USABILITY OF SMART PHONE BASED CONTACT TRACING IN FIGHTING PANDEMICS SUCH AS COVID 19; ISSUES AND SOLUTION

BY

BHUDIPTA TARAFDER
ID: 151-15-5452

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Aniruddha Rakshit
Sr. Lecturer
Department of CSE
Daffodil International University

Co-Supervised By

Mr. Abdus Sattar
Assistant Professor
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

AUGUST 2021

APPROVAL

This Project titled "**USABILITY OF SMART PHONE BASED CONTACT TRACING IN FIGHTING PANDEMICS SUCH AS COVID 19; ISSUES AND SOLUTION** ", submitted by * **BHUDIPTA TARAFDER** * to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on *11th September, 2021*

BOARD OF EXAMINERS

Chairman

Dr. Touhid Bhuiyan

Professor and Head

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

Internal Examiner

Abdus Sattar

Assistant Professor

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

Internal Examiner

Md. Riazur Rahman

Assistant Professor

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

External Examiner

Dr. Dewan Md. Farid

Associate Professor

Department of Computer Science and Engineering

United International University

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Name, Designation, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

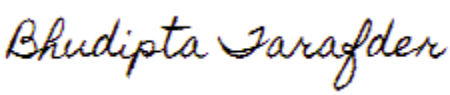
Supervised by:

Aniruddha Rakshit
Sr. Lecturer
Department of CSE
Daffodil International University

Co-Supervised by:

Mr. Abdus Sattar
Assistant Professor
Department of CSE
Daffodil International University

Submitted by:



Bhudipta Tarafder
ID: -151-15-5452
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

I really grateful and wish our profound our indebtedness to **Aniruddha Rakshit,**
Sr. Lecturer, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of "*Internet of Things*" to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete this project.

I would like to express our heartiest gratitude to Dr. Touhid Bhuiyan, Professor and Head**,** Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

I would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, I must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

The outburst of COVID-19 has overwhelmed the world. It brought lockdowns and it stressed general medical services frameworks. COVID-19 is known to be an exceptionally irresistible infection, and tainted people don't at first show side effects, while some stay asymptomatic. Contact Tracing is considered as the first and the best advance towards containing a flare-up, as assets for mass testing and huge number of vaccines are exceptionally far-fetched accessible for quick usage. Many govt and organizations are now using or plan to use various mobile based contact tracing solutions and apps. Nonetheless, tracing applications have created a lot of conversation around their key ascribes, including architecture, user data safety, ease of use, and security. In this article, I illuminate a portion of the issues and difficulties relating to the reception of robust contact tracing solutions for battling COVID-19. I proposed an Evaluation system for versatile contact tracing frameworks for decide their ease of use, practicality, versatility and effectiveness. Furthermore, I present potential assaults that can be dispatched against contact tracing arrangements along with their fundamental countermeasures to obstruct any chance of such assaults.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

Introduction

In this millennium, we have seen several mass outbreaks of various high transmitted diseases. For example, SARS; Severe Acute Respiratory Syndrome is a pneumonia which is identified by a high rate of transmission. The very first outbreak began in Guangdong Province, China, in November 2002 [1].

One of the biggest SARS episodes to date started in Singapore in mid-March 2003 [1] and was followed to a migrant getting back from Hong Kong. As of late in China, a few neighborhood health offices in Wuhan, Hubei Province, announced groups of patients with pneumonia of obscure reason that they evidently and epidemiologically connected to a fish and wild animal discount market in the region. Anyway, the due spread through untraced contacts ultimately led to its spread on a worldwide scale which is the thing that we consider today to be a pandemic (COVID-19) [2].

Contact Tracing is a key methodology for minimizing the effect of contaminations like COVID-19 on medical services frameworks and well-being of the populace all in all, and is consequently expected to slow the spread of irresistible illnesses. It permits people of a nation or a local area to soothe trouble from a local area's control measures, as it allows the people of that area to isolate themselves deliberately. Contact tracing is required to increment the affectability followed by the availability of a nation, a local area, or people for an arising pandemic like novel (COVID-19) by relieving the all-around weaknesses of the traditional contact tracing which exclusively depends on symptoms of an individual.

As per to the Guideline of the WHO [3], contact-tracing is done in three steps:

1. Recognizing the Contact: From the all-around affirmed positive cases, distinguishing those that the patient had contact with.

2. Contacts Listing: Keep a record of potential contacts of the contaminated patients and illuminate those people.

3. Contact Follow-Up: An important follow-up of the patients that are accepted to have interacted with the contaminated people and the individuals who are positive.

Thinking about the headways in innovation, pretty much every substitute individual on earth conveys a gadget which has the ability of being followed through GPS with a legitimate framework and infrastructure [3].

Such capacities, for example, the ability to track/log the locations with appropriate timestamps and the capacity to log them can unquestionably permit one to identify contaminated people and that of the ones who have been in their closeness, in this way empowering contact tracing.

Presently that we realize what is in question, it is additionally essential to comprehend the extent of the grave consequences it can draw. Since, digital contact tracing is highly being requested in light of the need of great importance, there are various propositions rising up out of established researchers utilizing cutting edge innovations to make contact tracing really conceivable and more convenient practically speaking. Notwithstanding, with the recommendations coming in numbers, one significant angle is their cautious evaluation and assessment from a nonexclusive perspective prior to being considered for wide usage by the majority. To this end, there is certifiably not an overall system or an appraisal model for computerized contact following answers for decide their achievability, ease of use and adaptability.

To address this issue close by, I propose an assessment system to examine and assess a portion of the contact tracing solutions/frameworks dependent on certain boundaries and what's more, examine about the chance of attacks on them and their countermeasures.

In this thesis, I researched a few contact following solutions under the evaluation framework I proposed. The parameters of the evaluation framework are profoundly essential to contact tracing solutions.

In this article, we investigated a couple of contact following tracing solutions under the evaluation framework I proposed. The limits of the evaluation framework are significantly crucial for contact tracing courses of action.

• I assessed a few of the accessible contact tracing solutions considering our framework.

• I additionally played out a comparative analysis of the evaluated contact tracing solutions to provide answers that far reached the bits of knowledge for better comprehend these arrangements.

• Furthermore, I gave potential attacks on contact tracing solutions and their possible countermeasures.

CHAPTER 2

Main Problems and Obstacles Regarding Smart Phone Based Contact Tracing

Smart Phone Based contact tracing accelerates up the cycle of recognizable proof of the people who may have come in close contact with the infectious ones.

In any case, prior to merge the conventional contact tracing methodology with the modern advanced methods there emerge likely dangers and issues

A portion of the essential worries of which are

1.safeguarding the identity of an infected person.

2.stopping the spread of misinformation,

3.stopping snoopers from causing panic among the masses and

4.withholding the countries from establishing a surveillance state.

There are a few technologies based arrangements recommended to be implemented as an advanced contact tracing apparatus, a few of which depend on GPS, and also Bluetooth based token sharing systems.

Regardless of the endeavors, there are issues with the basic nature of these technologies which are to be perceived, featured and relieved in most ideal approaches to reinforce the recommended apparatuses.

These issues ought to be routed to limit any essential loop hole for hackers, snoopers and the so-called big brother.

