International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 12 | Dec 2020 www.irjet.net p-ISSN: 2395-0072

Exposer Notification During Pandemic Via Multi-Level Contact Tracing

Aniket Singh[1], Vaishnavi Rane[2], Shreya Pednekar[3], Prof. Kirti Suryawanshi[4]

[1-3]Students, Dept. of Computer Science, Smt. Indira Gandhi College of Engineering, Navi Mumbai, Maharashtra, India
[4]Teacher, Dept. of Computer Science, Smt. Indira Gandhi College of Engineering, Navi Mumbai, Maharashtra, India

---

Abstract - *The recent outbreak of novel corona virus has taken the world with a toll forcing lockdown multiple restriction on the way of living and stressing the health care system to a brink. Hence business all over are now planning for the post-pandemic world and looking for innovative ways to protect the health and being of all. Where wireless systems like mobile application are proposed to be thriving example that can play a key role in assisting exposure tracing to get a halt on local infection outbreak and prevent further spreading of virus. Therefore, in this paper, we aim to present a theory and a working system and mechanism for multilevel exposure tracing and notification which can act as an updated version of application proposed till date to counter the problem*.

Key Words: TAN (one-time code), Seed, Chirps, Bluetooth Beacon, TempID's, Tuples.

1. INTRODUCTION

Across the world, governments and health authorities are working together to find solutions to the viral pandemic, and to protect people to get society back up and running. Software developers are providing their contribution by designing technical tools to help defeat the virus and save us. So, in this spirit of collaboration, international companies like Google and Apple have announced a joint architect to start the use of Bluetooth technology to help governments and health agencies reduce the spread of the covid, with user security and privacy central to the design. During this pandemic and world lockdown and an absolute grave threat to lives one thing has been challenged the most is the traditional method good? Is it safe to walk without making contact with an infected person or infecting anyone? How to trace how many people we have been in contact with or where. So, in response a way proposed and architected by engineers is exposure tracing via technology. This application can be used to trace a multilevel exposure of a person say Covid for instance or any other viral infection. So, to reduce the spread of Covid, it is necessary to let people know about their close proximity to positive tested individuals. Therefore, a chain can be traced with use of this application. So far, the health department and affected individuals have identified possibly infected individuals via personal conversations based on each individuals' memory. Which has led to a big number of unknown connections, e.g. When using public transport, we come in exposure with many people we don't know about hence this application is developed. With this application, we can help to interrupt chain of infection. With minimum effort and with max data protection. This system can avoid any personal information hence it does not know who you are. So that you can protect yourself and the people around you better.

Typically, digital contact tracing protocol have two major responsibilities namely exposure logging and infection reporting. Exposure Notification system only defines encounter log which is a decentralized architect, with majority of the infection reporting, currently most of it is centralized, so being neglected to individual app implementation. Even the present architect of one-layer tracing has not been enough to own this problem of community spread hence an updated version of this problem is required today it might just be a problem that can be dealt with one layer of exposure tracing but this is the high time when we get ready to overcome any such problem in the coming future? But the introduction of contact tracing apps to general public has led to a debate regarding the architect, data-management, security, and privacy of the application. Most of these application claim to be privacy-preserving which means that they do not reveal any Personally Identifiable Information identity, or information about location of the contacts without explicit user permission and hence divide into three chambers of development which would be discussed in upcoming parts. The aim of this paper is to provide an alternative to support world to stand again defeating this pandemic.

1.1 PROBLEM STATEMENT

Older methods of contact tracing are critical or trustworthy to contain the spread of infection. Technology can support and enlarge these efforts by allowing public health authority to quickly notify all people who may have been exposed to a person who has infected with COVID. Exposure tracing is the process of identifying, managing, and assessing people who have been exposed to a disease to prevent further transmission. When applied systematically, exposure tracing will surely break the chain of transmission of an infectious disease and is thus an essential public health tool for controlling infectious disease outbreaks The Application implementation should aim to augment the exposure-tracing process, via BLE (Bluetooth low energy) process over a distance of 3 meters or more max 6 meters The app uses Bluetooth device, and your Bluetooth data is stored securely on

your phone. It'll only be shared with centralized batch if you test positive for COVID, and for the sole purpose of exposure tracing. Also, all Bluetooth data stored on your phone is automatically deleted after 15 days. This system would be an essential part of transitioning back to our daily lives while managing the risk of further outbreak. But till which level should it be traced? Is this only pandemic me would ever face such question needs to answer and only answered by multilevel of exposure tracing by multiple loops to prevent any possibility of another world lockdown.

1.2 PROJECT OBJECTIVES

1. This system would be first to present a chain of exposure tracing or multi-level exposure tracing notification along with tracing distance up to 5meters.
2. As soon as person is in contact with other the Bluetooth function would do its job of saving the key from each other's phone and no one would know, even during notification the person won't know who they have been in contact with or who has tested positive respecting people's privacy.
3. The system would be decentralised and hence database of personal information would be stored in a personalized database which would be only access at times of emergency with the personals permission along with all contact traced would be stored in personal database in mobile and no other person can access the same or have any authority over the data.
4. To achieve the security measures the notification system would only be accessed with a special onetime code which would be given along with the test result if tested positive.
5. To avoid threat of hacking the system would use Bluetooth on static bases to avoid any other use of the function. Along with this the key generated by the Bluetooth would keep on changing every 15 min.
6. For people who don't to know how long they need to stay in Quarantine or isolation days respective information would be added.
7. This system can be transformed into any viral application tracing mode just by changing few data restriction and loops.

2. RELATED WORK

2.1 Present System Architecture

At present the type of system architecture adopted for the operation and data collection aspects of exposure tracing application has been a matter of great debate among both privacy and security issue and concerns as well. We will discuss these three proposed systems and widely used system architects for development of exposure tracing applications. Namely the centralized, the decentralized, and the hybrid approaches that combine features from both the centralized and the decentralized architectures.

