IoT in COVID
BLE based Contact Tracing

Abdul Saboor
High Integrity Systems M.sc.)
Frankfurt University of Applied Sciences
Faculty of computer sciences and engineering
Email:

***Abstract* - (COVID-19)* is a severe global pandemic and its spread negatively impacted the human mobility patterns so there is a requirement to understand the disease spread patterns and its routes among neighboring individuals for the timely implementation of corrective measures at the required placement. Contact tracing is a time-tested technique employed successfully to control and monitor historical outbreaks of diseases. As a vital component of the COVID-19 management strategy, IoT-enabled contact tracing applications increase the effectiveness in support of monitoring and containment of the COVID-19 pandemic. This paper gives a literature-based review to a comprehensive analysis of digital contact tracing solutions in terms of their methodologies and technologies including the most prominent approach to contact tracing i.e. Bluetooth Low Energy (BLE) interface, and its adaptability for COVID-19 globally. Also, the challenges and limitations faced in terms of privacy, security, accuracy, and adaptability are discussed.**

***Index Terms* – Digital Contact Tracing, Internet of Things (IoT), Bluetooth Low Energy (BLE), Privacy**

1. Introduction

(SARS-CoV-2)** Virus and the associated disease COVID-19 represent the most significant public health threat in the last 100 years. Spreading like wildfire across the globe, this pneumatic botched down the world's economy. Strict lockdowns, shut down of industries, workers losing jobs, self-isolations, and risk of the spread with anew once, greatly affected human mobility. Preventive measures including smart lockdown strategies, putting international travelers under surveillance and quarantine, use of face masks, social distancing, and more importantly contact tracing made it possible for some countries to minimize the disease's spread.

Contact tracing is an essential component to support the early identification of new cases among the population and to contain outbreaks of the disease like COVID-19. [1]

Traditional approaches of contact tracing i.e. 'manual' & 'semi-manual, are extremely time-consuming, inefficient, highly error-prone, and not scalable.[2] Contact tracing using smartphone technology seems to be a powerful tool that may be employed to collect data and limit disease transmission during an epidemic or pandemic. These contact tracing apps trace individuals' meetups by either using a local Bluetooth connection or the global network of the Global Positioning System (GPS) for location tracking.

Big tech companies like Apple and Google have also made efforts to accelerate in expanding the capabilities of existing tracing frameworks. [3] Digital contact tracing platforms like IoT-based contact-tracing apps are thus emerging as an essential component of global response against the COVID-19. Figure 1 shows the critical merits of IoT for the COVID-19 pandemic. With the successful implementation of this technology, we expect an improvement in medical and contact tracing staff's efficiency with a reduction in their workload.

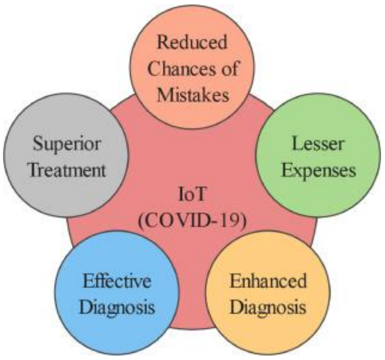

Figure 1: Key Merits of using IoT solution in combating COVID-19. [1]

***COVID: 'CO' stands for corona, 'VI' for virus, and 'D' for disease**
****SARS-CoV-2: Severe acute respiratory syndrome coronavirus 2**

2. IoT enabled Contact Tracing

Digital contact tracing is a framework in which smartphones close contacts with other ones, running the same contact tracing app. The architecture of the digital contact tracing framework is broadly classified into two types: centralized contact tracing and decentralized contact tracing. The main difference is the capacity to store the amount of information from wireless communication between users and the place of the decision-making process, remotely on a cloud server or locally in the users' device.[4]