The Automatic Contact tracing systems dependent on Bluetooth communications was first suggested by Altuwaiyan et al. [4] in 2018.

The Bluetooth based contact tracing framework can straightforwardly distinguish whether users came in vicinity of one another. The vicinity can be approximated by the strength of the signal, which despite the fact is diminished by obstacles like dividers. Consequently, in a high danger environment for close contact like apartment complexes or public travels it can all more adequately and precisely reflect useful vicinity [5].

In any case, with applications that assess exposure risk dependent on Bluetooth, proximity exchange is generally not adequate in light of the way that separated from the human-to-human communication, Coronavirus COVID-19 can likewise spread through normal conditions or regularly touched surfaces [6].

Another significant disadvantage of Bluetooth based framework is the issue of moderate or low pace of appropriation which thus restricts the client base along these lines influencing the viability of the framework. Zeadally et al. in [7] has given a highlighted conversation on issues and potential attacks on Bluetooth systems.

GPS, then again isn't secure by its innate nature. Additionally, there are a few functionalities that GPS based frameworks can't give. One of the primary concerns is spoofing attacks, where a spoofer makes a bogus GPS signal with a false time and location to a specific receiver [8]. Warner et al. in [9] gave a basic exhibition to show GPS is powerless against satirizing.

CHAPTER 3

Proposing a framework for evaluating contact tracing solutions

The proposed evaluation framework is a five-step method for assessing a specific contact tracing solution as appeared in Fig. 1.

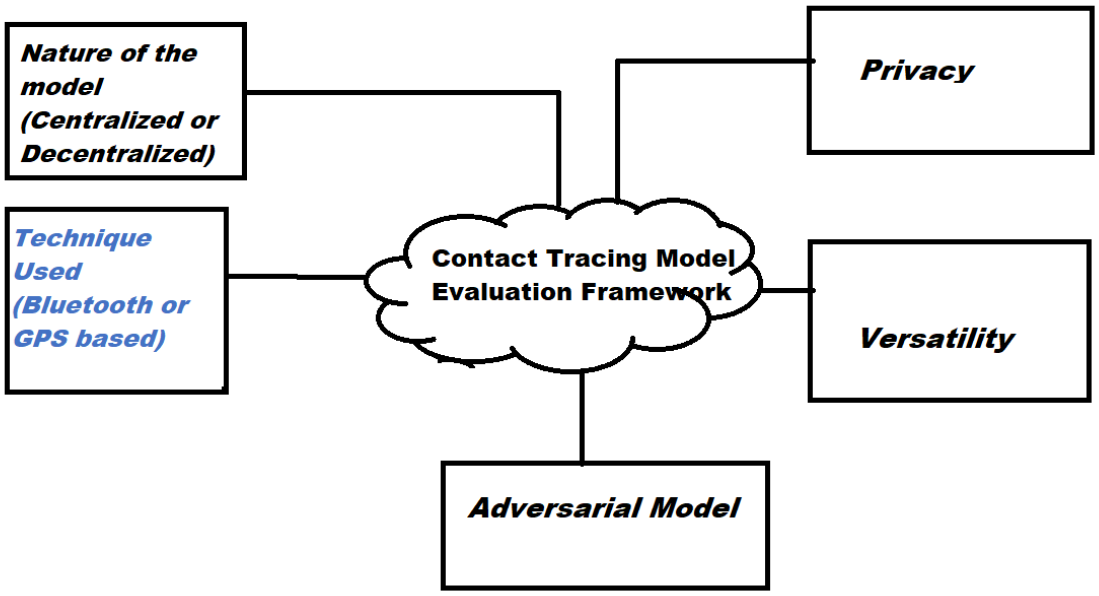


Fig 1. Proposed Contact Tracing Framework

The figure portrays the diagrammatic portrayal of the framework and each progression is summed up in detail beneath. The point of my assessment model is to classify the contact tracing solutions so as to have the option to recognize every solution effectively and additionally have a general measure for the assessment of contact tracing frameworks.

It is similarly essential to give the inspiration driving picking these boundaries for assessment of contact tracing solution. Since contact tracing solutions include assortment and utilization of sensitive information of people, for example, their wellbeing history, contamination state, current health condition, ailments and their area.

It is obvious that the utilization of this sensitive personal data of people has evoked genuine worries about the general uprightness of these solutions. These concerns have spurred interest in openness of the entire process, so the partners can better comprehend the fine subtleties, including the motivation behind the solutions, the security it offers, the information that is being gathered and the proposed solution's utilization of the gathered information. With all these factors in context, I sorted out the parameters that best suit the reason and are very much summed up in nature.

I further put 3 available contact tracing solutions under the framework's appraisal models and dissect them expressly.

3.1 Nature of the model (Centralized or Decentralized)

In a centralized system, all the users stay connected to a single point or a server. While as a decentralized framework or system, is one where no authority has the power over the entire system or the user's information.

The reasoning of a solution being Centralized or decentralized is of an utmost priority in any contact tracing solution. As in centralized systems, a semi trusted authority for example the government is in charge. Let us consider Singapore's TraceTogether app[14]. The Government keeps a database that joins arbitrarily created tokens from a person's smartphone to their telephone numbers and afterward to their real identities. They can construct a rundown of any remaining individuals they have been in contact with after a tainted user is constrained to transfer his data.

With these things into thought, no individual would need to be misused by a central authority under any conditions. Consequently, the idea of decentralization marks such surveillance foundations and gives people something to gaze upward to. I view it as a strategy that satisfies the vital prerequisites of contact tracing while at the same time giving the privacy and protection we need.

In any case, [15] provided extraordinary bits of knowledge into security and privacy examination of contact tracing solutions. He contended that as opposed to the normal belief that decentralization settles the security worries of centralized systems, it rather presents some new attack vectors against privacy itself. I have coordinated recommendations in this paper and described them in a context that I feel must be to contact tracing systems.

3.2 Technique Used (Bluetooth or GPS based)

My second assessment basis is to comprehend the fundamental method utilized by the contact following arrangement. Since, the workflow is to follow the individuals who came in close contact with one another, there are two instruments that are normally used to guarantee tracking of people. They are Bluetooth and GPS based.

A portion of the solutions utilize the utilization of both while the majority of them depend on either. The broadly embraced method is the one which utilizes Bluetooth based tracing because of the multitude of obvious reasons. Since Proximity based arrangements are normally more precise contrasted with GPS based arrangements [16], it is one of the reference determination boundaries.

Among different preferences is its capacity to characterize close contacts with an essentially lower false positive rate than GPS [16], its low power utilization and the rate of reception. The rate of adaptation is another significant parameter for contact tracing

solutions. It is very clear that individuals are careful about tracing their location, which can hamper its appropriation and clear a route for Bluetooth based proximity solution.

3.3 Privacy

Privacy is a broad idea, and incorporates a wide scope of things from control over one's objects, freedom of expression, opportunity of thoughts, control over personal information, independence from surveillance and insurance from cross examinations and searches [10]. There are a few notions of privacy that have been presented throughout the years and are generally utilized by and by.

