# Covid-19 Contact tracing using BLE and RFID for Data Protection and Integrity

Harish Anantharajah [1], Karanveer Harika [1], and Andrew Jayasinghe [1]

[1]Computer Information Technology, British Columbia Institute of Technology, Vancouver, Canada

*Abstract*—**Responding to the rapid spread of the COVID-19 virus, the need for contact tracing and self isolation has become the focus of many health experts and governments as being the primary option for containing the spread of the disease. The utilization of the smartphone has been the focus of many efforts, by creating mobile applications that harness the potential of GPS and BLE technologies in order to make the process of contact tracing as efficient and effective as possible. The prevailing issue with this system is the concern of privacy and data protection of app users. in order to address this problem, through this paper, we are suggesting the use of passive RFID technology similar to that of most public transit systems. This system contains a client-held RFID card as well as a reciever and a server that processes the data. Through this paper, we hope to present an alternative, less invasive system that will help governments and health officials prevent the spread of COVID-19 in their communities.**

***Keywords* — *Contact Tracing, Radio Frequency Identification, Passive RFID Tracking.***

## I. Introduction

Since the outbreak of COVID-19, many countries implemented strict lock down measures to contain the spread of the virus [1]. While months of lock down measures have slowed the spread of the disease, it has also taken a significant economic toll on a global scale [1]. Increasingly, many nations are coming to the conclusion that while the strict lock-down measures are effective in combating the spread of the disease, it cannot go on forever. Each lock-down takes a significant toll on the socioeconomic fabric of each community. Therefore after careful analysis and consideration, many nations are resorting to a contact tracing model that is combined with strict-precautionary measures in place in order to return to a new sense of normalcy. Contact tracing refers to the process of rapidly tracking down and self isolating those that came into contact with an infected individual thereby effectively limiting the spread of the virus in the greater public [2]. The importance of contact tracing is highlighted in the long incubation periods of the virus which causes those infected to be asymptomatic. This makes them carriers of the disease while being unaware of their infection [3].

Currently, the most widely used and technically advanced system in place to track and trace infected/potential carriers, is the mobile application system [4]. These apps have a dual purpose. Firstly, They allows government agencies and health authorities to keep track of infected or potentially infected individuals and secondly, it allows users to identify potential exposures and contact points with infected individuals which allows them to monitor themselves for symptoms and take the necessary precautions. Although certain details and specifications of this system may vary depending on the locality of use, the fundamental concept remains similar.

There are a few existing problems with the app based approach. Although in most countries where there are strict privacy regulations to comply with and the apps are designed with privacy as the main constraint, the sensitive data of the user has been vulnerable [5]. Another drawback of this approach is hard to reach the required critical mass needed for effective contract tracing which is typically 60% of the population [5]. In addition to this, these apps also require a continuous flow of data acquisition such as GPS, mobile data and at times even Bluetooth connectivity which increases the device battery consumption.

The primary contribution of this paper consists of firstly, analyzing the existing COVID-19 contact tracing implementations and their vulnerabilities and drawbacks with an emphasis on an individual user data protection while attempting to successfully implement COVID-19 Contact tracing protocols [6]. Secondly, through the analysis of the vulnerability points in data protection of existing systems for contact tracing, we aim to provide necessary solutions that can resolve the data vulnerability issues while maintaining the primary focus on contact tracing to prevent the spread of COVID-19. The paper is divided into the following sections. In Section 1, we describe the importance of contact tracing while also addressing the data vulnerability issues in the existing systems which will be followed by Section 2 where we will be discussing related works that address the importance of user-data protection while enabling Health authorities to perform contact tracing in order to slow the spread of the disease. In section 3, we will be introducing our concept for contact tracing while maintaining data protection at its core. Finally we will be concluding our paper with an analysis of the benefits and drawbacks of the proposed system.

## II. Related Works

There have been various amounts of studies on finding the most effective method to contact tracing. There are several methods pertaining to digital contact tracing solutions most of which are mobile applications. Many of these apps would be based on GPS tracking or Bluetooth token sharing. The authors in [7], [8] take the approach of using Bluetooth low energy signals (BLE). They determine that a contact has been made if the range between phones is less than 6 feet. The problem with this application is accurately determining the range between the RF devices. They propose solving the problem by leveraging two key aspects: i) relative carriage of the devices (if devices are hand-held or laying in pocket) and ii) signal power (using multiple measurements of received signal power). GPS technology on the other hand, is not a viable solution for many reasons. The main reason being spoofing attacks [9]. Spoofing attackers could easily create a false GPS signal with an incorrect time and location to a receiver. Other reasons being ethics and privacy concerns.