2.1 Centralized Architectures

During the detection of proximity between users in a given location, by available wireless technology and distance measurements on the base of Received Signal Strength Indicator RSSI, If the measured distance is not according to WHO physical distancing recommendations and over a certain period, in close contact, users will exchange the 'Encounter message' through BLE, which contains the exchange of TempID; generated by the server for users after registering on the server, Phone Model, and Transmit Power (TxPower). Each device also records the Received Signal Strength Indicator (RSSI) and the timestamp of the message delivery. All encounter messages are stored locally and uploaded to the server. Infected users voluntarily inform the server and also provide health data to the server for verification. In a centralized architecture, the server is the unit that computes the likelihood of getting infected and sends an exposure notification to each user deemed highly likely to have been infected.

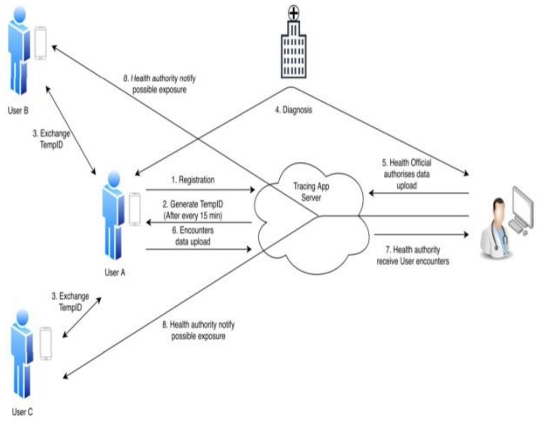
User B
8. Health authority notify possible exposure
4. Diagnosis
3. Exchange TempID
5. Health Official authorises data upload
1. Registration
Tracing App Server
2. Generate TempID (After every 15 min)
6. Encounters data upload
7. Health authority receive User encounters
User A
3. Exchange TempID
8. Health authority notify possible exposure
User C

Figure 2: Tracing apps centralised architecture.

2.2 Decentralized Architectures

In a decentralized approach, users are not required to register with the server. With the combination of current time and seeds, (used as input for a pseudorandom function) produced by phones to generate privacy-preserving pseudonyms or 'chirps' with a short lifespan. During the close interaction between the users 'chirps' have been shared among the users. Only infected users voluntarily upload their information of seeds and the relevant time information to the server. The server broadcasts the seeds of infected users to all other users or the app users can download any seeds uploaded by infected users from the server. Based on downloaded seeds from the server, users' app using pseudorandom calculations based on the seeds and discrete-time intervals between the start and expiry time device computes the likelihood to become infected and creates an exposure notification for the user. Sometimes these exposure notifications are also sent to the cloud server to collect statistics.

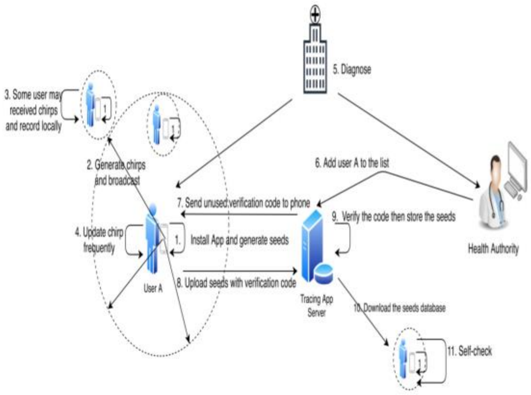
5. Diagnose
3. Some user may received chirps and record locally
2. Generate chirps and broadcast
6. Add user A to the list
7. Send unused verification code to phone
9. Verify the code then store the seeds
4. Update chirp frequently
1. Install App and generate seeds
Health Authority
User A
8. Upload seeds with verification code
Tracing App Server
10. Download the seeds database
11. Self-check

Figure 3: Tracing apps decentralised architecture.

3. Proximity Measurement Technologies in IoT for Contact Tracing

In terms of COVID-19, 1.5 meters of proximity with sufficient exposure to any COVID-19 patient may result in infection [5]. Therefore, correctly estimating the distance between two people and the duration of exposure is vital. Different technologies such as GPS [6], Bluetooth [7], and WiFi [8] help to estimate the physical distance and the extent of interactions.

