Commission (BTRC), the total number of mobile phone subscribers is 162.290 million [45] and the total number of mobile Internet subscribers is 93.101 million at the end of April 2020 [46]. As the total number of mobile phone subscribers is almost identical to the total population, we assume that almost 100% people have a mobile phone of some kind. Note that the official data of unique mobile users is not available during this analysis. We are considering the percentage of smartphone users based on the total number of mobile Internet subscribers. Thus, we can say that almost 58% of Bangladeshi

people are using smartphones. Without loss of generality, we assume that people need smartphones to be able to use the BLE-based tracing app.

Now, we use the value of the density parameter for any type of mobile phone users as lambda (λ) = 100 and for smartphone users as lambda (λ) = 58 in Poisson Point Process. Based on this assumption, we simulate the data for both type of mobile phone users in Cartesian two-dimensional space. We have repeated the simulation four times so that we can make a reliable inference with a more accurate performance measure. In order to understand the dispersion of the points, we use scatter plots (Figs. 7 and 8) and co-variance measures.

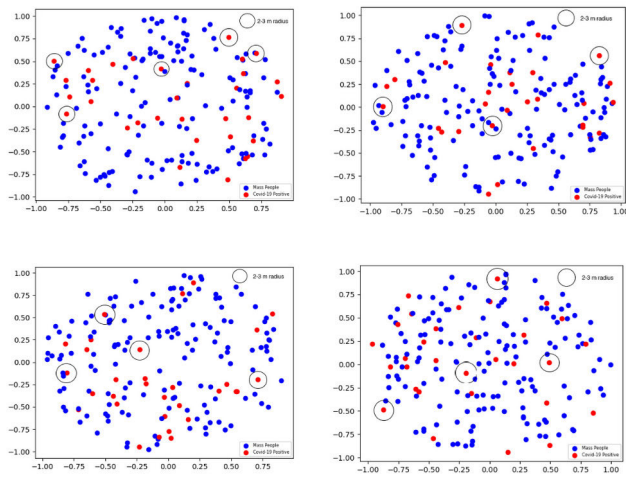


FIGURE 7. Scatter plots (four trials) using poisson point process (lambda = 58).

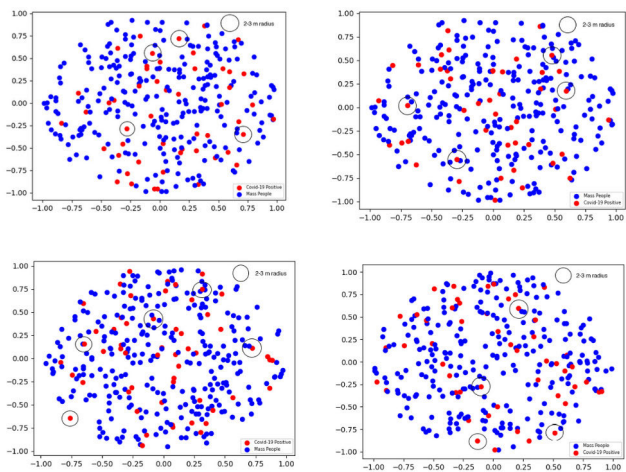


FIGURE 8. Scatter plots (four trials) using poisson point process (lambda = 100).

It is apparent that the points in any type of mobile phone users (Fig. 8) are more condensed than the points simulated based on only smartphone users (Fig. 7). The covariance analysis in Table 3 is also supporting this observation to draw the same inference as the covariance is always smaller for the points in any type of mobile phone users ($\lambda = 100$) than smartphone users ($\lambda = 58$).

TABLE 3. Co-variance analysis of the generated points using poisson point process.

Trial	Lambda (λ) = 58	Lambda (λ) = 100
T-1	0.00634	0.002947
T-2	0.001175	0.009763
T-3	0.024061	0.00306
T-4	0.00859	0.00582

According to the official statistics, 18% of the people who were tested for COVID-19 in Bangladesh were found positive [47]. So, we have randomly selected 18% of the points as COVID-19 positive and marked with red dots in Fig. 7 and Fig. 8. Then, we have measured the Euclidean distance of every point with respect to the red points (likely COVID-19 positive). Finally, we have counted the points which were within a 3-meter radius of any of the Covid-19 positive points. Similarly, we count the same considering the 2-meter distancing strategy. The contact tracing performance comparison for a maximum of 3-meter distance is shown in Table 4. Here, we can see that for each of the four trials, the count of contact tracing using any type of mobile phone is higher than that of smartphone users. During the trials, the highest percentage of change with respect to smartphone users is 300% and the lowest is 100%. The average count of contact tracing for any type of mobile phone users and smartphone users is 20 and 7.75, respectively. These observations clearly show the effectiveness of the proposed tracing strategy.