I) CENTRALIZED: - The initial requirement for the application is that a user has to pre-register with the central server. The server then generates a privacy-preserving Temporary ID (TempID) for particular device. This TempID is then encrypted with a unique key which is only know to the central server authority and sent to the devices. Devices exchange these TempIDs in Bluetooth encounter messages when they come in close contact with each other hence the mechanism of the application. Once a user has tested positive, they can volunteer to upload all of their stored encounter chirps to the central server.

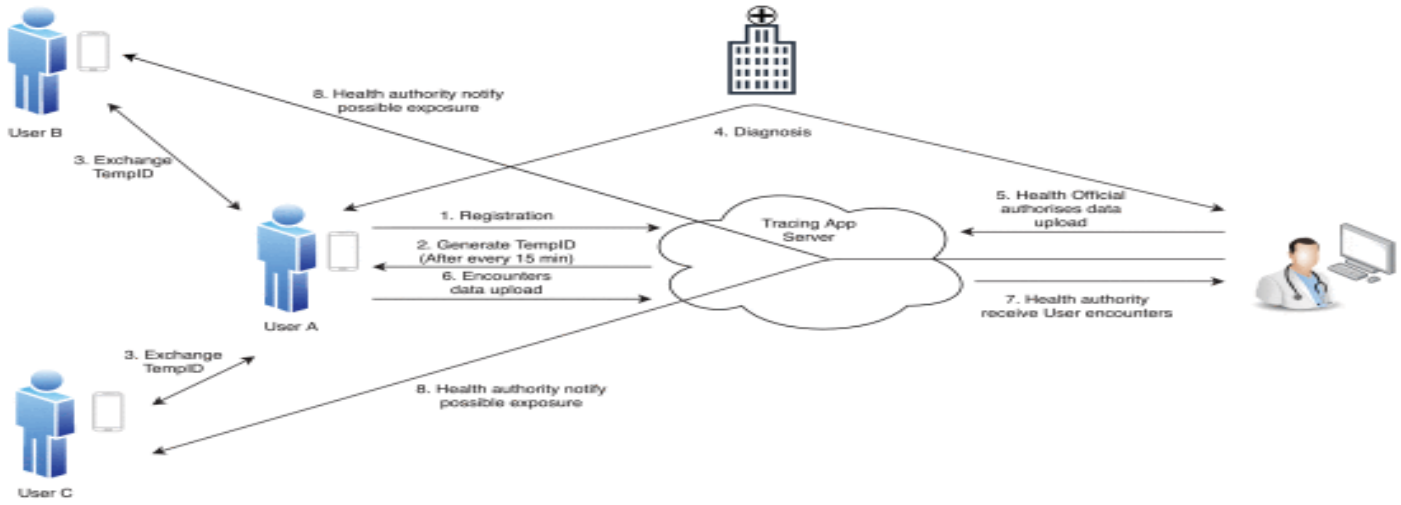

Fig -1: Centralized Architecture

The server maps these TempIDs in these messages to individual's data already with the central server to identify at-risk contacts. In this mod system, the authority knows enough to contact all the people who may have been near the person who has later tested positive. This includes all data about personal associations, which can be quite sensitive. Figure below shows the main entities and the interactions of a centralized system.

II) DECENTRALISED: -But to an absolute contrast of the centralized architect system, the decentralized process proposes to move core functionalities to the user devices, leaving the central server with minimal involvement in the contact tracing process leading to maximum support of privacy and least involvement of the centralized system at the best. The ideology behind this is to enhance user security and privacy by generating anonymous identifier at the user devices and keeping real

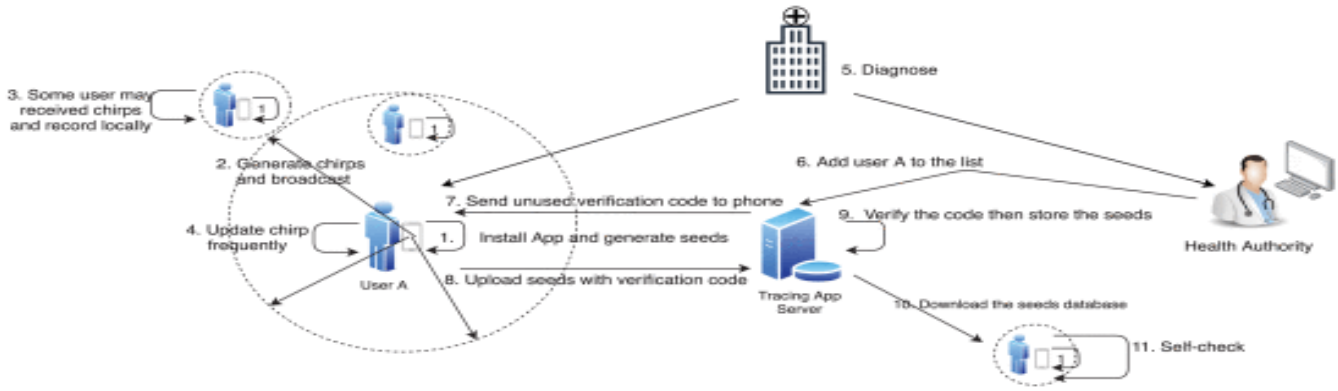

Fig -2: Decentralized Architecture

Users' identities as a secret from the other users as well as the main server and processing the exposure notifications on the centralized server with no personal details on that end. In the decentralized model, the authority usually it only knows the identities of the users who has been diagnosed with COVID-19. Under this decentralized model, the exposure tracing app compares that list of ID's of all people who tested positive with the list of IDs it has ever been in contact with locally, on the users' phone for past 15 days. And thus, it takes the Private Automated Contact Tracing protocol as its base to describe the decentralized approach. Since this architect does not require any app users to 'pre-register' itself before using, thus avoiding the storage of any info with the server.

