SN Computer Science (2021) 2:136
https://doi.org/10.1007/s42979-021-00520-z

ORIGINAL RESEARCH

A Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19

B. Sowmiya[1] · V.S. Abhijith[1] · S. Sudersan[1] · R. Sakthi Jaya Sundar[2] · M. Thangavel[3] · P. Varalakshmi[4]

Received: 11 November 2020 / Accepted: 11 February 2021 / Published online: 11 March 2021

Abstract

In response to the coronavirus (COVID-19) pandemic, Government and public health authorities around the world are developing contact tracing apps as a way to trace and slow the unfold of the virus. There is major divergence among nations, however, between a "privacy-first" approach that protects citizens' information at the price of very restricted access for public health authorities and a "data-first" approach that stores massive amounts of knowledge that, whereas of immeasurable price to epidemiologists. Contact tracing apps work by gathering information from people who have tested positive for the virus and so locating and notifying individuals with whom those people are in shut contact, oftentimes by use of GPS, Bluetooth, or wireless technology. All of the user's information is employed and picked up, the study found that users' information would be created anonymous, encrypted, secured, and can be transmitted on-line and stored solely in an aggregated format. Contact tracing apps use either a centralized or a decentralized approach to work the user's information. Apps that use a centralized approach have high privacy risks. In this paper, the researcher's contributions related to the security and privacy of Contact tracing apps have been discussed and, later research gaps have been identified with proposed solutions.

Keywords Tracing apps · User's privacy · Data security · AES encryption · Cloud storage

Introduction

The outbreak of COVID-19 has taken the world by unpleasant surprise and stressing public health care systems. This virus outbreak changed the lifestyle of every individual and forcing the governments to mandate lockdowns, recommended social distancing, self-isolation, work from home policies, and all educational institutions were closed. Abovementioned measures are aimed at decreasing the mass spread of the virus and leading to Flattening of the curve until the treatment an approved vaccine is developed. The COVID-19 pandemic has unfolded across the globe and resulted in substantial loss of lives and livelihoods. These viruses imposed substantial mortality, morbidity on human populations. It is an ongoing pandemic of coronavirus disease 2019 (COVID-19) caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2 and MERS), which spreads between people, mainly when an infected person is in close contact with another person, first identified in December 2019 in Wuhan, China. COVID-19 virus transmission occurs for several days before a person shows any symptoms. During this time, a person going about their daily life may interact with, and possibly pass the infection to, without knowing they are affected, an individual who has only mild symptoms or is asymptomatic may continue to interact with others, further spreading the virus. Public Health Emergency of International Concern was declared in January 2020 and a pandemic in March 2020. As of 1 November 2020, more than 46.1 million cases have been confirmed, with more than 1.19 million deaths attributed to

This article is part of the topical collection "Cyber Security and Privacy in Communication Networks" guest edited by Rajiv Misra, R K Shyamsunder, Alexiei Dingli, Natalie Denk, Omer Rana, Alexander Pfeiffer, Ashok Patel and Nishtha Kesswani.

✉ M. Thangavel
thangavelmuruganme@gmail.com

[1] Department of Information Technology, Thiagarajar College of Engineering, Madurai, Tamilnadu, India

[2] Melmaruvathur Adhiparasakthi Institute of Medical Sciences and Research, Melmaruvathur, India

[3] Department of Computer Science and Engineering, Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, Odisha, India

[4] Department of Computer Technology, Madras Institute of Technology, Anna University, Chennai, Tamilnadu, India

COVID-19. As the number of positive cases increases by the seconds, it was a more challenging task to control transmission. Traditionally, public health officials perform contact tracing manually, by interviewing patients diagnosed with a disease about their activity over the past days or weeks. Then they reach out to people who crossed paths with the patient during the time, the patient was infected and recommend targeted interventions to prevent further spread of the disease. To resolve this issue "contact tracing" is to identify the individuals who had proximity with a positive case, as these persons may themselves now be infected by the coronavirus disease. To fight this pandemic situation, many countries have developed Digital contact tracing mobile applications. Australia was the first country to launch its contact tracing application. A contact-tracing application [1] can track every user who has been having been in proximity and then it alerts all affected users when one of them confirms positive for infection. Some contact-tracing applications can also inform users when an infected person is nearby and helps in preventing possible infection. The major concern of these contact tracing apps is their architecture, data storage, data management, privacy, and security. However, the data collection process lacks transparency. For example, even with Bluetooth Low Energy (BLE) in which reallocation is used, it could have various data leakages and meanwhile, the identity of an infected user could be de-anonymized by authorities or other users.