Here we discuss the most incorporated technology in contact tracing for COVID-19.

4. BLE based Contact Tracing

Bluetooth BLE is a global short-range radio communications standard with a large ecosystem and with strong potential for the success of contact tracing applications.

Most of the contact tracing apps utilize BLE for contact tracing. The methodology is very simple; every time the contact-tracing app comes within the proximity of another app, it will locally save their information mutually. They may volunteer to share this contact information later with the health department.

4.1 **Bluetooth Low Energy (BLE) -** has become a dominant wireless communication protocol for proximity tracking. [9] In the BLE protocol definition, 40 channels, each 2 MHz wide at the 2.4 GHz ISM band, are used to transmit messages [10]. The duration for transmitting messages is extremely short to save battery power. Among these 40 channels, there are three channels (i.e., 37, 38, and 39) for broadcasting advertisement messages. The Received Signal Strength Indicator (RSSI) from these three channels can be used for estimating the target's proximity. The BLE advertising rate can be set up to 50 Hz. The transmission power for BLE beacons is also set from 0 dBm to −75 dBm. To reduce power consumption, BLE advertising rate and transmission power are usually set to less than 10 Hz and −16 dBm, respectively [11]. Here, dBm indicates decibel-milliwatts (dBm) with which the RSSI is measured, the higher the RSSI number, the stronger the signal is. As the contact-tracing apps are required to run continuously for logging the contacts, BLE's low battery consumption is very well suited.

5. Contact Tracing Protocols

Here is a brief introduction of the state-of-the-art approaches developed for contact tracing in COVID-19 using BLE Technology and also presents a quantitative comparison in terms of user privacy and performance.

5.1 **BlueTrace [12] -** BlueTrace is an open-source protocol that is utilized in Singapore's TraceTogether app. It adopts the BLE technology, where devices exchange their ephemeral IDs (i.e., beacons) via broadcast and log all encounters in their history logs. When a user is diagnosed as positive, his/her history logs are sent to a central authority, using a secure connection. Even though BlueTrace leverages the decentralized architecture, the ephemeral IDs are generated by the central authority and distributed to the individual devices. As such, the reconciliation function and exposure notification are performed at a centralized location, i.e., BlueTrace is considered a hybrid solution. The main cryptographic primitives involved in the computation of the ephemeral IDs is AES-256-GCM.

5.2 **DP-3T [13] -** European researchers proposed the Decentralized Privacy-Preserving Proximity Tracing protocol that leverages BLE technology to track and log encounters with other users. The contact logs are never transmitted to a central authority, but they are stored only on the client's device. When a user tests positive, his/her ephemeral IDs are transmitted to the central authority. The IDs are generated with symmetric key protocols, such as HMAC-SHA-256 and AES128-CTR. Finally, the project is completely open-source.

5.3 **Apple/Google [14] -** In April 2020, Apple and Google worked together to build an opt-in and decentralized way of allowing individuals to know if they have come into contact with confirmed cases based on Bluetooth technology. Similar to DP-3T, the contact tracing logs do not contain any private information, and ephemeral IDs are only stored on the user's device. From the cryptographic perspective, they adopt HMAC-SHA-256 and AES-128. Immuni [15] is the Italian State-sponsored official contact tracing app that leverages the Apple/Google framework.

5.4 **PEPP-PT [16] -** The Pan-European Privacy-Preserving Proximity Tracing protocol adopts BLE to discover and store locally the ephemeral IDs of devices that are in proximity. Similar to BlueTrace, it uses the hybrid architecture by having the health authorities generate the users' beacons. As such, a centralized server collects and processes the contact logs from infected users, and performs the reconciliation process in a centralized manner. The main cryptographic algorithm they employ is AES. This approach also adopts the open-source paradigm.