III) HYBRID: - Since in the centralized approach, the server performs all the complex tasks, e.g., risk analysis, TempID calculation, encryption, notifications, and decryption of alerts for the at-risk contacts. And on the other hand, all these functions are limited to devices in the decentralized approach, hence keeping the server only as a bulletin board for lookup purpose. Hence the hybrid architecture proposes that all these functionalities should be split between the server and the devices to achieve stability. Elaborately let the TempID generation and its management remain a decentralized approach protecting

privacy while the risk analysis part and the notifications be the responsibilities of the centralized server system.and privacy by generating anonymous identifier at the user devices and keeping real,

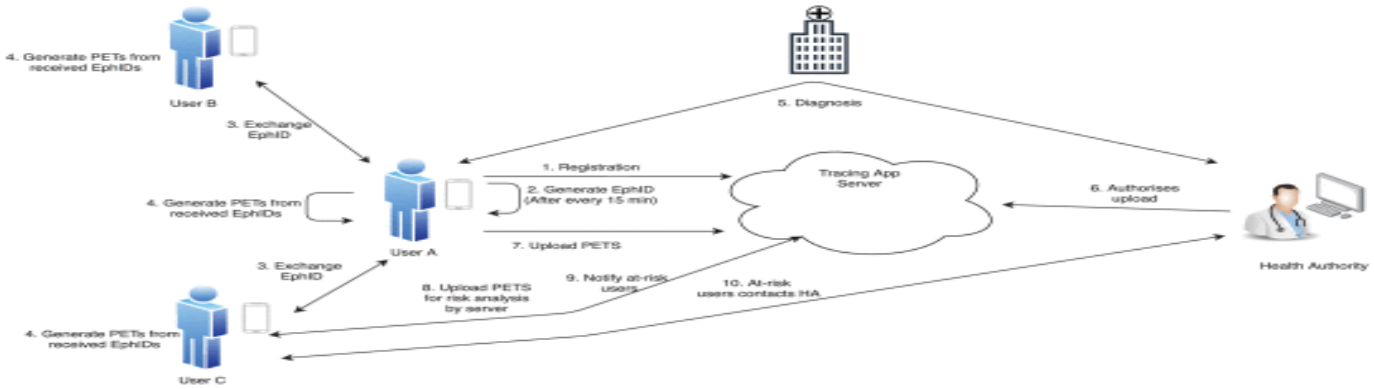

Fig -3: Hybrid Architecture

3. METHODOLOGY

1. First, two phones come near each other.

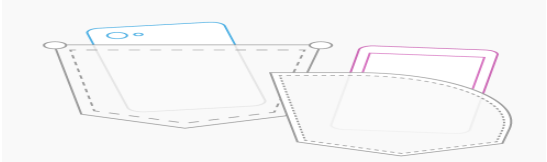

Fig -4: Close Contact

2. The phones exchange unique chirp codes that frequently changes.

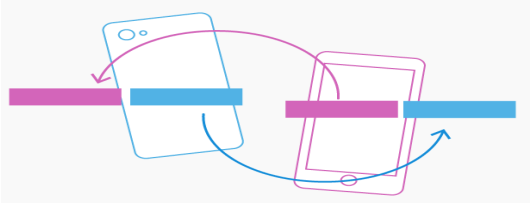

Fig -5: Exchange of Chirps

3. Each phone store the code it received and the one it transmitted.

Fig -6: Storing in personal database both Chirp and Seed

4. If a person has tested positive, they can upload all the log of chirp codes they transmitted to a public database.

Fig -7: Uploading Seed

5. Other phones regularly check that database for the code it has received from other phones.

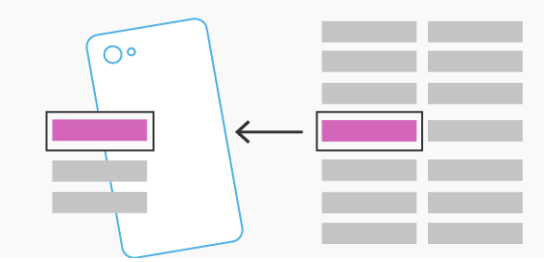

Fig -8: Checking in personal database of chirp

6. If a match is ever found, the phone knows it was near a person who has recently tested positive and triggers an alert.

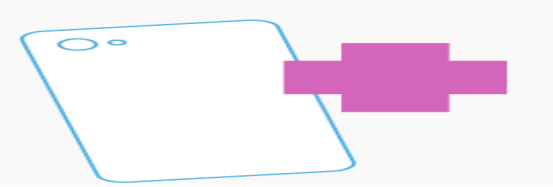

Fig -9: Notification Received of Exposure

7. Person receives the notification with a specially designed code with helps the machine understand the level of contact with recently tested positive patient.

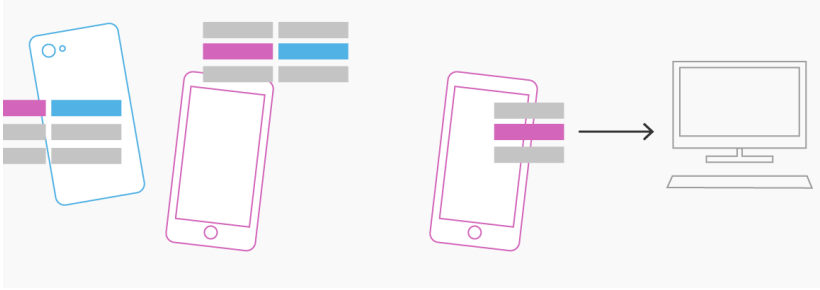

Fig -10: Checking for level of exposure and uploading dataset if level 1

8. The machine checks for level of contact if it is first level it asks permission to notify all people in there contact as well which gives a chain of exposure tracing.