There has been a study [10], [11] done on healthcare workers using contact tracing to identify potentially exposed workers. Staff were equipped with Real-Time Location System (RTLS) tags that could be located and identified. All patient rooms were fitted with location exciters and wireless access points. When a staff member passed a location with an exciter in place, the tag would receive a low-frequency signal and transmit a radio frequency to the access point. This would determine the exact location and room of the RTLS tag. Health care workers can experience contact with 14-18 persons in a work shift. Inpatients with a laboratory-confirmed diagnosis of COVID-19 infection were identified through the hospital's laboratory information system, and on-duty medical and nursing staff were identified from the RTLS tags.

In this work, data protection and security is the main priority. We apply the same principles used in [12] using new and innovative data encryption and Bluetooth technology. We mask all user information whereas it would not require much personal information. In [12] the authors state that sensitive location data such as GPS or radio cell data is not necessary nor useful. The only point of interest that really matters whether two people have come into close enough contact to risk an infection. An example of this is in [13] where they have contact tracing on "contact points". It is a smartphone app to create checkpoints of QR codes that can be scanned by all app users. The data collected from this app could let us know possible transmission paths. Our methods will use BLE signals with an emphasis on data protection as we are catered towards gathering more users and heavily dependent on public support.

## III. Problem Statement

The most fundamental drawbacks of the current application based tracing method is the security of private user data. Individuals that use such applications consent to the agencies and entities that use their data without completely knowing the ramifications of a potential breach in data security. We will be using a hybrid implementation of RFID cards and BLE transmitters that give users complete control over the amount of information that can be accessed by interested entities.

### A. Mobile Application

The current system relies heavily on users that are using smartphone technology. The main platforms that are utilized for the current contact tracing system are the IOS and Android platforms [14]. Most countries use their own proprietary Mobile applications A few examples would be ArriveCan (Canada), Immuni (Italy), COVIDTrace (Australia) and CoronaMelder (Netherlands) to name a few.

All of these applications are readily available on both the Android and IOS Application store for users to download. Some of these applications are mandatory requirements in certain countries and failing to register may have minor and in rare cases severe penalties [15].

In the modern digital environment, privacy and data protection is at the forefront of daily conversation and the lack of it, is also a growing fear amongst many smartphone users. Most of the applications are paired with government servers and use both or either Bluetooth Low Energy (BLE) and GPS technologies to track user movements [16]. Despite the fact that both of these technologies consume both cellular data/WiFi and battery power, the prospects of users constantly transmitting this data is unlikely. On top of that, the potential for misuse by the state, for mass public surveillance is also a risk factor [17]. These methods have also not taken into consideration the smaller group of the population that is largely remains disconnected from modern digital infrastructure [18]. The constant location transmission and Bluetooth activation capabilities of modern smartphones that [19] is demanded by these applications also increases the risk of potential malicious actors performing man-in-the-middle attacks that intercept traffic that is being transmitted through Bluetooth and WiFi technologies.

### B. Digital infrastructure

The storage of such large quantities of personal data is also a concern for many information security professionals. The use of big data in contact tracing apps appears to expand the scope of traditional concerns about anonymity, [20] as the data collected might be detailed enough to identify and track specific individuals. Apple and Google have proposed a decentralized system [21] of data storage to help protect privacy which involves information stored on user devices rather than in a centralized database while some governments are opting for a centralized approach instead. In the UK, the National Health Services [22] contact tracing app has been criticized for employing a central computer server to store data, which increases the likelihood of malign actors accessing and using personal information for malicious purposes.

In November 2019, security [23] researchers reported a critical vulnerability affecting Android 8, 8.1 and 9. Dubbed Blue-Frag, which allowed attackers in possession of a device's Bluetooth MAC address to remotely execute code when Bluetooth was enabled on said device. This in turn opened up opportunities for them to steal personal data or spread malware. Although a patch was made available in February of this year, there is never any guarantee that malicious actors will not discover new vulnerabilities in the Bluetooth protocol. In the summer of 2019, Apple [24]was also forced to patch a vulnerability after researchers discovered it was possible to snoop on communications between Bluetooth devices and even modify their content. Weaknesses in both operating systems could allow hackers to identify COVID-19 positive users of contact tracing apps or help advertisers track them.

Putting aside doubts over the efficacy of contact tracing apps, the question of whether the intended benefits of digital tracing outweigh the potential security risks of such a system remains unanswered [25]. app users would need to regularly update their devices' firmware to ensure the patching of any vulnerabilities, as well as verifying the permissions requested by the app. Additionally app developers and governments need to swiftly address weaknesses and ensure back-end databases are secure. Furthermore, smartphone users would need to remain vigilant to the potential threat posed by spoofed apps developed by cyber threat [26] agents. With the knowledge that no IoT device is ever truly safe, we propose a much simpler solution that involves more user control over the amount of information they transmit over mediums such as the internet and even BLE.