5.5 Comparison

Table 1 presents a quantitative comparison of these state-of-the-art protocols for a variety of metrics, such as privacy and operational cost. In this analysis, the health authorities are considered as trusted entities. In terms of health status privacy, decentralized protocols fail to protect the identity of the infected users, which is a violation of numerous health privacy acts, such as HIPAA and GDPR. Specifically, DP-3T and Apple/Google disclose all the ephemeral IDs that belong to the infected users, which allows an adversary to infer with certainty whether a known ID (i.e., person) has contracted the virus. As for hybrid solutions (BlueTrace and PEPP-PT) concerned, they only reveal the user's contact logs and are, thus, more privacy-preserving. However, the ephemeral ID of the infected individual might be inferred from its absence within a cluster of IDs with the same time/location tags.

Regarding location privacy, both the decentralized and hybrid protocols offer excellent privacy to the users who never test positive. This is due to the unidirectional flow of information, i.e., the devices only download data from the central authority's server without ever uploading any data of their own. However, a user who tests positive has to disclose some relevant information to the central server. Usually, the cited disclosure involves publishing ephemeral IDs, contact logs, or GPS coordinates, unfortunately leading, among others, to a complete compromise of the geographic locations that the user has visited in the near past. [17]

Table 1: Comparison of State-of-Art representative solutions for contact tracing.

n: Contact List Size, f Frequency: TX, BT Bluetooth:

Features	BlueTrace	DP-3T	Apple/ Google	PEPP-PT
Wireless Technology	BT	BT	BT	BT
Open-Source	YES	YES	YES	YES
Architecture (C/D/H)	H	D	D	H
RF Energy Consumption (mJ/min)	$\approx 1.23 \cdot 10^3$	$\approx 1.21 \cdot 10^3$	$\approx 1.21 \cdot 10^3$	$\approx 1.21 \cdot 10^3$
Security Level (Crypto)	HIGH	HIGH	HIGH	HIGH
Health Status Privacy	LOW	-	-	-
Location Privacy (w.r.t Positive)	-	-	-	-
Location Privacy (w.r.t Negative)	HIGH	HIGH	HIGH	HIGH
Device Storage Requirements (B)	$\approx n.140$	$\approx n.24$	$\approx n .16$	$\approx n.30$
Crypto Consumptional Cost (ms)	0	≈ 24.8973	≈30.2039	0
Broadcast TX Overhead (B)	$f.140$	$f \cdot 24$	$f \cdot 31$	$f .30$

6. Challenges and Road ahead

Contact tracing is a surveillance-type application. However, this generic contact tracing framework raises some concerns; in terms of usability, the main challenges are related to energy efficiency and computational cost. When it comes to privacy and security, the most recurrent threats are user de-identification and user tracking.

In the following section, some of the challenges are discussed that impede the effectiveness of these apps and must be addressed to maximize the coverage of contact tracing.

6.1 Social Considerations

In terms of user adaptability, digital contact tracing apps are facing a low penetration rate among the masses [25], e.g. Australia's COVIDSafe has a 28.6% penetration rate, Singapore's TraceTogether has a 25% penetration, India's Aarogya Setu has 12.05%, Turkey's Hayat Eve Sığar has 17% and UK's NHS COVID-19 App has 28.5%, which are among the highest in user adaptability. It is a challenge to achieve high user adaptability, given that the users are having reservations about the privacy issues surrounding the use of data generated through these apps.

The low penetration of smartphones is another reason for the less adaptability of these contract tracing apps. India having only 24%, the United States of America (USA) with 81%, and South Korea at a 95% penetration rate [28]. Even in the USA, 2 out of 10 individuals do not use smartphones; many of those who own such a device may opt not to install the contact tracing app on their device.

Automated contact tracing requires a modern and high-tech infrastructure. The better the technology infrastructure of a country, the better the digital contact tracing will be. From a global perspective, digital contact tracing may be suitable for developed countries while in developing and underdeveloped countries, digital contact tracing frameworks may not achieve their full potential.