TABLE 4. Contact tracing comparison for maximum 3-meter distance.

Trial	Contact Tracing Count (Any type of phone)	Contact Tracing Count (Only Smartphone)	Percentage of Change
T-1	19	9	111.11%
T-2	22	11	100%
T-3	19	6	216.67%
T-4	20	5	300%

The contact tracing comparison for a maximum of 2-meter distance is shown in Table 5, where we again notice that for each trial, the count of contact tracing using any type of mobile phone is higher than that of smartphone users. During the trials, the highest percentage of change with respect to smartphone users is 266.67% and the lowest is 60%. The average count of contact tracing for any type of mobile phone users and smartphone users is 9.5 and 4.25, respectively.

TABLE 5. Contact tracing comparison for maximum 2-meter distance.

Trial	Contact Tracing Count (Any type of phone)	Contact Tracing Count (Only Smartphone)	Percentage of Change
T-1	9	5	80%
T-2	10	4	150%
T-3	8	5	60%
T-4	11	3	266.67%

These two contact tracing comparisons are depicted graphically in Fig. 9 and Fig. 10.

Next, we extend the performance comparison to the case of two other countries, e.g. India and South Korea because

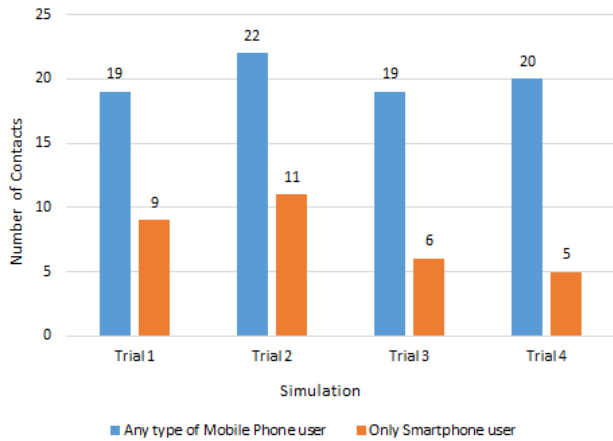


FIGURE 9. Pairwise contact tracing comparison considering the maximum 3-meter distance.

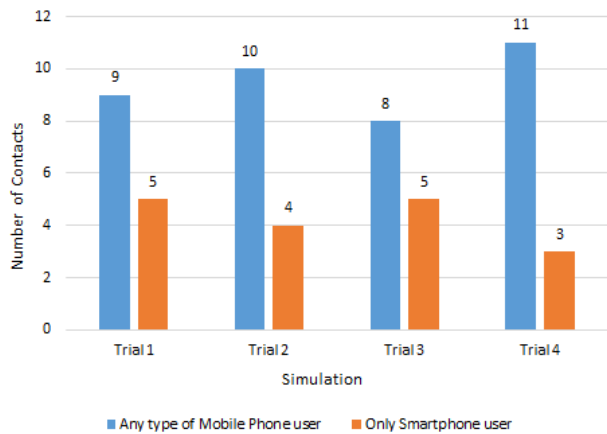


FIGURE 10. Pairwise contact tracing comparison considering the maximum 2-meter distance.

South Korea is ranked at the top of the list for smartphone usage (95%) and India at the last (24%) based on the total population [48]. In India, 24% of the total population use smartphones, 40% people use mobile phones that are not smartphones and 35% people do not use any mobile phone at all. Therefore, we simulate the data for India with the density parameter, $\lambda = 24$ for smartphone-only users and $\lambda = 64$ for any kind of mobile phone users. On the other hand, in South Korea, 95% people use smartphones and 5% use a mobile phone that are not smartphones. So, for South Korea, we consider the density parameter, $\lambda = 95$ for smartphone-only users and $\lambda = 100$ for any kind of mobile phone users. According to COVID-19 case statistics for both the countries, it is found that in India, 4.16 % of people were found positive after test [49] and it is 1.06 % in South Korea [50]. We have used these percentages to consider the COVID-19 positive points. The country-wise contact tracing performance of existing and proposed schemes is shown in Fig. 11. From Fig.11, it is noticeable that the count of contact tracing is higher for most of the time when any type of mobile phone users' geolocation is considered than smartphone-based apps.