Privacy of the common masses has not been a worry in a portion of the contact tracing solutions. A few nations have even received the thought of mass reconnaissance to track individuals for the sake of contact tracing. In spite of the fact that there is certainly not a solitary idea of privacy that can ensure with outright certainty, the privacy necessities that a contact tracing solution needs however I can attempt to detail certain thoughts of security and privacy in order to make privacy safeguarding a genuine entity by and by.

Keeping in view the unique circumstance of the issue in context, I include some mainstream definitions like k-anonymity [11], differential privacy [12], and information-theoretic privacy [13].

I characterized tiers of privacy that the proposed models fulfill. I mark them as following:

T1 (Tier One): Privacy from Snoopers.

T2 (Tier Two): Privacy from other Users.

T3 (Tier Three): Privacy from the Authorities.

3.4 Adversarial Model

The adversarial model portrays the environment in which the adversary is working or the unlawful capacities of a foe. There are a few adversarial models in the field of cybersecurity yet we utilize the Semi-honest/ Honest but Curious model for my situation. In this model, the adversary can attempt to get the data that they are most certainly not qualified for

3.5 Versatility

An answer is supposed to be adaptable on the off chance that it tends to be received by the masses without critical changes to the basic foundation. There can be different boundaries under the wide cover of versatility relying on the application being focused on like a number of downloads, Battery advancement, and so forth Nonetheless, in a nonexclusive way I think about the versatility.

CHAPTER 4

Evaluation of the proposed solutions and Review of Related Literature

4.1 EPIC

Altuwaiyan et al's. [4] model is an effective security and privacy guarding contact tracing solution that empower users to transfer their information safely to the server and if on the off chance that somebody gets infected, others can check whether they ever interacted with that tainted person.

No unnecessary data is uploaded to the server. A matching score is used to represent the result of the contact tracing.

The participating entities in the system model are:

• Smartphones

• short-range wireless devices like Access points

• Bluetooth devices and

• A Server; it keeps encrypted information from the clients and the relating timestamps in plaintext

The several phases of this architecture are described below.

Setup or introduction Phase

Since no unique arrangement is required. We accept that this stage has happened.

Filtering or Sensing Phase

During this stage, the user's cell phones will gather raw information about close by short-range wireless signals (Wi-Fi and Bluetooth) by performing convenient versatile wireless scanning.

Revealing stage or Detection Phase

At the point when a user is distinguished as certain, at that point the user will transfer its information to the server which is encoded with relating timestamps for each network scan. The information: Wireless Signal Unique Identifier (BSSID), Wireless Signal Strength Indication (RSSI) and Wireless Signal Type (Wi-Fi, Bluetooth) are portrayed as tuples of data point (tx, (mi,1,ri,1, pi,1), . . . , (mi,ni,x ,ri,ni,x , pi,ni,x))

where (mi,1,ri,1, pi,1) portrays data about the first experienced device or gadget. mi,1 is the hashed unique identifier, ri,1 is the strength of the detected sign and pi,1 is the gadget type for time intervals t0, etc.

Following stage: Tracing phase

At the point when a user is distinguished to be contaminated and another user needs to check whether they have been in close contact, the user sends a request to the server which incorporates his public key. The server coordinates the outputs between the contaminated client u_i and the requested dependent on timestamps.

Note that the timestamps are put away in plaintext on the server. After a match is discovered, the subsequent stage is to check whether these two people have scanned the same wireless devices.

The server has the data of the contaminated user in plaintext as of now. Be that as it may, no data about a regular user is accessible to the server.

The server employs the user's public key which it got and encodes each m_i .

The server gives back a matrix which has the encrypted subtraction of all sets of m_i and m_n utilizing a homomorphic encryption plot duplicated by an arbitrary value d added by the server to forestall un from knowing unnecessary data about u_i

	mi2	mi3
mn1	$Enc((m_{n,1} - m_{i,2}) * d1,2)$	$Enc((m_{n1} - m_{i,3}) * d1,3)$
mn2	$Enc((m_{n,2} - m_{i,2}) * d2,2)$	$Enc((m_{n,2} - m_{i,3}) * d2,3)$
mn4	$Enc((m_{n,4} - m_{i,2}) * d4,2)$	$Enc((m_{n,4} - m_{i,2}) * d4,3)$

Table 1 Tracing phase of EPIC.

The results of the matrix are then decrypted by the user and a binary array is recovered compared to the decoding result. 1 show that two wireless gadgets coordinated and the other way around. The infected user u_i additionally sends $r_{i,y}$ with the matched $m_{i,y}$ where $1 < y < n_{i,x}$.

EPIC is likewise another strategy to gauge the distance between two smart gadgets as is apparent from the actual proposition. This by and by is more precise than different solutions. Considering the security of the proposition model, the infected people should uncover the location information to the server where the network identifiers are hashed. Since network identifiers are regularly static, it is of significance that this gives the server the opportunity to figure the location data points of the infected users.

Another significant thing to note is that the timestamps are kept in plaintext, which proposes that, at a specific timestamp the location of the user is accessible to the server. In this way, in view of my evaluation criteria, obviously homomorphic encryption is utilized to guarantee privacy protection to the queries. The controls are done on the encoded information itself.

Despite the fact that the degree of privacy this framework gives is T1 (Tier One), T2 (Tier Two), and T3 (Tier Three), however, there are some genuine concerns with regards to T3 (Tier three).

Like I examined previously, there is a chance of attacks and some genuine security spills that ought to have stayed away from. Maybe certain measures ought to be taken into thought and if the changes are done effectively, we expect that the T3 (Tier three) security will be given completely.

Another significant interesting point is that I excluded the instance of a bad actor corrupting the database with flawed queries.

Versatility is another significant factor that impacts a solution's widespread adoption. They have additionally built up an android application and tried it under different situations. Despite the fact that the number of users that the application was tried with was 10; which turns out to be a less difficult situation towards its arrangement in a genuine situation. Despite the fact that a few situations are talked about in the proposed model itself, the overhead will doubtlessly increment as the quantity of clients increases.

4.2 Berke et al.'s location-based system

Berke et al's. [5] contact tracing model is a GPS-based arrangement for contact tracing that uses parceling of fine-grained GPS areas and private set convergence permitting the framework to identify when a user came in the closeness of positive patients to evaluate and illuminate them regarding the danger while protecting the security of the people.

The substances of the system are:

• Users (possessing a cell phone with GPS and android/ios as its main OS) and

• Server (used to store the redacted, changed and scrambled information)

The different periods of the system can be portrayed momentarily beneath:

Setup or introduction Phase

It is accepted that users have a capable cell phone able to do gathering and storing information.

Filtering or Sensing Phase

As the users move for the duration of the day, timestamped GPS points or location data are gathered inside a user's cell phone. The information is gathered as tuples of latitude, longitude, and time.

Revealing stage or Detection Phase

A user's mobile application examines/checks for matches between their gathered location data and the location data shared by other users who were analyzed as certain transporters to distinguish purposes of contact. Despite the fact that the GPS focuses are never straightforwardly contrasted with discovering the matches, they are rather coordinated to a 3-dimensional framework where two measurements are latitude and longitude while the third measurement is time. They are then jumbled utilizing a deterministic single direction Hash work (for example NIST Standard SHA256) [17].