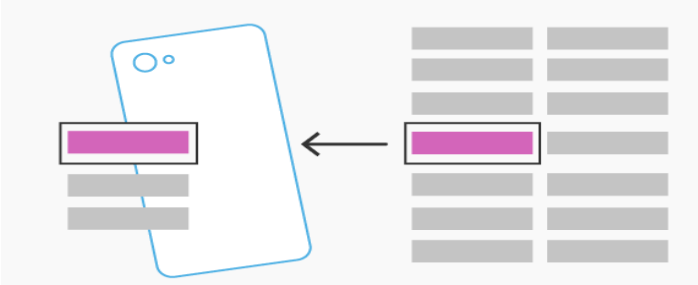

Fig -11: Checking for Exposure

9. 2nd level of exposure is also notified via this method

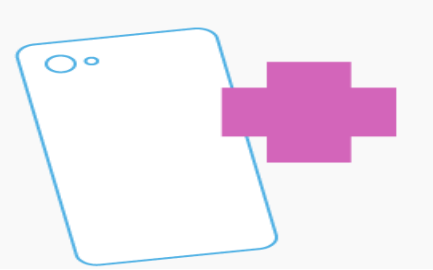

Fig -12: Notification Received

4. SYSTEM DESCRIPTION

4.1 PROCESS:

1) APP INSTALLATION

Exposure tracing apps that adopt the decentralized architecture do not necessarily require an interactive registration process during the app installation stage. The app installation process only verifies a user's smartphone and deploys a random TAN generation algorithm that is not linked to the phone.

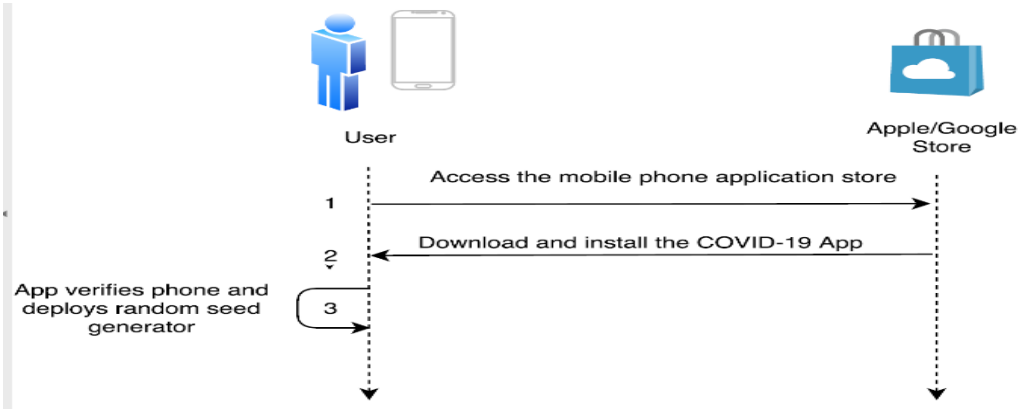

Fig -13: Installation Process

2) GENERATING TAN, CHIRPS AND EXCHANGING CHIRPS

1. Once the decentralized tracing app is installed, the TAN/seed is generated (with an expiry period of 10 min) by the user's device.

2. This seed and the current time are subsequently used in a pseudorandom function to generate the chirp.

3. The chirps are not linked to an individual or their phone - so in principle, they are anonymous. The app generates chirps with a time granularity of 1 min using seed.

4. These are broadcasted every min via the Bluetooth beacon. In the listener's phone, the system will impulsively store all chirps received to it (step 4).

5. The information stored in the receiving app includes the chirp, the timestamp when the chirp is received. All identical chirps that was received within a minimum difference are ignored. The main difference from the centralized architecture where Temp IDs are created by the main server in the decentralized case, the seeds and chirps are generated at the device.

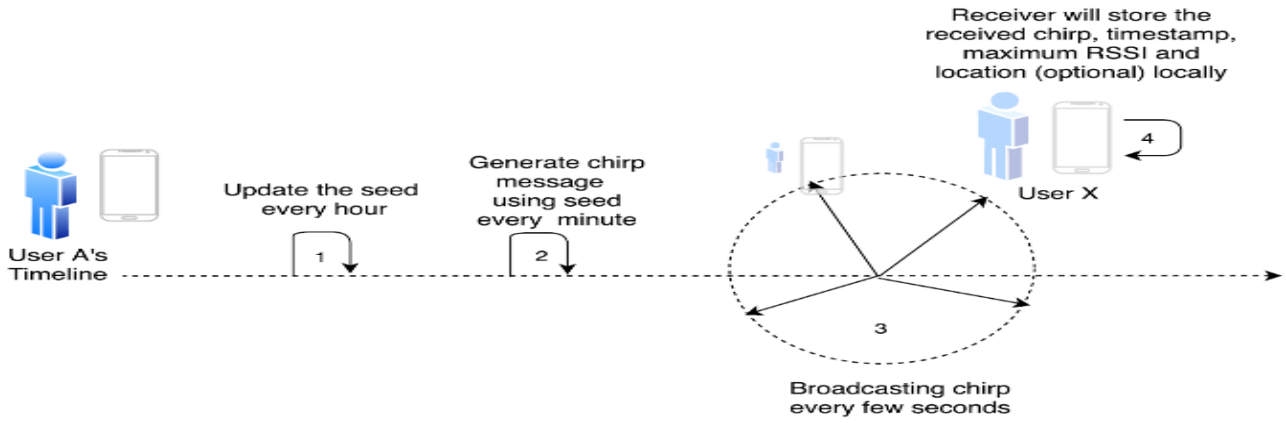

Fig -14: Chirps Seed Generation and Sharing Process

3) UPLOADING ENCOUNTERS DATA

1. If a user is diagnosed positive, they are given a unique ``permission number'' by the relevant authority to authorize the upload of all used seeds that are locally stored in their phone (illustrated in Figure), as well as the creation and expiry times of the seeds.

2. Note, the server in the decentralized architecture only gets the seeds associated with a single identified user.

3. This is to be compared with the centralized architecture where the complete contact list (with TempIDs) of all encountered individuals is uploaded to the server.

4) THE CONTACT TRACING PROCESS

1. Contrary to the centralized architecture, the tracing process in the decentralized architecture is performed locally by the app user on their device (instead of the central server).

2. The app users can have a communication with the server, typically once every day, to download any seed uploaded by infected users.