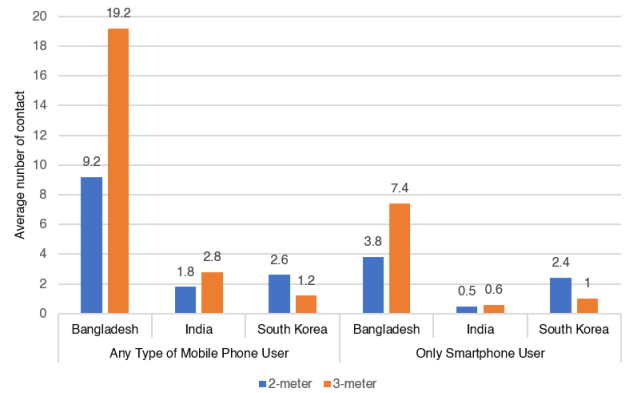


FIGURE 11. Country wise average contact tracing count comparison.

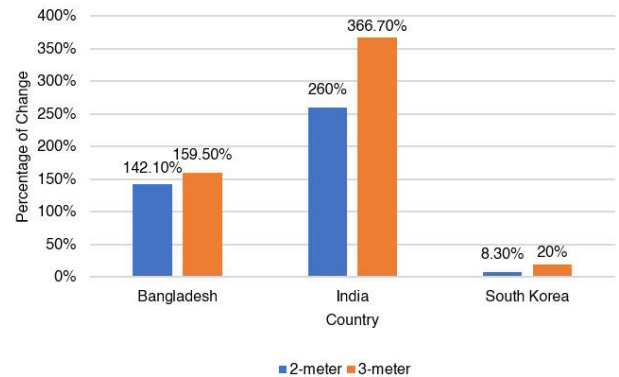


FIGURE 12. Country-wise comparison on percentage of change with respect to only smartphone users.

The percentage of changes with respect to smartphone users for each of the countries is also given in Fig. 12

VI. CONCLUSION

To slow down the spreading of the deadly virus termed as the novel Coronavirus, there is no alternative to finding out the infected persons as well as those who came into close contact with an infected person, then taking proper measures. Considering this fundamental approach, many countries have already developed contact tracing applications which are showing promising results but with significant privacy concerns. In this article, we have addressed the privacy issue by avoiding any smartphone-based apps for contact tracing through wireless connectivity (e.g. Bluetooth, Wi-Fi, NFC, etc.). The proposed model uses mobile users' geolocation data directly from the mobile operators. By doing so the overall contact tracing performance improves significantly while preserving users' privacy.

REFERENCES

- [1] K. T. D. Eames and M. J. Keeling, "Contact tracing and disease control," *Proc. Roy. Soc. London. Ser. B, Biol. Sci.*, vol. 270, no. 1533, pp. 2565–2571, Dec. 2003. [Online]. Available: <https://pubmed.ncbi.nlm.nih.gov/14728778>
- [2] S. O'Dea. (Aug. 2020). *Number of Smart Phone Users Worldwide*[Statista. [Online]. Available: <https://www.statista.com/statistics/330695/number-of-smartphone-users-w%worldwide/>