6.2 Technology Considerations

Received Signal Strength Indicator (RSSI) is the most incorporated technique in contact tracing technologies. The Radio-propagation model makes this feature useful in estimating the distance between the transmitter and the receiver nodes. Unfortunately, several factors can affect the accuracy of distance estimation, including radio noise, obstacles, multipath reflection and shadowing effects, or environmental factors like rain, temperature, and humidity. As a result, Bluetooth RSSI may produce a large number of false positives and false negatives. As a solution, alternative features like Angle-of-Arrival, Time Difference of Arrival, and Time of Arrival should be investigated. Furthermore, the localization accuracy of the Bluetooth technology can also be improved by incorporating AL Algorithms in the edge devices.

6.3 Security Considerations

An IoT smart device represents the edge component between the mobile devices and the hospital/authority. To meet the intended security and privacy goals, lightweight cryptographic protocols can be adopted to reduce the required computations. The exposure of the IoT smart devices equipped with BLE transiver to physical attacks is the most obvious concern in terms of security. As a result, no sensitive information, such as user beacons or private keys, should be stored in plaintext format. Furthermore, data at rest could be encrypted with the public key of the central authority and BLE-enabled devices should utilize a secure enclave to perform the necessary cryptographic operations, and all beacons (even when encrypted) should be erased as soon as they are received by the trusted authority.

Replay and Relay Attacks [17] generate a large number of false contacts such that, if one individual tests positive, the disclosure of his/her beacons will trigger many false positive alerts. Such attacks can be addressed such as the beacon generation protocol may incorporate certain cryptographic protocols to thwart replay attacks. And the trusted authority can analyze the collected data and identify fraudulent beacons.

6.4 Privacy Considerations

The misuse of the collected data at the trusted authority, under the centralized and hybrid models, could be the main privacy concern in Contact tracing protocols and applications. Indeed, a malicious insider with access to all beacons, locations, timestamps, and contact lists, can extract sensitive information about the underlying individuals (such as locations visited, routes, social contacts, etc.). Such attacks can be made less feasible by design if users do not submit their contact lists. Instead, all the beacons are aggregated at the distributed IoT devices, which makes it much harder for an adversary to track individuals.

7. Conclusion

Digital Contact Tracing - IoT-based architecture is a more scalable adoption in the aftermath of the COVID-19 pneumatic. Although several research works have reviewed contract tracing applications and techniques, in this paper a thorough analysis of contact tracing applications and techniques is presented, and among which, the most prominent, globally recognized and adapted state of art technology i.e. BLE Protocol Interface is also discussed. Furthermore, some concerns about the usability of the solution are also experienced including system privacy and security of the contact tracing framework, highlighting their successes, failures, and pitfalls.

8. Acknowledgments

This paper is prepared under the guidance of Professor Luigi La Blunda during the study for the master's degree in high integrity systems, for the subject of the internet of things.

9. References

[1] Muhammad Shahroz, Farooq Ahmad, Muhammad Shahzad Younis , Nadeem Ahmad , Maged N. Kamel Boulos, Ricardo Vinuesa , Junaid Qadir, 'COVID-19 digital contact tracing applications and techniques: A review post initial deployments' published in Transportation Engineering Volume 5, September 2021, 100072, journal homepage: www.elsevier.com/locate/treng

[2] Piergiuseppe Di Marco, Pangun Park, Marco Pratesi and Fortunato Santucci, 'A BluetoothBased Architecture for Contact Tracing in Healthcare Facilities.' Published in Journal of Sensor and Actuator Networks by MDPI 2021, https://doi.org/10.3390/jsan10010002

[3] Apple and Google. Exposure Notification—Bluetooth Specification v1.2. 2020. Available online: https://www.blog.google/documents/62/Exposure_Notification_-_Bluetooth_Specification_v1.2.pdf (accessed on 1 December 2020).