Following stage: Tracing phase

At the point when a patient is analyzed as a positive transporter, the patients share their redacted, anonymized, hashed guide spans with the server. Users intermittently share their direct spans with the focal server to distinguishing if their hashed point stretches coordinated with any individual who is analyzed to be a positive transporter. This occurs by methods for a private set convention.

Breaking down this arrangement considering my assessment system, this is a GPS-based arrangement where protection conservation is finished either physically or programmed redaction and muddling utilizing a deterministic hash work alongside a private set crossing point.

Despite the fact that the framework gives T1 (Tier One) and T2 (Tier Two) security. All things considered, the framework gives T3 (Tier Three) level security in any event, when the semi-legit nature of the server proposes that it very well may be undermined also. Talking of attack possibilities in the semi-autonomous setting, a few things are to be contemplated. Since, for the wide selection of Bluetooth-based solutions specific applications are required, that could experience the ill effects of slower or limited adoption. Along these lines, the way that the applications on a user's smartphone are now gathering the user's GPS location data and GPS location history, this solution uses the way that this is in fact imperative to all more rapidly reveal their framework as a daily existence saving option for contact tracing arrangements. They gave a basic plan that utilizes Diffie–

Hellman protocol [18] to better see how Private set intersection bolsters the privacy protection objectives set by the model.

There are of course privacy concerns if a model is built dependent on their delegate execution which includes distributing data points to a level information data file for other users to download as opposed to having a server perform a private set intersection protocol.

The worry with this is the hacker's endeavor to reproduce the GPS location history of users analyzed as carriers of diseases and conceivable re-recognizable proof of those from their shared anonymized information. There are different issues with regards to tradeoff between privacy, security, adoption, and potential dangers which may be a central consideration for versatility. Notwithstanding, it is additionally proposed that proximity and GPS location sharing should be opt-in.

4.3. TraceTogether

TraceTogether [14] is the first smartphone application-based solution of contact tracing. A framework created by Singapore's Government Technology Agency alongside the Ministry of Health to handle the current pandemic. The application works by trading time-varying tokens through Bluetooth connection between smartphones. The substances in this solution are:

• Users and

• Ministry of Health (MoH)

It is accepted that the Ministry of Health (MoH) of the Singapore government is trustworthy to secure the user’s data consequently making this solution a centralized one. It is to be mentioned that a user may be constrained by the medical specialists to deliver his information on the application in the event that somebody is determined to have COVID-19 and in Singapore, it is considered as a criminal offense to not help the Ministry of Health in documenting one's movement. The various periods of the solution are portrayed underneath:

Setup or introduction Phase

During this stage, users download the TraceTogether application [14] and introduce it on their smartphones. Before the application is dispatched, the MoH of Singapore chooses some time intervals [t0, t1, . . .], which will end right when the pandemic is finished. The application at that point sends the cellphone number to MoH and gets an identifying name or pseudonym for them. MoH stores in its database the pair (NUMi , IDi) where NUMi is the telephone number of the user I and the IDi is the pseudonym by the authority against this number. The authority creates the secret key K and chooses an encryption algorithm

Enc. For a user I, MoH sends the initial pseudonym TUDi,x= Enc(IDi,tx ; K) to the user's application toward the very beginning span tx for x0.

Filtering or Sensing Phase

In this stage, a user communicates TIDi,x at the time interval [tx, tx+1) for all x0. Users store the TID's of one another alongside the sign strength for example in the event that user i and j come in the scope of Bluetooth range they will store (TIDi,x, TIDj,x, Sigstren) where the initial two passages are the comparing nom de plumes the users I and j separately at time span tx and Sistren is the sign between their gadgets.

Revealing stage or Detection Phase

At the point when a user is tried positive for COVID-19 then the contaminated user should follow MoH and transfer the privately put away information to MoH's database.

Following stage: Tracing phase

After the user i stores the information on to the MoH's server, MoH at that point decrypts each and every TIDj,x and obtains IDj through which they can query his NUMj and afterward do the vital follow up. Presently, that the proposal is totally surely well known, it is quite evident that the proposed contact tracing solution is a proximity-based centralized solution where the centralized authority is the Ministry of Health. The encryption technique is picked by the authority so the notion of privacy is not satisfactory; it could be said that it is under the direct control of MoH.

As far as the degree of privacy, the application provides T1 (Tier One) and T2 (Tier Two) levels of privacy since time-varying tokens offer privacy among the users. In any case, it is to be noticed that the time-varying nature of these arbitrary tokens likewise provides privacy from snoopers undeniably if the refresh rate is all-around set. If the rate is too regular, at that point the server will need to store a colossal number of tokens and if the rate is moderate then the user can be found by a snooper while walking down the road. Here the semi-honest model of privacy appears to fit which is quite obvious because of the way that the solution is centralized and under unlimited oversight of the MoH of the Singapore government.

Despite the fact that the central authority is following the protocol yet if the situation arises, they can deviate from it depending upon the circumstances and severity of the explanation behind deviation. Since, the proposed model relies on a central authority it fails to fulfill the third degree of privacy (T3) on the grounds that there is a possibility of a linkage assault [21]. The behavior of TraceTogether [14] under various modifications is given in [19] and the underlying protocol behind TraceTogether is Bluetrace [20].

Regarding versatility, the application has received over 2.1 million downloads so far [22] which is practically 36% of the complete population of the nation [23], and it is a willful

choice for Singaporeans to install the application. However, the noticeable part here is, if the greater part of the Singaporean population adjusts this innovation as a measure to stop the spread of COVID-19, the measure of time-varying location information which is presented to the authorities will be colossal and can draw serious results.

There is a possibility that a malicious user can manipulate (i.e., add or erase) the information gathered by the application. Another possibility is relay attacks. In addition, there are some different attacks proposed in [15]. In spite of the fact that there is a preferred position of identifying infected individuals yet at the expense of an expensive compromise among privacy and utility

Contact Tracing Solution	Privacy			Open Source	Technology Used	Architecture	Owner of the Project	Server Role	Contact Finding Method
	T1	T2	T3						
EPIC	Yes	Yes	Minimum	No	WiFi + Bluetooth Low Energy (BLE)	Centralized	Private	Encrypted Information Storage	Weight based Method
TraceTogether	Yes	Yes	Almost	Yes	Bluetooth Low Energy (BLE)	Centralized	Government	Stores Locally stored pair of Points	Matching Locally Stored Data-points of Users
Berke et al's location based system	Yes	Yes	Minimum	No	Global Positioning System (GPS)	Centralized	Private	Stores and Encrypts location History	Private Set Intersection Protocol

Table 2 Comparison of the evaluated solutions.