- [3] Statista Research Department. (Nov. 2016). *Number of mobile phone users worldwide from 2015 to 2020*. [Online]. Available: <https://www.statista.com/statistics/274774/forecast-of-mobile-phone-use%rs-worldwide/>
- [4] M. A. Abdulla and A. M. Esmaeel, "Providing information through smart platforms: An applied study on academic libraries in Saudi universities," *J. Edu., Soc. Behavioural Sci.*, vol. 5, pp. 1–24, Jun. 2019.
- [5] G. Kaptchuk, D. G. Goldstein, E. Hargittai, J. Hofman, and E. M. Redmiles, "How good is good enough for COVID19 apps? The influence of benefits, accuracy, and privacy on willingness to adopt," 2020, *arXiv:2005.04343*. [Online]. Available: <http://arxiv.org/abs/2005.04343>
- [6] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. Parker, D. Bonsall, and C. Fraser, "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science*, vol. 368, no. 6491, May 2020, Art. no. eabb6936. [Online]. Available: <https://science.sciencemag.org/content/368/6491/eabb6936>
- [7] M. Zastrow, "Coronavirus contact-tracing apps: Can they slow the spread of COVID-19?" *Nature*, May 2020. [Online]. Available: <https://www.nature.com/articles/d41586-020-01514-2>
- [8] E. Redmiles, "User concerns & tradeoffs in technology-facilitated COVID19 response," *Digit. Government: Res. Pract.*, vol. 5, Oct. 2020, Art. no. 6, doi: 10.1145/3428093.
- [9] Y.-A. de Montjoye, F. Houssiau, A. Gadotti, and F. Guepin. (2020, Apr.) *Evaluating COVID-19 Contact Tracing Apps Here Are 8 Privacy Questions We Think you Should Ask*. [Online]. Available: <https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/>
- [10] D. K. M. Farhana. (2020). *Knowledge and Perception Towards Novel Coronavirus (COVID-19) in Bangladesh*. [Online]. Available: <https://ssrn.com/abstract=3578477>
- [11] T. Jasarevic, C. Lindmeier, and F. Chaib. (Jan. 2020.) *Statement on the Second Meeting of the International Health Regulations (2005) Emergency Committee Regarding the Outbreak of Novel Coronavirus (2019-nCoV)*. [Online]. Available: [https://www.who.int/news/item/30-01-2020-statement-on-the-second-meeting-of-the-international-health-regulations-\(2005\)-emergency-committee-regarding-the-outbreak-of-novel-coronavirus-\(2019-ncov\)](https://www.who.int/news/item/30-01-2020-statement-on-the-second-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-outbreak-of-novel-coronavirus-(2019-ncov))
- [12] (Mar. 2020). *WHO Director-General's Opening Remarks at the Media Briefing on COVID-19*. [Online]. Available: <https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19-11-march-2020>
- [13] J. Hua and R. Shaw, "Corona virus (COVID-19)—infodemic and emerging issues through a data lens: The case of China," *Int. J. Environ. Res. Public Health*, vol. 17, no. 7, p. 2309, 2020. [Online]. Available: <https://www.mdpi.com/1660-4601/17/7/2309>
- [14] E. Shim, A. Tariq, W. Choi, Y. Lee, and G. Chowell, "Transmission potential and severity of COVID-19 in South Korea," *Int. J. Infectious Diseases*, vol. 93, pp. 339–344, Apr. 2020. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1201971220301508>
- [15] N. AL-Rousan and H. AL-Najjar, "Data analysis of coronavirus COVID-19 epidemic in South Korea based on recovered and death cases," *J. Med. Virology*, vol. 92, no. 9, pp. 1603–1608, Sep. 2020. [Online]. Available: <https://pubmed.ncbi.nlm.nih.gov/32270521>
- [16] H. Ko, J. Leitner, E. Kim, and J. Jeong, "Structure and enforcement of data privacy law in South Korea," *Int. Data Privacy Law*, vol. 7, no. 2, pp. 100–114, May 2017, doi: 10.1093/idpl/ix004.
- [17] J. Bay, J. Kek, A. Tan, and C. S. Hau. (2020). *Bluetrace: A Privacy-Preserving Protocol for Community-Driven Contact Tracing Across Borders*. [Online]. Available: https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632de%ff383eb33b3c.pdf
- [18] H. Cho, D. Ippolito, and Y. William Yu, "Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs," 2020, *arXiv:2003.11511*. [Online]. Available: <http://arxiv.org/abs/2003.11511>
- [19] V. Ollikainen and K. Halunen, *Rendezvous Based Pandemic Tracing by Sharing Diffie-Hellman Generated Common Secrets*. Helsinki, Finland: VTT Technical Research Centre of Finland, 2020.
- [20] P. K. Mishra, "Bluetooth security threats," *Int. J. Comput. Sci. Eng. Technol.*, vol. 4, no. 2, pp. 147–151, 2013.
- [21] M. Naveed, X. Zhou, S. Demetriou, X. Wang, and C. A. Gunter, "Inside job: Understanding and mitigating the threat of external device Misbonding on android," in *Proc. Neww. Distrib. Syst. Secur. Symp.*, 2014, p. 23.