## IV. RFID and BLE Implementation

The use of Radio Frequency Identification technology has been increasing in popularity due to its versatility and cost effectiveness [27].Over the years, the RFID technology has come a long way since it was first introduced during the 1940s, to become more efficient while continuing to decrease in cost compared to BLE Interfaces [28] due to its simplicity and reduced consumption of resources. The technology is currently being widely used in the Metro Vancouver transportation system [29]. The process is quite clear and simple in nature and is as follows.

- The system is equipped with RFID readers on all entry point in its network. These include train stations, Busses and Ferries [30].
- Each user of the transport system requires an RFID tag which can be purchased in the form of a plastic card, wrist band or paper tag.
- At the point of entry into the network, the RFID tag which can be in the form of a card, band or tag is placed against the reader and the fare is then deducted [30].

Currently the cost to purchase the Plastic RFID card is at 5 Canadian dollars. This card which is also known as the Compass Card, is the most widely used form of the passive RFID technology. The benefits of using such a technology as passive RFID are immense [31]. The technology requires no internal or external power source which makes it cheaper to produce and easier to carry. In essence, the compass card is carried by thousands of people, in their pockets along with bank cards among other things. This means that users are able to use this technology without any form of technical expertise while also remaining completely independent from smartphone technology. Our proposal is to implement a simple process using this elegant technology which will prove to be useful to health services when tracking potential infections. The primary system will contain 2 major components which are as follows.

1) The hardware components of the system
2) The web/software based component of the system

### A. Hardware Components

This will be the physical devices and components that the users of the system will primarily be using. The system will comprise two primary components. The first is the RFID reader which will be stationed initially at restaurants and Gyms among other heavily trafficked indoor venues. The objective is to start with a small sample size and gradually increase it as we gather more data. These readers will be used to scan the second hardware component which is the RFID card that will be carried by the user. This card will be about the same size as the current compass card and ATM cards issued by most banking institutions. This card will be using passive RFID technology which works with no internal power source and is instead powered by the electromagnetic energy transmitted from the RFID reader. The lower price point and ease of use for this technology makes employing passive RFID cards the better choice. The RFID card will contain an alpha-numeric or numerical serial number which is used to register the card to a particular user. This is much like the bank card system where each card is unique and is registered under a particular user. This would ensure that each user is able to be identified in case of a potential outbreak through the serial number of the RFID card. Both these components will be unusable unless they are linked to real data that is translated into names and contact information that is to be used by health agencies in case of potential exposure. Below is a simple diagram of how the card is used together with the reader at a selected location.

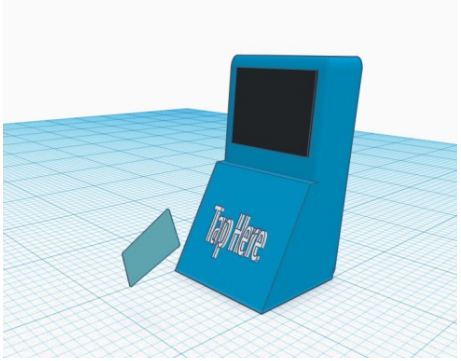

Fig. 1. Card and Reader

### B. BLE Add-on

As an additional/secondary feature, we aim to utilize Apple and Google Bluetooth Low Energy API systems alongside RFID scanning technology. BLE will determine that a contact has been made if the range between phones is less than six feet. Any contact made will be directly posted into our database infrastructure. In our mobile application, the user will have the ability to mark themselves as positive with COVID-19. If one person tests positive for the virus, they could tell the app they have been infected, and it could notify other people whose phones passed within close range in the preceding days. All users that have been affected will keep their information private and anonymous. Our servers only maintain the database of shared keys, rather than the interactions between those keys. The system also takes a number of steps to prevent people from being identified, even after they have shared their data.

- The app regularly sends information out over Bluetooth, it broadcasts an anonymous key rather than a static identity, and those keys cycle every 15 minutes to preserve privacy.
- Even once a person shares that they have been infected, the app will only share keys from the specific period in which they were contagious.
- This BLE app would not track people's physical location. It would basically pick up the signals of nearby phones at 5-minute intervals and store the connections between them in a database

This feature is considered an add-on because users may not be comfortable with this aspect and may not comply. This feature has also been to cause battery life to drain quickly on mobile devices. Overall this feature acts as a bonus and will provide an added layer of protection and safety. The figure below is a outline of how the BLE technology will interact with our RFID system.

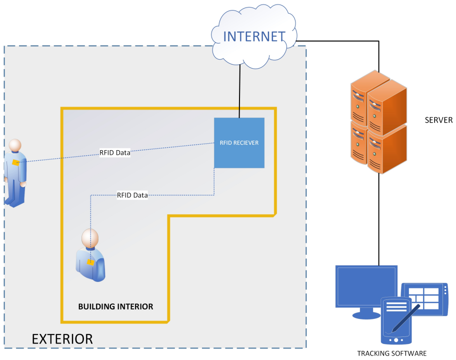

Fig. 2. Network Diagram

### C. Web/Software Component

This is essentially the brains of the operation and is where the data transfer and monitoring will occur. Once a user purchases the RFID card, they will have to register themselves along with the card through a web based portal.The registration process is quite straightforward and will require basic information from the user. Because it is imperative for health agencies to contact potentially infected persons as soon as possible, the user will be asked to provide a valid cellphone number and a valid email address which will be verified by using a two factor authentication system.