3. Given such seeds are downloaded (step 8), the user's app then reconstructs all the corresponding chirps (using pseudorandom calculations based on the seeds and discrete-time intervals between the start and expiry time).

4. Finally, the app performs a search to check if any of the reconstructed chirp information appear in its local encounter log. If so, proximity and duration times are then derived for contact level analysis purposes.

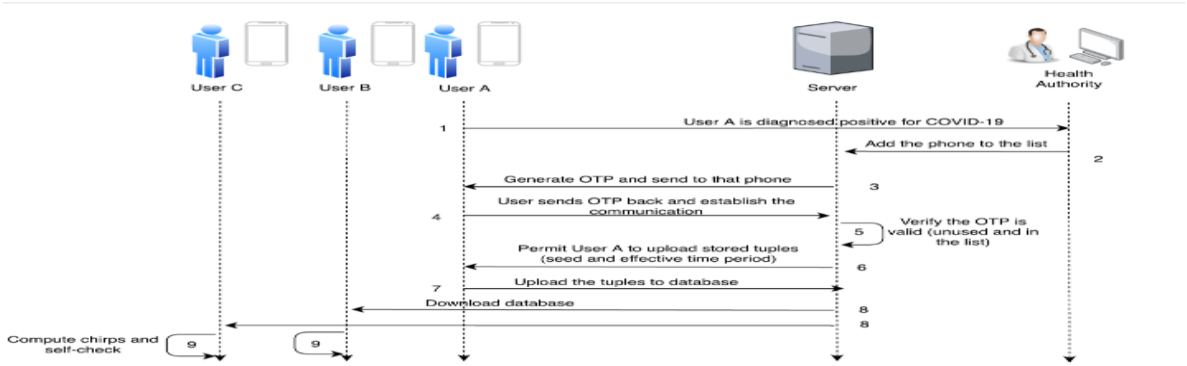

Fig -15: Contact Tracing Process

5) Multilevel Notification

1. During self-check of chirp check the level of contact by the support message from server.
2. If the level of contact 1 notify server.
3. Upload the set of tuples
4. Broadcast of the recently received data set of second level with specially designed message to let machine know it is second level contact
5. Absolute no human intervention required during this process.
6. Follow the same process of self-check

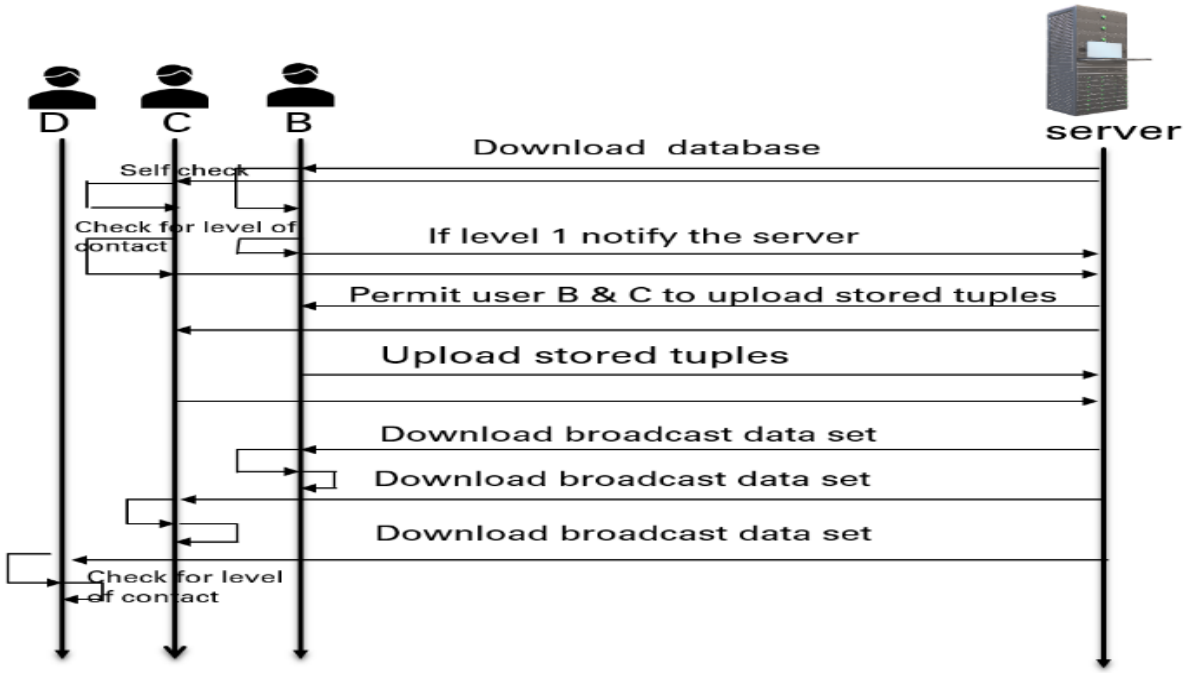

Fig -16: Multilevel Notification

4.2 DATABASE:

1) Functions of Main Server

1. Store the TAN of person if he/she under goes test.
2. If tested positive notify the personal.
3. Ask to upload the set of tuples of past 15 days
4. This set of tuples would contain all the seeds and chirps generated by the mobile in past fifteen days.
5. Broadcast the set of tuples along with a specially designed message of level of contact.
6. Get notified from level 1 exposed mobile data sets
7. Ask for the set of tuples from the user who have been in 1st level of contact.
8. Broadcast the set of tuples received from 1st level of contact.
9. Add them with designed message that states it is not the first level contact.