[4] NADEEM AHMED, REGIO A. MICHELIN, WANLI XUE, SUSHMITA RUJ, ROBERT MALANEY, SALIL S. KANHERE, ARUNA SENEVIRATNE, WEN HU, HELGE JANICKE AND SANJAY K. JHA, A Survey of COVID-19 Contact Tracing Apps, published by IEEEACCESS july 20,2020, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9144194

[5] Viktoriia Shubina , Sylvia Holcer , Michael Gould and Elena Simona Lohan, Survey of Decentralized Solutions with Mobile Devices for User Location Tracking, Proximity Detection, and Contact Tracing in the COVID-19 Era, published by MDPI Published: 23 September 2020

[6] P. Misra and P. Enge, Global Positioning System: Signals, Measurements and Performance, 2nd ed. Lincoln, MA, USA: Ganga-Jamuna Press, 2011.

[7] J. C. Haartsen, ''The Bluetooth radio system,'' IEEE Pers. Commun., vol. 7, no. 1, pp. 28–36, Feb. 2000.

[8] WiFi Alliance. (2010). WiFi Certified WiFi Direct. [Online]. Available: https://www.wi-fi.org/system/files/wp_WiFi_CERTIFIED_WiFi_Direct_Industry_20140409_0.pd

[9] Mohammad Jabed Morshed Chowdhury, Md Sadek Ferdous, Kamanashis Biswas, Niaz Chowdhury and Vallipuram Muthukkumarasamy, COVID-19 Contact Tracing: Challenges and Future Directions date of published on November 9, 2020 in IEEE*ACCESS* VOLUME 8, 2020

[10] R. Faragher and R. Harle, ``An analysis of the accuracy of Bluetooth low energy for indoor positioning applications,'' in Proc. 27th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSSC), vol. 812. Tampa, FL, USA, 2014, pp. 201_210.

[11] J. Liu, C. Chen, Y. Ma, and Y. Xu, ``Adaptive device discovery in Bluetooth low energy networks,'' in Proc. IEEE 77th Veh. Technol. Conf. (VTC Spring), Jun. 2013, pp. 1_5, doi: 10.1109/VTCSpring.2013.6691855.

[12] J. Bay et al., "BlueTrace: A privacy-preserving protocol for community driven contact tracing across borders," Government Technology Agency-Singapore, Tech. Rep, 2020.

[13] "Decentralized Privacy-Preserving Proximity Tracing: Overview of Data Protection and Security," https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf, 2020, (Accessed: 2021-1-1).

[14] Apple Google. (2020) Privacy-Preserving Contact Tracing. (Accessed: 2021-1-1). [Online]. Available: https://www.apple.com/covid19/contacttracing

[15] Italian Ministry of Health, "Immuni," https://www.immuni.italia.it/, June 2020, (Accessed: 2021-1-1).

[16] PEPP-PT Team. (2020) PEPP-PT Team. (2020) Pan-European Privacy-Preserving Proximity Tracing. (Accessed: 2021-1-1). [Online]. Available: https://www.pepp-pt.org/

[17] Pietro Tedeschi, Spiridon Bakiras, and Roberto Di Pietro, IoTrace: A Flexible, Efficient, and Privacy-Preserving IoT-enabled Architecture for Contact Tracing, available at https://arxiv.org/pdf/2007.11928.pdf

Covid tracing tracker - read only, (https://docs.google.com/spreadsheets/d/ 1ATalASO8KtZMx_zJREoOvFh0nmB-sAqJ1-CjVRSCOw/edit#gid=0).

[4] Viktoriia Shubina , Sylvia Holcer , Michael Gould and Elena Simona Lohan, Survey of Decentralized Solutions with Mobile Devices for User Location Tracking, Proximity Detection, and Contact Tracing in the COVID-19 Era, published by MDPI Published: 23 September 2020