The users will only need to provide a valid cellphone number, a valid email address and their full name. Details such as residential address and household information may only be requested once a potential infection is confirmed and further tracing is necessary to contain the spread. This ensures complete data integrity for the users in case of any security breach.

The client side portal where users register will contain a dashboard with all of the recent locations where the card was used and will present the user with accurate and timely data regarding any relevant updates such as potential exposures. In case a potential infection is discovered at a venue where the user had visited, the health authorities would be able to immediately contact any user that may have been exposed to the contagion. On the end of the RFID reader, is a different approach to the problem. The locations containing the readers will need infrastructure such as a functional internet network connection as well as power supplies for the micro computers that will process the data that is obtained by the readers and transmit that data into the government servers. Initial roll out for the cards will be available at selected vendor locations such as grocery stores and pharmacies.The user flow of the system will be as follows.

- A user purchases a card from a selected vendor location.
- Next, the user goes to the web portal to register themselves thus linking and activating the card purchased.
- Once the card has been registered, the card is activated by the authoritative body and all relevant information of the user such as their phone number, name and email address, along with the serial number of the card is entered into the database of the user
- Now that the card is active and linked to an individual, all they have to do is tap the card on the reader when entering a reader available location.
- Once tapped, the serial number of the card is sent by the reader and the processor to the authoritative server which updates the database for the given card by entering the location of the reader.

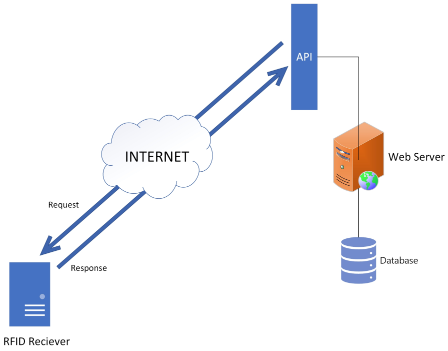

Fig. 3. Web Components

### D. Further Technical Details

Passive RFID tags do not all operate at the same frequency. There are three main frequencies within which passive RFID tags operate. The frequency range, along with other factors, strongly determines the read range and attachment materials [31].

- 125 - 134 KHz – Low Frequency (LF) – An extremely long wavelength with usually a short read range of about 1 - 10 centimeters.It is not affected much by water or metal [31].
- 13.56 MHz – High Frequency (HF) and Near-Field Communication (NFC) – A medium wavelength with a typical read range of about 1 centimeter up to 1 meter. This frequency is used with data transmissions, access control applications, DVD kiosks, and passport security – applications that do not require a long read range [32].
- 865 - 960 MHz – Ultra High Frequency (UHF) – A short, high-energy wavelength of about a one meter which translates to long read range. Passive UHF tags can be read from an average distance of about 5 - 6 meters, but larger UHF tags can achieve up to 30+ meters of read range in ideal conditions. This frequency is typically used with race timing, IT asset tracking, file tracking, and laundry management as all these applications typically need more than a meter of read range [32].

As a general rule, higher frequencies will have shorter, higher-energy wavelengths and, in turn, longer read ranges [32]. Moreover, the higher the frequency, generally speaking, the more issues an RFID system will have around non-RFID-friendly materials like water and metal.For our system, we will be using the 13.56 MHz or HF and Near Field Communication range. This is because of the adequate distance required for reading which can extend to as far as 1 meter and for the durability that the tags may have when contacted with water and other non-RFID-friendly materials. For the database will be hosted in a government data-center and each time the user taps their card on a reader, the serial number of the card will be uploaded to the server. the server will receive the inbound traffic and insert the location data of the reader into the database of the relevant card. While the BLE feature will be an extra feature that will be beneficial for the overall system, it does not contain any location data which is useful for the health authorities to use for contact tracing, which is why the RFID reader location data is a necessary aspect of all data sent by the receivers to the server. Figure 3 below shows the higher level functionality of how the different components of the system work together to provide a reliable network of information that may prove essential to in preventing the spread of the virus.