- [22] D. Spill and A. Bittau, "BlueSniff: Eve meets Alice and Bluetooth," in *Proc. 1st Workshop Offensive Technol.*, Boston, MA, USA, Aug. 2007, pp. 1–5.
- [23] X. Bai, L. Xing, N. Zhang, X. Wang, X. Liao, T. Li, and S.-M. Hu, "Staying secure and unprepared: Understanding and mitigating the security risks of apple ZeroConf," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 655–674.
- [24] M. Ruef. (Apr. 2020). *Contact Tracing App DP3T—These are the Risks of the Swiss Solution*. [Online]. Available: <https://www.scip.ch/en/?labs.20200427>
- [25] D. Watts. (2020). *COVIDSafe, Australia's Digital Contact Tracing App: The Legal Issues*. [Online]. Available: <https://ssrn.com/abstract=3591622>
- [26] M. M. Lab. (Apr. 2020.). *Safe Paths: A Privacy-First Approach to Contact Tracing*. [Online]. Available: <https://news.mit.edu/2020/safe-paths-privacy-first-approach-contact-tra%cing-0410>
- [27] A. Hekmati, G. Ramachandran, and B. Krishnamachari, "CONTAIN: Privacy-oriented contact tracing protocols for epidemics," 2020, *arXiv:2004.05251*. [Online]. Available: <http://arxiv.org/abs/2004.05251>
- [28] T. Li, Jackie, Yang, C. Faklaris, J. King, Y. Agarwal, L. Dabbish, and J. I. Hong, "Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing apps," 2020, *arXiv:2005.11957*. [Online]. Available: <http://arxiv.org/abs/2005.11957>
- [29] N. Trieu, K. Shehata, P. Saxena, R. Shokri, and D. Song, "Epione: Lightweight contact tracing with strong privacy," 2020, *arXiv:2004.13293*. [Online]. Available: <http://arxiv.org/abs/2004.13293>
- [30] G. Lee, "Legitimacy and Constitutionality of Contact Tracing in Pandemic in the Republic of Korea," *SSRN*, 2020. [Online]. Available: <https://ssrn.com/abstract=3594974>
- [31] M. Veale, "Analysis of the NHSX contact tracing App 'isle of wight' data protection impact assessment," *LawArXiv*, Dec. 2020. [Online]. Available: <https://osf.io/preprints/lawarxiv/6fvgh>
- [32] K. Roomp and N. Oliver, "ACDC-tracing: Towards anonymous citizen-driven contact tracing," 2020, *arXiv:2004.07463*. [Online]. Available: <http://arxiv.org/abs/2004.07463>
- [33] J. Bell, D. Butler, C. Hicks, and J. Crowcroft, "TraceSecure: Towards privacy preserving contact tracing," 2020, *arXiv:2004.04059*. [Online]. Available: <http://arxiv.org/abs/2004.04059>
- [34] D. Andreoletti, O. Ayoub, S. Giordano, M. Tornatore, and G. Verticale, "Privacy-preserving multi-operator contact tracing for early detection of Covid19 contagions," 2020, *arXiv:2007.10168*. [Online]. Available: <http://arxiv.org/abs/2007.10168>
- [35] J. K. Liu, M. H. Au, T. H. Yuen, C. Zuo, J. Wang, A. Sakzad, X. Luo, and L. Li. (2020). *Privacy-Preserving COVID-19 Contact Tracing App: A Zero-Knowledge Proof Approach*. [Online]. Available: <https://eprint.iacr.org/2020/528>.
- [36] L. Reichert, S. Brack, and B. Scheuermann. (2020). *Privacy-Preserving Contact Tracing of COVID-19 Patients*. [Online]. Available: <https://eprint.iacr.org/2020/375>.
- [37] J. Trogh, D. Plets, E. Surewaard, M. Spiessens, M. Versichele, L. Martens, and W. Joseph, "Outdoor location tracking of mobile devices in cellular networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, p. 115, May 2019, doi: 10.1186/s13638-019-1459-4.
- [38] K. Pahlavan, X. Li, and J. P. Makela, "Indoor geolocation science and technology," *IEEE Commun. Mag.*, vol. 40, no. 2, pp. 112–118, 2002.
- [39] H. Seyyedhasani, J. S. Dvorak, M. P. Sama, and T. S. Stombaugh, "Mobile Device-Based Location Services Accuracy," *Appl. Eng. Agricult.*, vol. 32, no. 5, pp. 539–547, 2016.
- [40] J. Tomatík, J. Tomatík, Š. Salo, and R. Piroh, "Horizontal accuracy and applicability of smartphone GNSS positioning in forests," *Forestry*, vol. 15, pp. 187–198, Aug. 2016, doi: 10.1093/forestry/cpw031.
- [41] S. M. Toapanta, O. A. Escalante Quimis, L. E. M. Gallegos, and M. R. Maciel Arellano, "Analysis for the evaluation and security management of a database in a public organization to mitigate cyber attacks," *IEEE Access*, vol. 8, pp. 169367–169384, 2020.
- [42] R. Raskar, "Apps gone rogue: Maintaining personal privacy in an epidemic," 2020, *arXiv:2003.08567*. [Online]. Available: <http://arxiv.org/abs/2003.08567>
- [43] 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. 134577–134601, 2020.
- [44] *Bangladesh Statist.* Ministry of Planning, Bangladesh, India, 2018.
- [45] (Apr. 2020). *Mobile Phone Subscribers in Bangladesh BTRC*. [Online]. Available: <http://www.btrc.gov.bd/content/mobile-phone-subscribers-bangladesh-apri%1-2020>