App's Name	Country	Centralized/ Decentralized	Type of Project	Type of Tracking	Medium of information sharing
Private Tracer [23]	Netherlands	Decentralized	Public	Proximity Tracing	x
''Stopp Corona'' app [24]	Austria	Decentralized	Red Cross	Proximity Tracing	Selective Broadcasting
NOVID20 [25]	Austria	Decentralized	Private	Location & Proximity Tracing	x
Ketju project [26]	Finland	Decentralized	Private & Public	Proximity Tracing	Selective Broadcasting
''Corona-Datenspende'' (Robert Koch Institut) [27]	Germany	Decentralized	Government	Data Tracking	Broadcasting
NZ Covid Tracer App [28]	New Zeeland	Decentralized	Government	Proximity Tracing	Selective Broadcasting
Aarogya Setu mobile app [29]	India	Decentralized	Government	Proximity and Location Tracing	Selective Broadcasting
Hayat Eve Sığar[30]	Turkey	Decentralized	Government	Proximity Tracing	x
''Hamagen'' app [31]	Israel	Decentralized	Government	Location Tracing	Unicasting
''TraceTogether'' app [14]	Singapore	Centralized	Government	Proximity Tracing	Broadcasting
''WeTrace'' app [32]	Switzerland	Decentralized	Private	Proximity Tracing	Selective Broadcasting
NHSX/University of Oxford tracking app [33]	United Kingdom	Decentralized	Government	Proximity Tracing	Selective Broadcasting
Covid Watch (Stanford University) [34]	United States	Decentralized	Public	Proximity Tracing	Selective Broadcasting
CoEpi [35]	United States	Decentralized	Private	Proximity Tracing	Selective Broadcasting
PeduliLindungi[36]	Indonesia	Decentralized	Private	Location and Proximity Tracing	x

Table 3 Summary of available Contact Tracing Mobile Applications.

CHAPTER 5

Proposing a Framework for evaluating contact tracing Applications

The proposed evaluation framework is a four-step method for assessing a specific contact tracing mobile application as appeared in Fig. 1. The figure portrays the diagrammatic portrayal of the framework and each progression is summed up in detail beneath. The point of my assessment model is to classify the contact tracing mobile applications so as to have the option to recognize every application effectively.

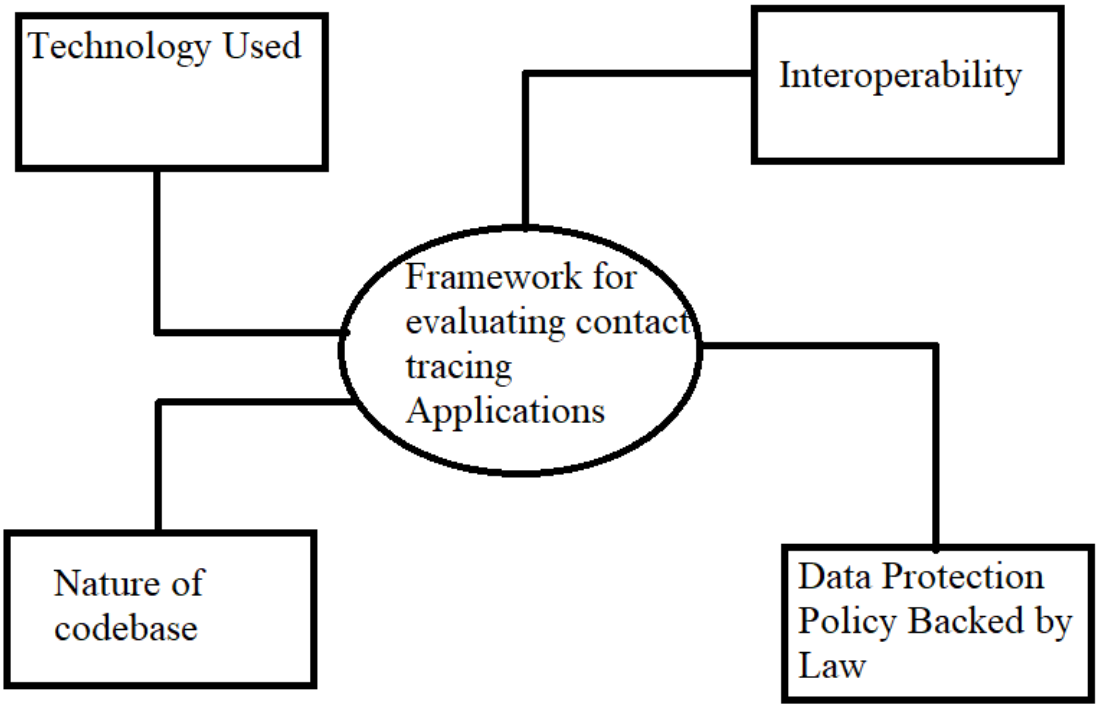


Fig 2: Contact Tracing Applications Evaluation Framework

5.1 Interoperability

Interoperability means whether the application has the ability to communicate with other 3rd party contact tracing solutions. In a connected world where citizens of a given country can easily travel to various destination and many private and non-government organizations also develop their own contact tracing solution, a contract tracing mobile application with interoperability can effectively perform contact tracing in a given location. Users do not have to install other contact tracing applications to stay safe and secured. I recognize the technical and logistic difficulties of creating an application that can communicate with all other contact tracing applications in the world but I expect countries

with close proximity and busy travel of its citizens among themselves should come up with a system or facilitate the devolvement of such contact tracing solutions that can easily communicate with each other.

5.2 Data Protection Policy Backed by Law

User data is a being called the new gold of 21st century. The accidental or deliberate leakage of any user data can pose a serious risk. The data collected by the contact tracing solution must be protected under the laws and respect the privacy of the user. The purpose of any contact tracing application and the mechanisms must be clearly expressed. There should exist a strong law nationwide that guarantees the proper usage and storage of data and taking user's consent. By doing so, user's data will be stayed safe and secured. The authority will not be able to misuse the data in any nefarious acts and the cases of an accidental data breach will be a minimum.

5.3 Nature of codebase (Open Source or Close Source)

Tracing the individuals who have had Covid-19 is a non-specialized issue that won't be fixed by just utilizing technology, obviously innovation and technology can give an apparatus to work with contact tracing. Public acknowledgment of the mobile application is additionally basic to their utility. Assuming that public confidence isn't accomplished, we hazard yoyoing among lockdowns and no lockdowns, at last drawing out the period of time where the economy will be affected.

The ethical necessity on the general population to use these applications will be high and governments in this manner hold a significant weight of responsibility for the decisions they make under their crisis environment, just as the drawn-out sway these will have. The best way to promise the public that their security is enough ensured and to accomplish this acknowledgment is to open source these mobile applications.

5.4 Technology Used

There are mostly three kinds of technology are being used in the evaluated contact tracing applications. There are (i) Wi-Fi (ii) Bluetooth and (ii) GPS. For a robust and fail-safe contact tracing solutions all three of this technology must be used. As mentioned before, Bluetooth may suffer connectivity issues in a house with thicker walls. GPS might not work all the time in indoors and Wi-Fi access points are rarely available outside. I propose, for a robust and fail-safe usage of contact tracing applications, proper technologies must be used.