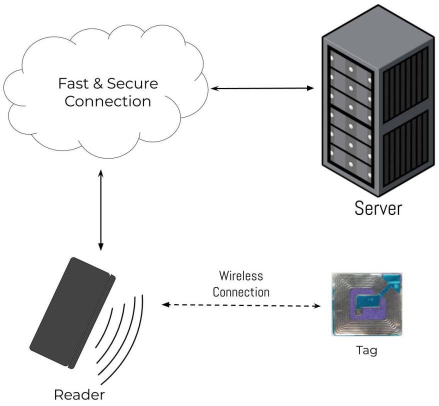

Fig. 4. System Components

## V. Simulations

Since there is no existing large scale, public implementation of the RFID system, we plan to analyze existing smaller scale implementations of both the BLE and RFID tracking technologies. By doing so, we will be able to effectively calculate the potential costs incurred as well as the logistical numbers and most importantly, the effectiveness of the technology in preventing the spread of the disease. A concept known as Real-Time Location system is being used in a variety of industries at the moment. The technology was initially developed for the warehousing sector but has since been implemented in many smaller scale applications. The concept uses a host [33] of technologies, one of which include passive and RFID tracking. For the purpose of our simulations, we will be using data obtained through the implementation of this process. In addition to this, we will also be analysing roll out and implementation options from multiple entities that have been successfully using the RFID system for commercial purposes such as Translink and other transport systems.

We will examine the data obtained by the metro Vancouver transit system's RFID component. The system which is known as the Compass card system, allows riders [38] to purchase the RFID card at selected vendors, and then load money onto the card and tap in at the RFID readers which are stationed in busses and stations. The system was primarily implemented to avoid fare evasion which existed with the former paper based system of tickets. The initial roll out included replacing all the manual fare gates at train stations with Automated gates that had integrated RFID readers as well readers on busses.

Initially the whole transit network comprised of a paper based, manual fare gate system, where enforcement of fare payment was done through manual fare gate attendants performing spot checks and enforcing transit policies. When the RFID system was introduced, the agency did not have the resources to implement the newer system on all transit locations simultaneously. Therefore the solutions was a phased implementation approach where they implemented the new system in phases which eliminated the need to shutdown mission critical systems network wide. This approach also provided great feedback to the agency [38]because they were able to compare both systems while they were in use simultaneously. The first phase involved upgrading 5 metro-train stations within a network of 50 at the time. this meant that the system would be introduced to the public at a slower pace. after the pilot phase which lasted for 2 months [39], they moved to implement the system in an entire route of a single rail-line. This phase meant that users that used that railway line, were now using the RFID card to pay for their fares. the total system was not completely implemented until 2 years after the first phase of the project began, but the phased approach provided the company with more time needed to analyse the user data and metrics. this also helped the company increase awareness regarding the system among transit users, which helped with the adaptability of such a novel concept among it's users.

The system had a total ridership [39] of about 915,000 by April 2016 and that number has gradually increased over the years. As of June 2016, there were 371 million taps of the compass card on the readers on fare gates at a rate of 1.5 million every weekday.The system had an initial cost of implementation was 90 million Canadian dollars [39]. By the time the old system was completely phased out and the compass card system was implemented, there was a 95% adoption rate. Currently, a user may purchase the RFID compass card for 5 Canadian dollars. An individual card may only be used by a single individual to ride the transit system.

After successful analysis of the studies conducted by various groups and the scopes of each study, we will be able to successfully extrapolate the potential results of the successful implementation of the RFID based contact tracing system.

The system implementation for our simulations would need to be conducted in phases. Phase 1 would include a small scale implementation of the systems with a single or dual server back-end which will cater to 1000 initial RFID cards with readers implemented in a select amount of highly trafficked areas. We would only be rolling out to one city at a time such as Burnaby. Phase 2 will increase the scale to about 10,000 cards with 10 servers processing card data. The amount of RFID readers would increase to many more high trafficked areas to issue more reliability and accuracy in the received data.

### A. Phase I

The current price of a single compass card is at 5 Canadian dollars for purchase [39]. The manufacturing rates of each card ranges between 0.50 - 0.85 cents. If we compare this to the cost of production for the RFID card used in our interface, we would have an initial roll out of 1000 cards in the City of Burnaby. This would aggregate a production cost for the cards between 500 - 850 Canadian dollars.

In addition to this, we would need card readers to be positioned at highly trafficked indoor locations such as restaurants, grocery stores, malls and apartments. An individual receiver has an average cost of 200 Canadian dollars. We would be spending an estimated amount of 5000 Canadian dollars for receivers placed in 25 locations [40]. The Servers will be hosted offsite which will be connected to onsite processors via the internet. The servers would be using cloud providers such as Amazon Web Services to collect and store all the data collected. This is a pay as you go level service, which means you only pay for what you use. The minimum payment tier which is known as the free tier, would give us 750 hours of free server instances and 5GB of Data Storage and 750 hours per month of Relational Database services for the data we collect from the receivers and cards. Once the allocated free tier runs out, the charge is per gigabyte of data per hour [41]. The selected locations RFID readers will process and transmit the data to our cloud infrastructure where we can then analyze and report of any outbreaks. [41].