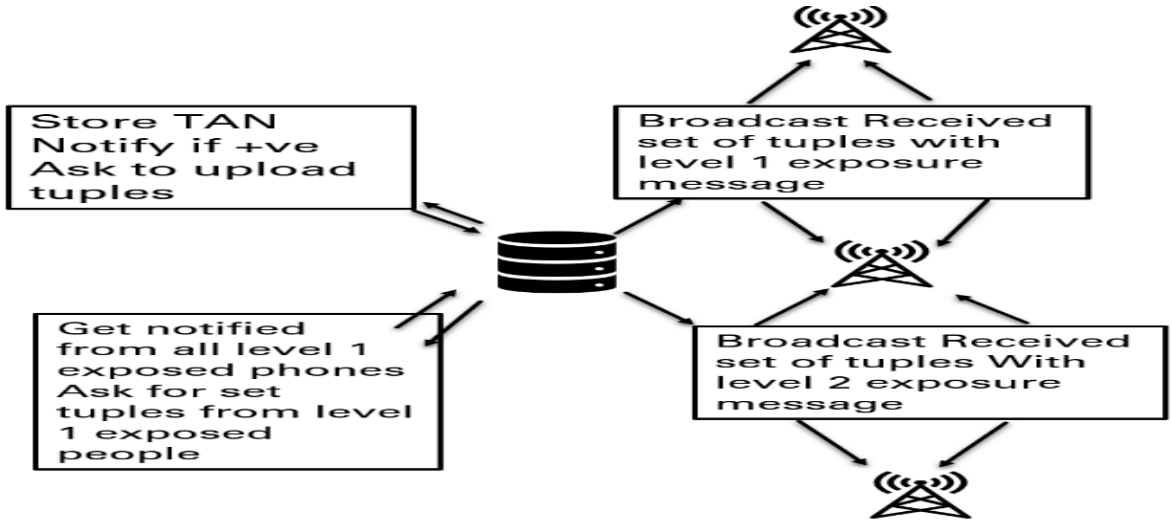

Fig -17: Main Server Database

2) Functions of personal Database

1. Store all seeds generated for 15 days.
2. Store chirps of people been in contact with in separate database
3. Delete the sets of seed after 16 days.
4. Download all broadcasted tuples from main server run a search algorithm with our data and check for if been in contact or close vicinity of a recently tested positive person.
5. While searching for tuples in seed data check the level of contact and notify accordingly.
6. And if in level 1 contact send a copy of tuples from your data set to main server.If underwent a test
7. Verify store Send TAN to main server
8. Send all sets of chirps generated in past 15 days to main server.