CHAPTER 6

Evaluation of Mobile Contact tracing Applications with Recommendations

In this segment, considering the proposed evaluation framework, I assess and dissect a portion of the proposed contact tracing mobile applications. Be that as it may, there are sure contact tracing solutions where inadequate data is accessible. In spite of that, I have given brief synopses of the majority of the applications in Table 1. I will give recommendations of the contact tracing applications in light of my framework

App's Name	Interoperability	Data Protection Policy Backed by Law	Nature of Codebase	Technology Used	Recommendations
Private Tracer	Yes	Yes	Open Source	Bluetooth	1. Wi-Fi and GPS tracing technology should be added.
''Stopp Corona'' app	Yes	Yes	Open Source	Bluetooth	1. Wi-Fi and GPS tracing technology should be added.
NOVID20	Yes	Yes	Open Source	Bluetooth and GPS	1. Wi-Fi tracing technology should be added.
Ketju project	Yes	Yes	Open Source	Bluetooth	1. Wi-Fi and GPS tracing technology should be added.
''Corona-Datenspende'' (Robert Koch Institut)	Yes	Yes	Open Source	WiFi	1. Bluetooth and GPS tracing technology should be added.
NZ Covid Tracer App	No	No	Open Source	Bluetooth	1. Wi-Fi and GPS tracing technology should be added. 2. The app's source code

					should be made public 3. The app must have data protection policy which will be protected by necessary laws. 4. The app should be made interoperable with the neighboring countries' apps.
Aarogya Setu mobile app	No	x	Open Source	Bluetooth and GPS	1. Wi-Fi tracing technology should be added. 2. The app's source code should be made public 3. The app must have data protection policy which will be protected by necessary laws. 4. The app should be made interoperable with the neighboring countries' apps.
Hayat Eve Sığar	No	x	Close Source	Bluetooth	1. Wi-Fi and GPS tracing technology should be added. 2. The app's source code should be made public

					3. The app must have data protection policy which will be protected by necessary laws. 4. The app should be made interoperable with the neighboring countries' apps.
''Hamagen'' app	No	Yes	Open Source	GPS	1. Wi-Fi and Bluetooth tracing technology should be added. 2. The app should be made interoperable with the neighboring countries' apps.
''TraceTogether'' app	No	No	Open Source	Bluetooth	1. Wi-Fi and GPS tracing technology should be added. 2. The app must have data protection policy which will be protected by necessary laws. 3. The app should be made interoperable with the neighboring countries' apps.
''WeTrace'' app	No	No	Open Source	Bluetooth	1. Wi-Fi and GPS tracing technology should be added. 2. The app must have data

					protection policy which will be protected by necessary laws. 3. The app should be made interoperable with the neighboring countries' apps.
NHSX/University of Oxford tracking app	No	Yes	Open Source	Bluetooth	1. Wi-Fi and GPS tracing technology should be added. 2. The app should be made interoperable with the neighboring countries' apps.
Covid Watch (Stanford University)	No	Yes	Open Source	Bluetooth	1. Wi-Fi and GPS tracing technology should be added. 2. The app should be made interoperable with the neighboring countries' apps.
CoEpi	No	Yes	Open Source	Bluetooth	1. Wi-Fi and GPS tracing technology should be added. 2. The app should be made interoperable with the neighboring countries' apps.
PeduliLindungi	No	No	Close Source	Bluetooth and GPS	1. Wi-Fi tracing technology should be added. 2. The app must have data

					protection policy which will be protected by necessary laws. 3. The app's source code should be made public

Table 4 Evaluating various contact tracing application under proposed framework

CHAPTER 7

Potential attacks on contact tracing systems and their countermeasures

This segment presents a scientific classification of potential attacks on contact tracing systems. Other than that, recommendations on the potential countermeasures are also given.

5.1. Conventional attacks

This part classifies attacks dependent on their consensus unlike to those that are explicit to a specific application of a procedure. Be that as it may, there may be other potential attacks other than the ones I have examined in this part. The attacks examined beneath are normal and needn't be required with any high specialized arrangement.

5.1.1. Resource drain attack

Most contact tracing applications face resource drain attacks. The most notable is the Denial-Of-Service attack. In a resource drain attack, an attacker sends a colossal number of garbage requests from a lot of devices, compelling different gadgets to drain the energy if the message is invalid or drain the energy and capacity if the message is legitimate [37]. Such attacks don't influence the services given by contact tracing mechanisms, yet may prompt low performance of cellphones.

Countermeasures

Various countermeasures incorporate garbage request filtering, recognition of attack, and answering to the cell phone user that will assist with relieving the attacks brought about by resource drain attacks.

5.1.2. Trolling attacks

In trolling attacks, an attacker spreads fear of infection or disease exposure by making a claim of being in closeness to the diagnosed individuals [38]. As a result, the non-affected individuals will conduct tests and waste the resources of diagnostic centers, prompting the loss of trust in the contact tracing systems.

Countermeasures

The essential countermeasure incorporates attack location by health specialists. Further, a legitimate security component is needed to ensure that the attacker doesn't compromise a contact tracing application and accordingly forestall the spread of bogus news and rumors about an individual (trolling) or releasing individual data from such applications while associating with different devices for contact tracing.

5.1.3. Proximity app attack

Any contact tracing application on a smartphone can spill location data about an individual. A log of a user's proximity to different users could be utilized to show who they were with and surmise what they were doing [39]. The dread of divulgence of such location data may fear users from taking part in expressive action in public places.

Countermeasures

The application ought not to gather location data and time stamp data, and it should assemble time limits into their applications themselves, alongside customary registration with the users regarding whether they want to keep broadcasting.

5.1.4. Screen lock attack or ransomware

In this attack, hackers are utilizing counterfeit contact tracing applications to exploit android smartphones, subsequently abusing the worldwide pandemic to take bank details, photographs, recordings, and other private data [40]. For instance, CovidLock changes the password of the smartphone and requests a payment of $100 bitcoins for opening; else it threatens to erase their information for good or release their information to social media [28].

Countermeasures

Few countermeasures incorporate introducing anti-virus, never installing from an unauthorized application store, stop visiting any obscure sites, and so on

5.1.5. Backend impersonation

In backend pantomime, an attack is dispatched by an attacker device by taking on the appearance of another device and distorting its identity by changing its own character. It would then be able to publicize the inaccurate data to other participating devices prompting the making of loops in the data routing [41].

Countermeasures

Basic network protection systems are needed to forestall such attacks.

5.1.6. False injection or false report attack

In this attack, an attacker injects bogus information and exploits the correspondence of data among smartphones [42]. Bogus reports can be infused through exploited smartphones, consequently prompting low performance of any contact tracing applications. In COVID recognition components, when an attacker exploits more smartphones and consolidates all the acquired secret keys, the attacker can unreservedly produce the event reports.

Countermeasures

Successful filtering schemes, for example, interleaved hop-by-hop authentication, Statistical en-Route filtering, and so on are needed to moderate the effects of false data injection attacks [47,48].

5.2. Attacks specific to Bluetooth based solutions

Since mobile contact tracing use the way that there are billions of gadgets that are being used today equipped for Bluetooth based data trade, yet these gadgets are likewise presented to a ton of safety gives that are to be moderated for better utilization of these solutions. We have examined certain Bluetooth based assaults that can be dispatched with little arrangement. However, Zeadally et al. in [7] has sorted and further talked about a full scientific classification of assaults on Bluetooth. For quickness, I examine a few assaults that I feel are normal to this setting and afterward we momentarily expound on its potential countermeasures.

5.2.1. Bluejacking

In this sort of attack, Bluetooth communication system is taken advantage of by sending un-invited messages to those gadgets that have Bluetooth installed. The recipient has no information on the sender. The data it gets is the message alongside the name and model of sender's gadget. The messages sent doesn't do any damage to the client yet are really planned to make the client counter respond in a specific way or to add another contact in his gadget's address book [45].