### B. Phase II

In this phase, we would ramp up our roll out to 10,000 cards in Burnaby. This would aggregate a production cost for the cards at 5,000 - 8,500 Canadian dollars.

In addition to this, we would need to increase the amount of card readers to be positioned. We would be spending an estimated amount of 20,000 Canadian dollars for receivers placed in 100 more locations. The servers will be hosted offsite which will be connected to onsite processors via the internet. The server side costs will see an increase due to the large amounts of data that will be trafficked and stored on the servers. The on site processors will transmit the data to the same online cloud database hosted on Amazon Web Service.

## VI. Results

### A. Existing Data

We will start by analyzing data collected from the RTLS implementation in Tan Tock Seng Hospital in Singapore. The data collected was conducted by tracking a total of 796 patients and staff. [34] The study was conducted over a 2-day study period, all admitted patients with COVID-19, their ward locations, and the health care workers assigned to each ward were identified to determine the total number of potential contacts between patients with COVID-19 and health care workers. The numbers of staff-patient contacts determined by Medical record reviews and RTLS-based contact tracing were evaluated. The RTLS-based contact tracing method was further validated by comparing their sensitivity and specificity against self-reported staff-patient contacts by health care workers.The results obtained by the study were conclusive and are as follows.

The performance of the RTLS-based contact tracing method performed with moderate sensitivity of 72% and high specificity of 88%, While they did not specifically measure the time taken, [34] it was estimated that the RTLS data extraction time was approximately 2 to 3 minutes per patient. These findings are comparable to other studies validating the accuracy and ease of RFID technology in quantifying human contact episodes.

Of 796 potential staff-patient contacts (between 17 patients and 162 staff members), 104 (13.1%) were identified by both the RTLS and medical records (EMR), 54 (6.8%) by the RTLS alone, and 99 (12.4%) by the EMR alone; 539 (67.7%) were not identified through either method. Compared to self-reported contacts, EMR reviews had a sensitivity of 47.2% and a specificity of 77.9%, while the RTLS had a sensitivity of 72.2% and a specificity of 87.7%. The highest sensitivity was obtained by including all contacts identified by either the RTLS or the EMR (sensitivity 77.8%, specificity 73.4%) [34]. According to this study, in order to identify the number of staff members in contact with an infectious patient as accurately as possible, high test sensitivity is desired. Based on the study, RTLS-based contact tracing would be able to identify most contacts with exposure to a patient with COVID-19.

| System | Specifictiy | Sensitivity |
|---|---|---|
| EMR | 77.9% | 47.2% |
| RTLS | 87.7% | 72.2% |

Next, we will use a study conducted by Chang et al [35] which examined contact behavior between health caregivers and patients in order to reduce cross infections in healthcare institutions using Proximity sensing using radio frequency identification (RFID) technology. The study was conducted as follows. Firstly, the proximity sensing of RFID was tested, following which RFID technology was deployed in a Clinical Skill Center in one of the medical centers in Taiwan. Next, they simulated clinical events and developed a model using variables such as duration of time, frequency, and identity (tag) numbers assigned to caregivers. All clinical proximity events were classified into close-in events, contact events and invasive events. Observers were recruited to do real time recordings of all clinical events in the Clinical Skill Center with the deployed automated RFID interaction recording system. The observations were used to verify the model data [35]. There were a total of 193 events which validated the accuracy of RFID tag readers (80%) in detecting proximity events in the intensive care unit by comparing data obtained from direct observation; they demonstrated sensitivities ranging from 73.8%-90.9% as well as specifics ranging from 83.8%-98.0% for the technology used.They found no difference in the interaction duration between health care workers and patients with tuberculosis in airborne isolation when comparing records obtained from RFID network sensors, direct observations, and interviews.

| Range | Specifictiy | Sensitivity |
|---|---|---|
| High | 98.0% | 90.9% |
| Low | 73.8% | 83.8% |

A study conducted in China [36] showed that the use of RFID technology in the emergency department generated twice as many contacts compared with the conventional method of Electronic Medical Record review during a pertussis outbreak, and each RTLS data query required less than 5 minutes, compared to 30-60 minutes per Electronic Medical Record review.

Another study coducted in singapore [37] to compare the performance of the contact tracing app-TraceTogether-with that of a wearable tag-based real-time locating system (RTLS). The data was used to validate them against the electronic medical records at the National Centre for Infectious Diseases (NCID), the national referral center for COVID-19 screening.

All patients and physicians in the NCID screening center were issued RTLS tags (CADI Scientific) for contact tracing. In total, 18 physicians were deployed to the NCID screening center from May 10 to May 20, 2020. The physicians activated the TraceTogether app (version 1.6; GovTech) on their smartphones during shifts and urged their patients to use the app. They compared patient contacts identified by TraceTogether and those identified by RTLS tags within the NCID vicinity during a physicians' posting. They also validated both digital contact tracing tools by verifying the physician-patient contacts with the electronic medical records of 156 patients who attended the NCID screening center over a 24-hour time frame within the study period [37].