A typical contact tracing app works as follows: the app should be installed on an individual's cell phone and the Bluetooth of the phone must always remain on. Two users, who have the same app, reach in proximity, the app exchanges a unique identifier using Bluetooth which is stored either in the phone storage or in a centralized database. If a person is found to be COVID-19 positive, his/her mobile is taken to collect all the details that had so far been stored in the device and centralized server. Then those individuals are warned as soon as possible. For providing timely exposure notifications, accurate contact tracing information plays an important role. For that intention, users' personal information such as movements, details of the persons the suspected user contacted, etc. has to be disclosed. The application can make available for the use of the data with reliable accuracy only if the collected data is sufficient. In the case of storing more information, will leads to increased breach of privacy which is a major privacy concern these days. By analyzing a lack of transparency as well as privacy concerns in contact tracing applications, we conducted a systematic study of the contact tracing applications that have been released by governments and healthcare authorities. While there are many aspects to consider, we focus on the following ones: (i) which type of privacy-related information (i.e., information that reveals one's identity) has been collected for contact tracing? (ii) Are these apps designed and implemented correctly to avoid privacy leakage? (iii) is the data being transmitted to other parties, e.g., servers or other users, privacy-preserving (e.g., has the data been protected against eavesdropping, tracking, and de-anonymization attacks)? And (iv) do these apps behave consistently on different mobile platforms?

The Literature Survey describes the features of current contact tracing apps and gives insights into their privacy and security implications [3].

Covid Tracing Application

Information disclosure is defined as information leakage when individuals intentionally reveal sensitive data to others. With the outbreak of Coronavirus disease, contact tracing is becoming an intervention to control the spread of this highly infectious disease. Traditionally health workers perform contact tracing manually by patients diagnosed with the disease. Then workers reach out to the people and suggest measures to prevent further spread of the disease. Mass spread, fast-flowing transmission by respiratory droplets which is in the case of coronavirus disease challenges. Manual Tracing is limited, time-consuming, not accurate, and resource-intensive. Digital Contract Tracing tools can solve these challenges. The contract Tracing process finds the recent location history and connections of those who were infected and alerts the people before they have interacted with their exposure to the virus. In this way, contact tracing allows measures such as social distancing, self-quarantining, virus testing to be applied to the infected individuals. Today, most of the world's population carries a smartphone, GPS tracking, and Bluetooth Communication. Each device is capable of creating a location trail of an individual when the device's user crosses in proximity to another device. By estimating the device user's trails or Unique ID, they have collected from those people who were infected with Covid-19, one can identify others who have been near the infected individual. These types of contact tracing applications are timely manner than the traditional manual approach.

The most commonly used Covid-19 tracing apps are centralized and decentralized approaches. Figure 1 shows the generalized architecture which follows a centralized approach based on Bluetooth technology and GPS. The initial requirement of the application is that the user needs to register with the server. The server generates a temporary ID for each device. The temporary key is encrypted using a secret key and it is sent to other devices. Devices exchanges their temporary ID through Bluetooth when they are in proximity to an infected individual. Once the individual tested positive for Covid-19, corresponding health workers are mandated to upload the encounter messages to the central server or the user can voluntarily