Countermeasures

This attack can be stayed away from by setting the gadgets in non-discoverable mode or undetectable mode. Gadgets that are set in these modes are not vulnerable to this sort of attack [45]

5.2.3. Bluebugging

This attack is of most and genuine concern. In this sort of attack, the attacker gets unapproved access to a gadget, subsequently being fit for running commands or run unauthorized codes and so forth. This outcome is serious issues. This attack takes advantage of various bugs present in the firmware of typically previous generation Bluetooth to access the targeted gadgets [46]

Countermeasures

This sort of attack can be stayed away from by turning off the Bluetooth while it isn't being utilized. The attackers can possibly make access a device when Bluetooth is turned on. Another significant practice is to check every one of the received multimedia messages for potential viruses or malwares. The attackers normally obtain access by sending this kind of data or messages to it [46].

5.3. Attacks specific to geo location-based solutions

With the headway in advances, GPS (Global Positioning System) gadgets have gotten more reasonable and with the outcome our lives are turning out to be progressively subject to exact situating and timing. However, there have been a great deal of analysts that have demonstrated that GPS is defenseless against two fundamental attacks viz., sticking and ridiculing attacks. In this subsection, we examine these attacks against GPS and their countermeasures [47]

5.3.1. Jamming attacks

Jamming is the deliberate or inadvertent impedance of the signal that keeps it from being gotten, which is moderately easy to do [48]. The point is to overwhelm the incredibly feeble GPS signals so they can't be obtained and followed any longer by the GPS recipient, and greater part of GPS collectors don't execute any countermeasures against jamming.

Countermeasures

To countermeasure the jamming attack, we can utilize a notch filter or adaptive notch filter for GPS assault detection in contact tracing devices.

5.3.2. Spoofing attacks

In GPS spoofing, an attacker utilizes radio signals situated close to the gadget to meddle with the GPS signals so that it communicates no information at all or sends incorrect directions; subsequently making the area usefulness of cell phones, utilized for contact tracing applications, defenseless against spoofing assaults [49].

Countermeasures

Utilization of encrypted adaptations of the framework in the defense area, fundamental network safety standards to ensure different advanced threats in organizations and government, AI and other analytics to distinguish any dubious assaults, and so forth.

CHAPTER 8

Conclusion

The COVID-19 pandemic keeps on influencing the lifestyle of everybody. With developing interest for contact tracing solutions, it is the need of great importance to have one general solution that thinks about every one of the viewpoints. From security and privacy perspectives to legitimate and moral angles. However, the proposed solutions don't take a gander at all perspectives overall but instead center most around either. The principal concerns are identified with the user information the board, possibly non-insignificant bogus positive and negative occurrences, and the security and protection issues of these applications. Directed by these worries, this article introduced an outline of the three normal tracing application designs: concentrated, decentralized, and mixture; and an outline of mainstream applications inside these classifications.

I infer that Open-Sourceness is a significant boundary in keeping a solution straightforward in order to stay away from the abuse of an innovation for reconnaissance, embeddings secondary passages or being utilized as a Trojan pony. The need of great importance recommends an overall solution and its wide reception i.e., Standardization.

CHAPTER 9

Appendices

See **Table 3**.

Reference

[1] Hsu, L. Y., Lee, C. C., Green, J. A., Ang, B., Paton, N. I., Lee, L., Villacian, J. S., Lim, P. L., Earnest, A., & Leo, Y. S. (2003). Severe acute respiratory syndrome (SARS) in Singapore: Clinical features of index patient and initial contacts. Emerging Infectious Diseases, 9(6), 713–717. https://doi.org/10.3201/eid0906.030264

[2] Report of clustering pneumonia of unknown etiology in wuhan city, wuhan municipal health commission. (2019) [Online]. http://wjw.wuhan.gov.cn/front/web/showDetail/2019123108989

[3] Raskar, R., Schunemann, I., Barbar, R., Vilcans, K., Gray, J., Vepakomma, P., Kapa, S., Nuzzo, A., Gupta, R., Berke, A. et al. Apps gone rogue: Maintaining personal privacy in an epidemic. (2020). arXiv preprint arXiv:2003.08567.

[4] Altuwaiyan, T., Hadian, M., & Liang, X. (2018). EPIC: Efficient privacy-preserving contact tracing for infection detection. In IEEE International Conference on Communications (ICC), 2018 (pp. 1–6). IEEE Publications.

[5] Berke, A., Bakker, M., Vepakomma, P., Raskar, R., Larson, K., & Pentland, A. Assessing disease exposure risk with location histories and protecting privacy: A cryptographic approach in response to a global pandemic. (2020). arXiv preprint arXiv:2003.14412.

[6] Kampf, G., Todt, D., Pfaender, S., & Steinmann, E. (2020). Persistence of coronaviruses on inanimate surfaces and its inactivation with biocidal agents. Journal of Hospital Infection, 104(3), 246–251. https://doi.org/10.1016/j.jhin.2020.01.022

[7] Zeadally, S., Siddiqui, F., & Baig, Z. (2019). 25 years of Bluetooth technology. Future Internet, 11(9), 194. https://doi.org/10.3390/fi11090194

[8] Security and privacy issues with GPS tracking. (2020) [Online]. Navigation.

[9] Warner, J. S., & Johnston, R. G. (2002). A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. Journal of Security Administration, 25(2), 19–27.

[10] Solove, D. J. (May 2008). Understanding privacy. Harvard University Press.

[11] Sweeney, L. (2002). k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), 557–570. https://doi.org/10.1142/S0218488502001648

[12] Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In. Lecture Notes in Computer Science. Springer, 265–284. https://doi.org/10.1007/11681878_14

[13] Shannon, C. E. (1949). Communication theory of secrecy systems. Bell System Technical Journal, 28(4), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[14] TraceTogether. (2020) [Online]. https://www.tracetogether.gov.sg/. Retrieved November 1 2020

[14] Vaudenay, S. (2020) [Online]. Analysis of DP3T. https://eprint.iacr.org/2020/399. Retrieved November 1 2020

[15] Tang, Q. Privacy-preserving contact tracing: Current solutions and open questions. (2020). arXiv preprint arXiv:2004.06818.