RTLS tags had a high sensitivity of 96.9% for detecting patient contacts identified either by the system or TraceTogether while TraceTogether had an overall sensitivity of 6.5% and performed significantly better on Android phones than iPhones (Android: 9.7%, iPhone: 2.7%; P¡.001). When validated against the electronic medical records, RTLS tags had a sensitivity of 96.9% and specificity of 83.1%, while TraceTogether only detected 2 patient contacts with physicians who did not attend to them.

| System | Specifictiy | Sensitivity |
|---|---|---|
| RTLS | 83.1% | 96.9% |
| App | 4.2% | 6.5% |

## VII. Final Analysis and Conclusion

Based in the results of the findings from various studies conducted, we can come to the following conclusions.

Of 1000 potential cardholders, we can speculate that with a sensitivity of 73.8%-90.9% which corresponds to 738-901 cardholders as well as specificities ranging from 83.8%-98.0% which corresponds to 838-980 cardholders accurately traced. These result were based on positive case contact tracing correlations conducted by previous studies in smaller settings. This value can be further elaborated to represent the phase 2 of our simulations with a sample size of 10,000 cardholders. Scaling up on the results obtained from these studies, we can concur that our system will prove effective in small cities with high population density. We will be able to accurately trace affected patients will high precision and reduce the number of COVID-19 transmissions.

We have demonstrated the feasibility of using Radio Frequency Identification together with Bluetooth Low Energy technologies to successfully perform contact tracing in order to contain the COVID-19 Contagion. We have highlighted the key features and functions of each technology we will be using in the system. We have also analysed studies and concepts that are currently using this technology in order to generate usable data that can be used to assess the feasibility and effectiveness of implementing the proposed system. Although we do not have practical simulation data of our own, we aim to continue to asses the practicality of the system and its effectiveness in the real world for future works.

## References

Please number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use "Ref. [3]" or "reference [3]" except at the beginning of a sentence: "Reference [3] was the first . . ."

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished" [4]. Papers that have been accepted for publication should be cited as "in press" [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

## References

[1] "Do Lockdowns Actually Work?" Gavi, The Vaccine Alliance, www.gavi.org/vaccineswork/do-lockdowns-actually-work.

[2] "Contact Tracing." BC Centre for Disease Control, www.bccdc.ca/health-info/diseases-conditions/covid-19/self-isolation/contact-tracing.

[3] L. Ferretti et al., "Quantifying dynamics of sars-cov-2 transmission suggests that epidemic control and avoidance is feasible through instantaneous digital contact tracing," medRxiv, 2020.

[4] R. Raskar et al., "Apps gone rogue: Maintaining personal privacy in an epidemic," arXiv preprint arXiv:2003.08567, 2020

[5] H. Cho et al., "Contact tracing mobile apps for covid-19: Privacy considerations and related trade-offs," arXiv preprint arXiv:2003.11511, 2020.

[6] "Major Security Flaw Uncovered in Qatar's Contact Tracing App." Amnesty International, www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw.

[7] Hatke, Gary F., et al. "Using Bluetooth Low Energy (BLE) signal strength estimation to facilitate contact tracing for COVID-19." arXiv preprint arXiv:2006.15711 (2020).

[8] Gvili, Yaron. "Security analysis of the covid-19 contact tracing specifications by apple inc. and google inc." IACR Cryptol. ePrint Arch. 2020 (2020): 428.

[9] Warner, Jon S., and Roger G. Johnston. "GPS spoofing countermeasures." Homeland Security Journal 25.2 (2003): 19-27.

[10] Ho, Hanley J., et al. "Use of a real-time locating system for contact tracing of health care workers during the COVID-19 pandemic at an infectious disease center in Singapore: validation study." Journal of Medical Internet Research 22.5 (2020): e19437.

[11] Ho, H. J., et al. "Validation of a Real-Time Locating System for Contact Tracing of Healthcare Workers during the COVID-19 Pandemic in Singapore." Journal of Medical Internet Research (2020).

[12] Abeler, Johannes, et al. "COVID-19 contact tracing and data protection can go together." JMIR mHealth and uHealth 8.4 (2020): e19359.

[13] Yasaka, Tyler M., Brandon M. Lehrich, and Ronald Sahyouni. "Peer-to-Peer contact tracing: development of a privacy-preserving smartphone app." JMIR mHealth and uHealth 8.4 (2020): e18936.

[14] "Europe eyes smartphone location data to slow virus spread [Internet] 2020", PBS Newshour, www.pbs.org/newshour/health/europe-eyes-smartphone-location-data-to-slow-virus-spread.

[15] "Digital government response to Covid-19", Government of Canada, www.canada.ca/en/government/system/digital-government/digital-government-response-to-covid-19.html.