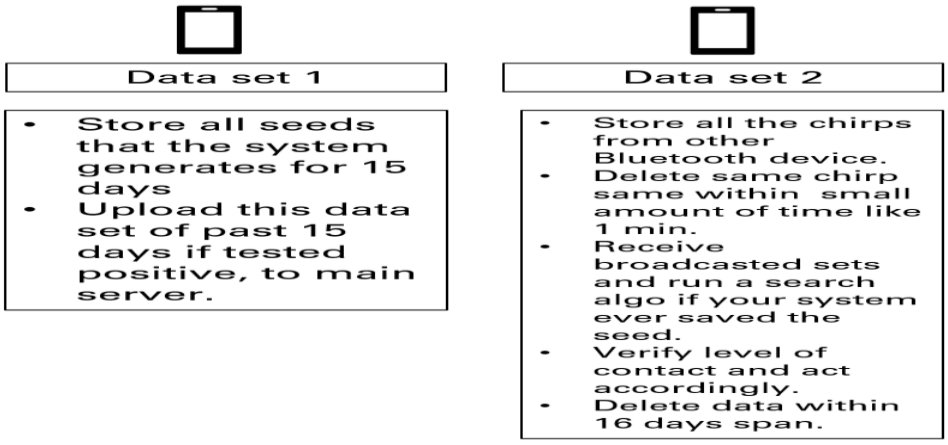

Fig -18: Personal Database

5. SYSTEM APPROACH

5.1 Use case model

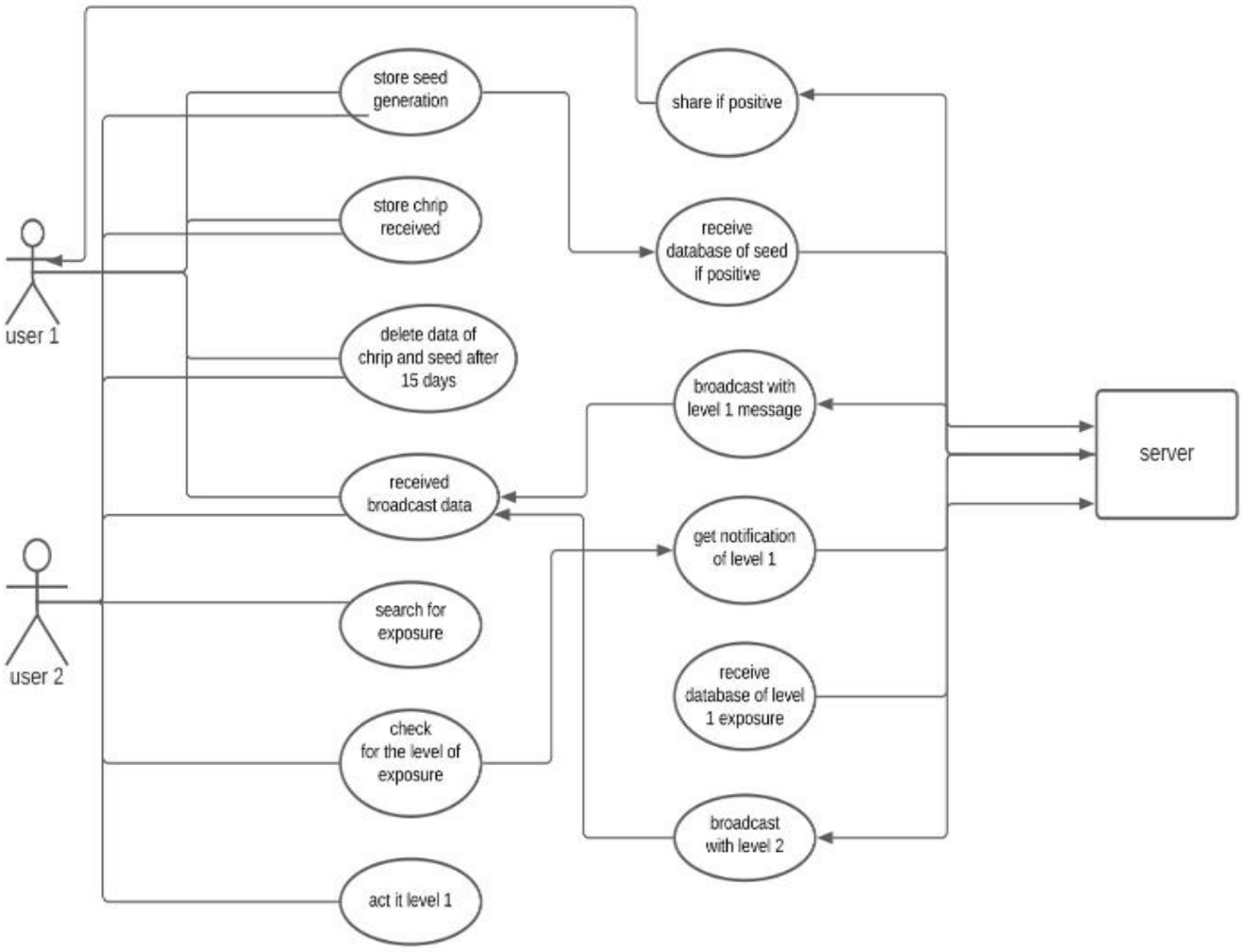

Fig -19: Use Case model

5.2 Flowchart

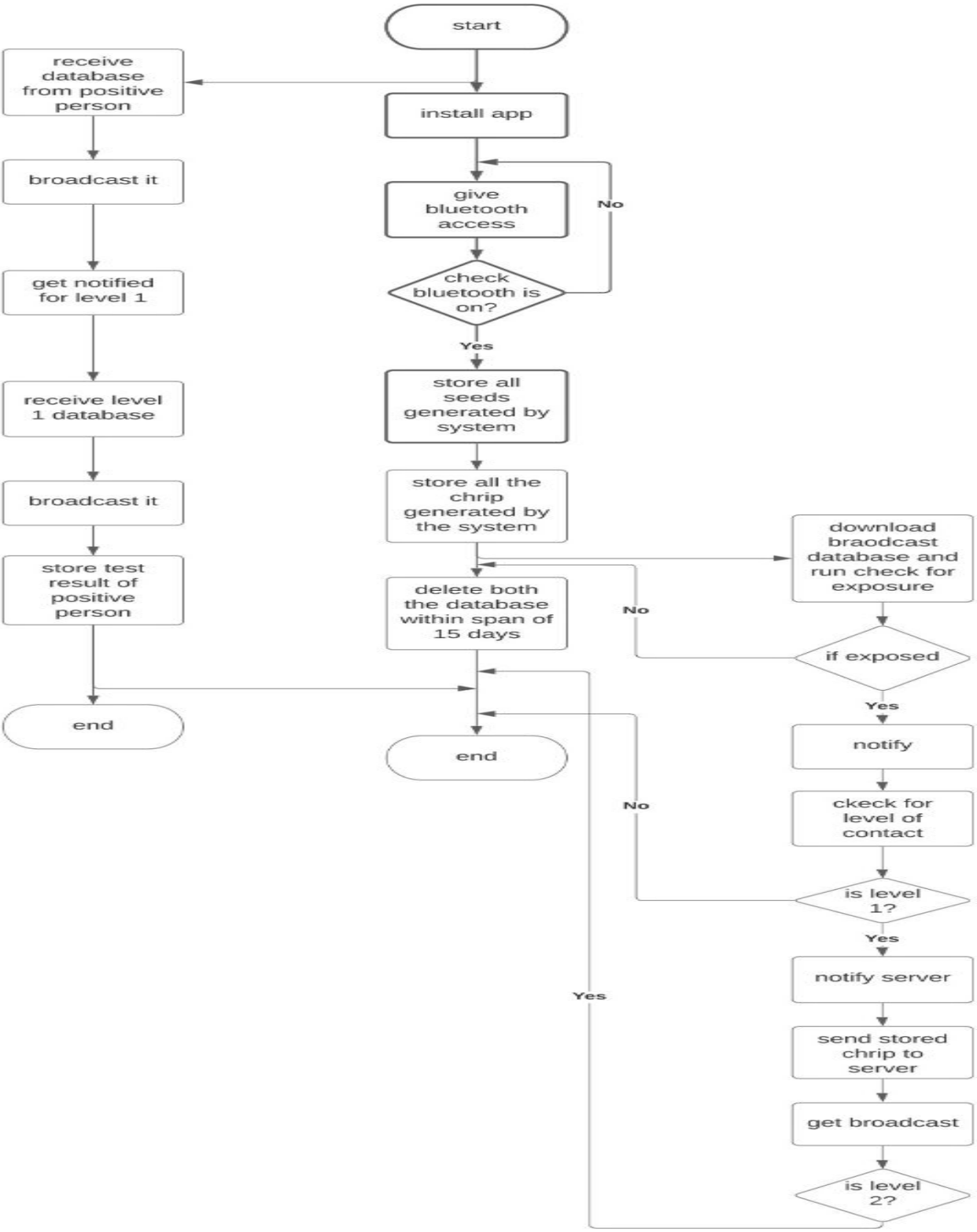

Chart -1: Flowchart

6. CONCLUSIONS

In this paper, we propose a joint end-to-end model, of an exposure notification application model. The COVID-19 pandemic still continues to affect the way of life. Hence the contact tracing apps are likely to play a crucial role in halting the spread of the virus while also aiding the health authorities quickly identify individuals that may have been exposed to the virus. The important interest for adoption of tracing app technology will actually improve the tracing capability for health authorities. There are many responses to this system including protection of vulnerable, building new protocols for daily life to reduce transmission, and containing uncontrollable local outbreaks of corona virus. Testing and exposure tracing will be crucial to this last strategy, especially, in period of the high transmission rate of COVID-19 and exposure notification can be a key element to the toolbox of public health authority. As the response to the pandemic evolves, technological solution will need to continue on adaption as well so the efforts of public health authority can be amplified. As such, it is necessary to have a clear understanding of the steps and requirements of the contact tracing process and clearly identify which are being optimized by digital tools.