[46] (Apr. 2020). *Internet Subscribers in Bangladesh BTRC*. [Online]. Available: <http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-april-20%20>

[47] (2020). *COVID-19 Situation Updates|IEDCR*. [Online]. Available: <https://iedcr.gov.bd/covid-19/covid-19-situation-updates>

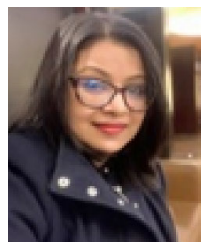
[48] (Feb. 2020). *Smartphone Penetration Rate by Country 2018|Statista*. [Online]. Available: <https://www.statista.com/statistics/1003406/smartphone-penetration-by-c%ountry/>

[49] (Nov. 2020). *COVID-19 Cases By Country, Worldwide 2020|Statista*. [Online]. Available: <https://www.statista.com/statistics/1111696/covid19-cases-percentage-by%-country/>

[50] W. So. (Aug. 2020). *Coronavirus (COVID-19) in South Korea - Statistics & Facts | Statista*. [Online]. Available: <https://www.statista.com/topics/6082/coronavirus-covid-19-in-south-kore%a/>



MD. TANVIR RAHMAN was born in Meherpur, Bangladesh. He received the B.Sc. (Hons.) and M.S. degrees in information technology from Jahangirnagar University, Bangladesh, in 2013 and 2015. From 2015 to 2019, he was a Lecturer with the Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh. He is currently a Lecturer with the Department of Information and Communication Technology, Mawlana Bhashani Science and Technology University, Bangladesh. His research interests include wireless communication and the Internet security concerns.



RISALA T. KHAN (Member, IEEE) was born in Dhaka, Bangladesh. She received the B.Sc. (Hons.) and M.Sc. degrees in computer science and engineering from Jahangirnagar University, Dhaka, in 2003 and 2005, respectively, and the Ph.D. degree in the field of cognitive radio system from Jahangirnagar University.

She was a Lecturer with the Department of Computer Science and Engineering, Daffodil International University, Dhaka. She is currently a Professor with the Institute of Information Technology, Jahangirnagar University. Her research field is wireless communications, network traffic, and network security. She is acting as Counselor of the IEEE WIE Affinity Group JU SB.



EURASIP Journal on Wireless Communications and Networking.

MUHAMMAD R. A. KHANDAKER (Senior Member, IEEE) received the Ph.D. degree from Curtin University, Australia. He is currently an Assistant Professor with the School of Engineering and Physical Sciences, Heriot-Watt University. He was a Postdoctoral Research Fellow with the University College London, U.K., from 2013 to 2018. He is an Associate Editor of the IEEE WIRELESS COMMUNICATIONS LETTERS, the IEEE COMMUNICATIONS LETTERS, IEEE ACCESS, and the



MATHINI SELLATHURAI (Senior Member, IEEE) is currently a Full Professor in signal processing and intelligent systems with Heriot-Watt University, Edinburgh, U.K. In her 15-year research on signal processing for communications, she has made seminal contributions on MIMO wireless systems. She has authored or coauthored 200 IEEE entries. She has written a book and several book chapters in topics related to this project. She is a Fellow of HEA. She was a member for the IEEE SPCOM Technical Strategy Committee, from 2014 to 2018. She received the IEEE Communication Society Fred W. Ellersick Best Paper Award in 2005, the Industry Canada Public Service Award for contributions in science and technology in 2005, and the Best Ph.D. thesis medal from NSERC Canada, in 2002. She was also the General Co-Chair of the IEEE SPAWC2016 in Edinburgh. She was an Editor of the IEEE TSP from 2009 to 2014 and from 2015 to 2018. She has given invited talks.



MD. SIFAT A. SALAN was born in Panchagarh, Bangladesh. He received the B.Sc. (Hons.) and M.Sc. degrees in statistics from Jahangirnagar University, Dhaka, in 2015 and 2016, respectively. He was a Permanent Faculty of statistics with Primeasia University and Daffodil International University. He is currently an Assistant Professor with the Department of Statistics, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. His research field is statistical data modeling with simulation, machine learning, and time series analysis.

...