[16] Saudi Heart Association-3 Standard: Permutation-Based Hash and Extendable-Output Functions. (2015) [Online]. https://www.nist.gov/publications/sha-3-standard-permutation-based-hash-and-extendable-output-functions?pub_id=919061 Retrieved February 18 2021

[17] Diffie, W., & Hellman, M. (November 1976). New directions in cryptography. In IEEE Transactions on Information Theory, 22(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

[18] Hamilton, I. A. (2021). 11 Countries are now using people's phones to track the coronavirus pandemic, and it heralds a massive increase in surveillance. http://www.businessinsider.com/countries-tracking-citizensphonescoronavirus-2020-3?r=DE&IR. Retrieved February 18 2021

[19] Privacy-preserving cross-border contact tracing. (2021) [Online]. https://bluetrace.io/. Retrieved February 18 2021

[20] Privacy-preserving cross-border contact tracing. (2021) [Online]. https://bluetrace.io/. Retrieved February 18 2021

[21] TraceTogether. (2021) [Online]. safer together. https://www.tracetogether.gov.sg/. Retrieved February 18 2021

[22] Privacy Tracer. (2021) [Online]. https://www.privatetracer.org/. Retrieved August 10 2021

[23] Meet the stop corona. (2020) [Online]. https://www.roteskreuz.at/site/meet-the-stopp-corona-app/. Retrieved August 10 2021

[24] The private way of tracing contacts. (2021) [Online]. https://www.novid20.org/en. Retrieved August 10 2021

[25] How close were you and for how long—Were you exposed? This is how the official corona app works, which may soon be on your phone as well. (2021) [Online]. https://yle.fi/uutiset/3-11299573. Retrieved August 10 2021

[26] Corona data donation. (2021) [Online]. https://corona.datenspende.de/. Retrieved August 10 2021

[27] NZ COVID Tracer app. (2021) [Online]. https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus/covid-19-resources-and-tools/nz-covid-tracer-app/. Retrieved August 10 2021. Ministry of Health, New Zealand.

[28] Aarogya setu mobile app. (2021) [Online]. https://www.mygov. in/aarogya-setuapp/. Accessed August 10 2021.

[29] hayatevesığar. (2021) [Online]. https://hayatevesigar.saglik.gov.tr/hes-eng.html/. Retrieved August 10 2021

[30] Health ministry launches phone app to help prevent spread of coronavirus. (2021) [Online]. https://www.timesofisrael.com/health-ministrylaunches-phone-app-to-help-prevent-spread-of-coronavirus/. Retrieved August 10 2021

[31] WeTrace. (2021) [Online]. Community Tracing App; A marriage between technology and the bayanihan spirit! https://www.wetrace.ph/ Retrieved August 10 2021

[32] Using a mobile app for contact tracing can stop the epidemic. (2021) [Online]. https://045.medsci.ox.ac.uk/mobile-app. Retrieved August 10 2021

[33] Reduce the spread of COVID-19 without increasing the spread of surveillance. (2021) [Online]. https://covid-watch.org/. Retrieved August 10 2021

[34] CoEpi. (2021) [Online]. https://github.com/Co-Epi. Retrieved August 10 2021

[35] PeduliLindungi. (2021) [Online]. https://pedulilindungi.id/. Retrieved August 10 2021

[36] Countries in the world by population. (2021) [Online]. https://www.worldometers.info/world-population/population-by-country/. Retrieved February 18 2021

[37] Brownfield, M., Gupta, Y., & Davis, N. (2005). Wireless sensor network denial of sleep attack. In Proceedings of the From the Sixth Annual IEEE SMC Information Assurance Workshop, IEEE (pp. 356–364).

[38] Gaus, A. (2012). Trolling attacks and the need for new approaches to privacy torts. U.S.F.L.Rev., 47, 353.

[39] Halevi, T., Ma, D., Saxena, N., & Xiang, T. (2012). Secure proximity detection for NFC devices based on ambient sensor data. In. Lecture Notes in Computer Science European Symposium on Research in Computer Security. Springer, 379–396. https://doi.org/10.1007/978-3-642-33167-1_22

[40] Andronio, N., Zanero, S., & Maggi, F. (2015). Heldroid: Dissecting and detecting mobile ransomware. In. Lecture Notes in Computer Science International Symposium on Recent Advances in Intrusion Detection. Springer, 382–404. https://doi.org/10.1007/978-3-319-26362-5_18

[41] Coronavirus stimulus scams are here. How to identify these new online and text attacks. (2021) [Online]. https://www.cnet.com/how-to/coronavirus-stimulus-scams-are-herehow-to-identify-these-new-online-and-text-attacks/. Retrieved February 18 2021

[42] Wood, P. (2021) [Online]. Web application hacking: Exposing your backend. https://www.helpnetsecurity.com/2003/11/11/web-applicationhacking-exposing-your-backend/. Retrieved February 18 2021

[43] Yu, Z., & Guan, Y. (2005). A dynamic en-route scheme for filtering false data injection in wireless sensor networks. In Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems (pp. 294–295).

[44] Kaviarasu, S., & Muthupandian, P. (2016) [Online]. Bluejacking technology: A review. Int. J. Trend Res. Dev. (IJTRD). https://www.ijtrd.com/papers/IJTRD6518.pdf, 3(6) (ISSN: 2394, 9333).

[45] Padgette, J., Bahr, J., Batra, M., Holtmann, M., Smithbey, R., Chen, L. et al. (2017). Guide to Bluetooth security (NIST Special Publication 800-121 Revision 2). National Institute of Standards and Technology.

[46] Dhuri, S. (2017). Bluetooth attack and security. Int. J. Curr. Trends Eng. Res., 3, 76–81.

[47] Nighswander, T., Ledvina, B., Diamond, J., Brumley, R., & Brumley, D. (2012). GPS software attacks. In Proceedings of the 2012 ACM Conference on Computer and Communications Security (pp. 450–461).

[48] Vadlamani, S., Eksioglu, B., Medal, H., & Nandi, A. (2016). Jamming attacks on wireless networks: A taxonomic survey. International Journal of Production Economics, 172, 76–94. https://doi.org/10.1016/j.ijpe.2015.11.008

[49] Warner, J., & Johnston, R. (2003). GPS Spoofing countermeasures, Homeland. Security Journal, 25(2), 19–27.

Turnitin Originality Report

Processed on: 10-Sep-2021 19:47 +06
ID: 1645281551
Word Count: 8454
Submitted: 1

Similarity Index	Similarity by Source
15%	Internet Sources: N/A Publications: N/A Student Papers: 15%

Usability of Smart Phone based ~~Contact Tracing in fighting~~ Pandemics such as Covid 19; ~~Issues and solution By~~ Bhudipta Tarafder

2% match (student papers from 03-May-2021)
Submitted to University of Adelaide on 2021-05-03

1% match (student papers from 16-Oct-2020)
Submitted to Study Group Australia on 2020-10-16

1% match (student papers from 26-Oct-2020)
Submitted to Charles Sturt University on 2020-10-26

1% match (student papers from 03-Jun-2020)
Submitted to British University in Egypt on 2020-06-03

1% match (student papers from 16-Feb-2021)
Submitted to IIHMR University on 2021-02-16

1% match (student papers from 07-Sep-2018)
Submitted to University of Hong Kong on 2018-09-07

< 1% match (student papers from 19-Oct-2020)
Submitted to Study Group Australia on 2020-10-19

< 1% match (student papers from 30-Apr-2019)
Submitted to Study Group Australia on 2019-04-30

< 1% match (student papers from 22-Oct-2020)
Submitted to University of Western Sydney on 2020-10-22

< 1% match (student papers from 01-May-2021)
Submitted to University of Queensland on 2021-05-01

< 1% match (student papers from 26-Oct-2020)
Submitted to University of Queensland on 2020-10-26

< 1% match (student papers from 11-May-2020)
Submitted to Napier University on 2020-05-11

< 1% match (student papers from 23-Jun-2020)
Submitted to University of Johannesburg on 2020-06-23

< 1% match (student papers from 25-Mar-2020)