Integration of digital techs for exposure tracing needs to identify carefully and address technical, ethical, and cost issues. Privacy related concerns about the disclosure of personal data always needs to be addressed. Data processing agreements must disclose which data are transmitted to third parties and for what purpose. Chain process is proposed with an intention to trace longer and wider spread to make people trust in model its effectiveness should be trust worthy and proof full.

REFERENCES

[1] Asaf, G.; Davis, H.; McCorkell, L.; Wei, H.; O'Neill, B.; Akrami, A. "What Does COVID-19 Recovery Actually Look Like? An Analysis of the Prolonged COVID-19 Symptoms," Survey by Patient-Led Research Team. 2020.

[2] Viktoriia Shubina, Aleksandr Ometov, Elena Simona Lohan, "Technical Perspectives of Contact-Tracing Applications on Wearables for COVID-19 Control", UltraModern Telecommunication and Control Systems and Workshops (ICUMT) 2020 12th International Congress on, pp. 229-235, 2020.

[3] L Leith DJ, Farrell S.,"Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection." ACM Computer Communication Review, 2020

[4] 0. R. Hinch, W. Probert, A. Nurtay, M. Kendall, C. Wymant, M. Hall, K. Lythgoe, A. B. Cruz, L. Zhao, A. Stewart, L. Ferretti, M. Parker, D. Motero, J. Warren, N. K. Mather, A. Finkelstein, L. Abeler-Dorner, D. Bonsall, C. Fraser, "Effective Configurations of a Digital Contact Tracing App", A report to NHSX (2020) in press.

[5] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology,"Sensors, vol. 12, no. 9, pp. 11 734–11 753, 2012

[6] N. Ahmed *et al*., "A Survey of COVID-19 Contact Tracing Apps," in *IEEE Access*, vol. 8, pp. 134577-134601, 2020, doi: 10.1109/ACCESS.2020.3010226.

[7] S. Vaudenay, "Centralized or decentralized? The contact tracing dilemma", *IACR Cryptol. ePrint Arch.*, vol. 2020, pp. 531, May 2020.

[8] L. Reichert, S. Brack and B. Scheuermann, "A survey of automatic contact tracing approaches", 2020, E-Print.

[9] S. Liu, Y. Jiang and A. Striegel, "Face-to-face proximity estimation using Bluetooth on smartphones", *IEEE Trans. Mobile Comput.*, vol. 13, no. 4, pp. 811-823, Apr. 2014.

[10] J. K. Becker, D. Li and D. Starobinski, "Tracking anonymized Bluetooth devices", *Proc. Privacy Enhancing Technol.*, vol. 2019, no. 3, pp. 50-65, Jul. 2019.

[11] J.-F. Biasse, S. Chelleppan, S. Kariev, N. Khan, L. Menezes, E. Seyitoglu, et al., " Trace- \$Sigma\$: A privacy-preserving contact tracing app ", 2020, E-print.

[12] T. Altuwaiyan, M. Hadian, and X. Liang, "Epic: Efficient privacy-preserving contact tracing for infection detection," in 2018 IEEE In-ternational Conference on Communications (ICC), May 2018, pp. 1–6

[13] Martin, T.; Karopoulos, G.; Hernández-Ramos, J.L.; Kambourakis, G.; Fovino, I.N., "Demystifying COVID-19 digital contact tracing: A survey on frameworks and mobile apps", arXiv 2020, arXiv:2007.11687.

[14] Li, T.; Yang, J.; Faklaris, C.; King, J.; Agarwal, Y.; Dabbish, L.; Hong, J.I. "Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing app",. arXiv 2020, arXiv:2005.11957.

[15] Haartsen, J.C.; Mattisson, S.," Bluetooth-a new low-power radio interface providing short-range connectivity.", Proc. IEEE 2000, 88, 1651–1661

[16] Jarvinen, K.; Kiss, A.; Schneider, T.; Tkachenko, O.; Yang, Z. ,"Faster privacy-preserving location proximity schemes for circles and polygons". IET Inf. Secur. 2020, 14, 254–265.

[17] Ng, P.C.; She, J.; Ran, R.," A Compressive Sensing Approach to Detect the Proximity Between Smartphones and BLE Beacons." IEEE Internet Things,. 2019, 6, 7162–7174.

[18] Ding,H.; Qian,C.; Han,J.; Xiao,J.; Zhang,X.; Wang,G.; Xi,W.;Zhao,J. "Close-Proximity Detection for Hand Approaching Using Backscatter Communication", IEEE Trans. Mob. Comput. 2019, 18, 2285–2297.

[19] Ng, P.C.; She, J.; Park, S. "High resolution beacon-based proximity detection for dense deployment", IEEE Trans Mob. Comput. 2017, 17, 1369–1382.

[20] Ng, P.C.; Spachos, P.; Plataniotis, K. "COVID-19 and Your Smartphone: BLE-based Smart Contact Tracing", arXiv 2020, arXiv:2005.13754.

BIOGRAPHIES

"Singh Aniket Ramesh Student of Smt. Indira Gandhi College of Engineering, in Computer Science branch, 2017-2021."

"Rane Vaishnavi Sudhir, Student of Smt. Indira Gandhi College of Engineering, in Computer Science branch, 2017-2021 "

"Pednekar Shreya Hariram Student of Smt. Indira Gandhi College of Engineering, in Computer Science branch, 2017-2021"

"Prof. Kirti Manoj Suryawanshi working as Assistance Professor at Smt. Indira Gandhi College of Engineering, Navi Mumbai. She has completed her ME in Computer Engineering. 5 years of successful University Teaching experience at Under Graduate and Graduate level Proficiency in conducting lectures, tutorials and workshops using new teaching media. "