[16] "How the Covid apps work", Government of Canada, www.canada.ca/en/public-health/services/video/covid-alert.html.

[17] ”How China Uses High-Tech Surveillance to Subdue Minorities”,New York Times, www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.

[18] ”Researchers explore contact tracing app for Coronavirus pandemic”, med-tech news, www.med-technews.com/news/researchers-explore-contact-tracing-app-to-contain-coronavirus.

[19] ”Cell phones self and other problems with big data detection and containment during epidemics”, Erikson SL, Medical anthropology quarterly Report.

[20] ”uk-contact-tracing-app-problem”,medicaladvice-network, www.medicaldevice-network.com/features/uk-contact-tracing-app-problems/.

[21] ”apple iphone google android contact tracing app upgrade”, Forbes.com ,www.forbes.com/sites/zakdoffman/2020/09/04/apple-iphone-google-android-contact-tracing-app-upgrade-release-phone-tracking-warning/.

[22] ”NHS Contact tracing app fails”, healthcareitnews, www.healthcareitnews.com/news/emea/nhs-covid-19-contact-tracing-app-fails-ask-users-self-isolate/.

[23] ”Contact tracing app unsafe if bluetooth vulnerabilities are not fixed”, zdnet.com, www.zdnet.com/article/contact-tracing-apps-unsafe-if-bluetooth-vulnerabilities-not-fixed/

[24] ”contact tracing app faces big technological-problems-in urban environments”,HillTimes.com, www.hilltimes.com/2020/08/24/contact-tracing-app-faces-big-technological-problems-in-urban-environments-studies-say.

[25] Jorge Ricardo, Nova Blanco, ToTran Nguyen, Martine Denis. ”CONTACT TRACING TOOLS FOR PANDEMICS.” Rega Institute KU Leuven 8.4 (2020): e19359.

[26] ”Coronavirus contact tracing apps, the problem and potential.”, Sky News, www.news.sky.com/story/coronavirus-contact-tracing-apps-the-problems-and-the-potential-11980579

[27] ”RFID beginners guide”, Atlas RFID Store, www.atlasrfidstore.com/rfid-beginners-guide/

[28] ”BLE vs RFID”, Airfinder.com, www.airfinder.com/blog/rtls-use-cases/ble-vs-rfid-how-to-select-asset-location-technology

[29] ”Translink skytrain fare gates”, Dailyhive.com, www.dailyhive.com/vancouver/translink-skytrain-fare-gates-rfid-universal-access-disabilities

[30] ”first handsfree fare gate solution”, rfidworld.com, www.rfidworld.ca/public-private-partnership-between-translink-and-hyperlight-systems-results-in-the-worlds-first-hands-free-fare-gate-solution

[31] ”Active vs Passive RFID”, Atlasrfid.com, www.atlasrfidstore.com/rfid-insider/active-rfid-vs-passive-rfid

[32] ”diference between Active vs Passive RFID”, serialio.com, www.serialio.com/support/learn-rfid/difference-between-active-and-passive-rfid-tags

[33] ”RTLS For Healthcare providers”, stanelyheathcare.com, www.stanleyhealthcare.com/hospitals-clinics/rtls/aeroscout-contact-tracing

[34] Jorge Ricardo, Nova Blanco, ToTran Nguyen, Martine Denis. ”Use of a Real-Time Locating System for Contact Tracing of Health Care Workers”, JMIR Publications

[35] Chang Y, Syed-Abdul S, Tsai C, Li Y. A novel method for inferring RFID tag reader recordings into clinical events. Int J Med Inform 2011 Dec;80(12):872-880

[36] Hellmich TR, Clements CM, El-Sherif N, Pasupathy KS, Nestler DM, Boggust A, et al. Contact tracing with a real-time location system: A case study of increasing relative effectiveness in an emergency department. Am J Infect Control 2017 Dec 01;45(12):1308-1311

[37] Zhilian Huang, Huiling Guo, Yee-Mun Lee , Eu Chin Ho, Hou Ang, Angela Chow . Performance of Digital Contact Tracing Tools for COVID-19 Response in Singapore: Cross-Sectional Study. JMIR Publications 2020 Oct 29 01;45(12):1308-1311

[38] ”Translink Smart Card”, ToolsofChange.com www.toolsofchange.com/en/case-studies/detail/713/

[39] ”5th anniverssary of compass card system”, Dailyhive.com, www.dailyhive.com/vancouver/translink-compass-card

[40] ”Contactless RFID technology”, www.crownsecurityproducts.com, www.crownsecurityproducts.com/time-clocks/fingerprint-time-clocks/

[41] ”AWS Free Tier Pricing”, www.aws.amazon.com, aws.amazon.com/free/?all-free-tier.sort-by=item.additionalFields.SortRankall-free-tier.sort-order=asc