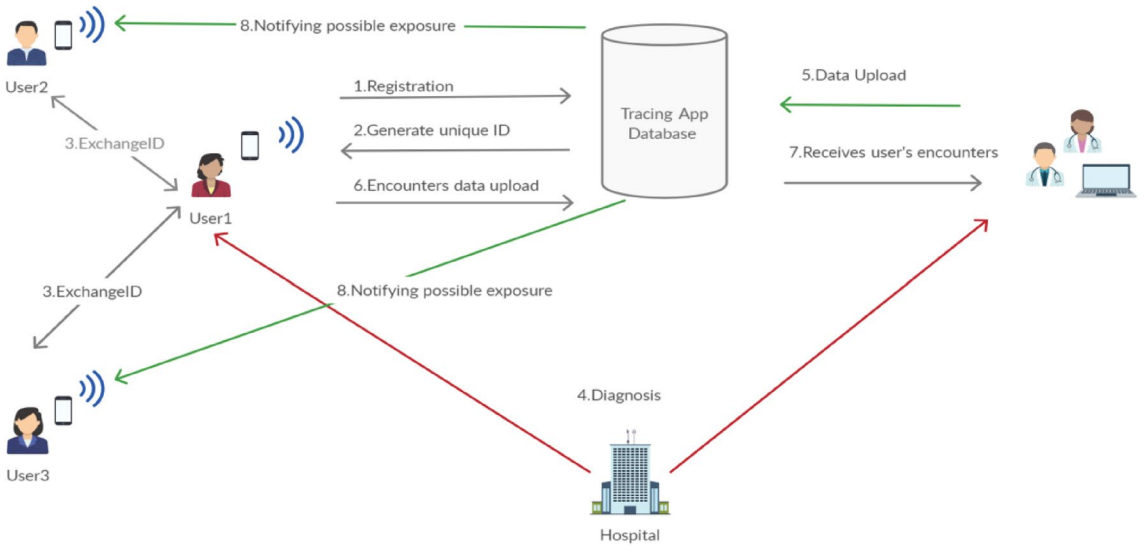

Fig. 1 The centralized architecture of Covid Tracing Apps

upload all of their details to the server. The centralized server maps the temporary ID in the messages to individuals to identify at-risk contacts. Figure 2 shows the decentralized architecture which has core functionalities to the user's devices, leaving the server with minimal involvement in the contact tracing process. This approach enhances the user's privacy by generating anonymous identifiers at the user devices and processing the exposure notifications on individual devices instead of the centralized server. Once the person tested positive for Covid-19, they can upload their coded key to a central server. This is in contrast to the centralized architecture where the complete details of the user are uploaded.

Existing Contact Tracing applications

Several countries have different apps for contract tracing. Table 1 provides overview of existing contact tracing solutions. Digital contact tracing applications use data to interfere with the contact of two individuals. The most used data resource is GPS location and Bluetooth technology. GPS-based contact tracing applications create a trail for every user by recording their temporal GPS location. If the individual catches Covid-19, they should share their trail with the authority. The authority may be a health worker, government officials. Then the corresponding authority releases the trail for other users to identify the infected individual.

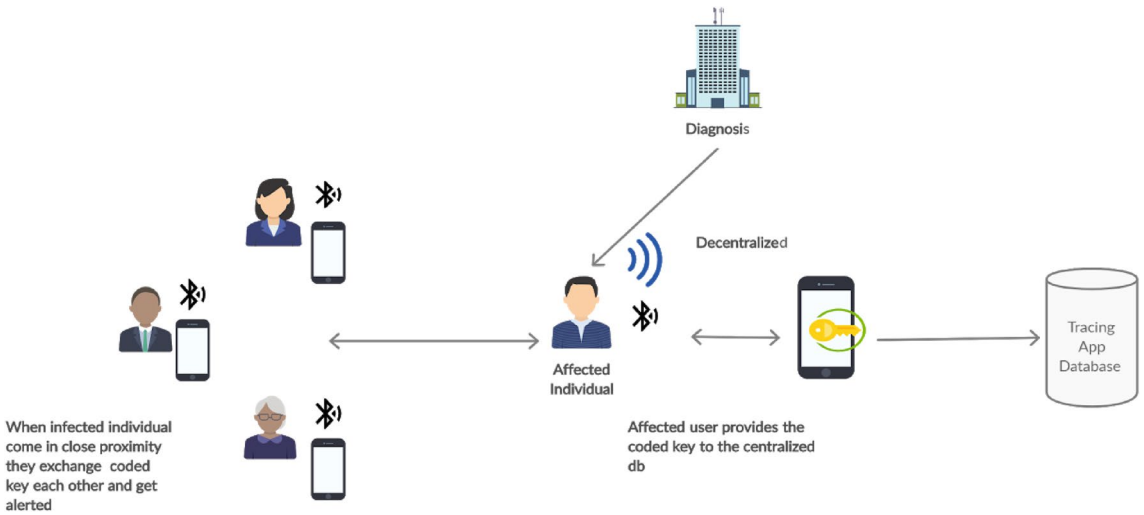

Fig. 2 The decentralized architecture of Covid Tracing App

Table 1 Overview of the existing contact tracing solutions

Country	App name	SSL	Transparency	Centralized/decentralized	Access control
India	Arogya Setu	N/A	Yes	Centralized	Location access,bio data
Singapore	TraceTogether	N/A	Yes	Centralized	Microphone, location, camera, storage, Wifi Connection, and Media access
Australia	CovidSafe	N/A	No	Centralized	Location access, Connects personal data to the server
Canada	CovidAlert	No	No	Centralized	Location access, Personal data connected to the health authority
Dubai	DXB Smart App	N/A	No	Centralized	Microphone, location, camera, storage, Wifi Connection, and Media access
United States	CovidWise	No	No	Decentralized	Microphone, location, camera, storage, Wifi Connection, and Media access
Pakistan	COVID-19 Gov PK	No	No	Centralized	Location access
Vietnam	Bluezone	N/A	No	Centralized	Microphone, location, camera, storage, Wifi Connection, and Media access
Malaysia	Mytrace	Yes	Yes	Centralized	Microphone, location, camera, storage, Wifi Connection, and Media access
Saudi Arabia	Covid-19KSA	N/A	No	Decentralized	Location access, Personal data connected to the health authority
UK	NHS Covid-19	N/A	No	Centralized	Network access
Netherlands	CovidRadar	N/A	Yes	Decentralized	Location access, Personal data connected to the health authority

Bluetooth-based contact tracing apps create a unique identity for every user which may be static or dynamic in which the application transmits to nearby devices. The user's mobile then records the identifiers of other mobiles it has been near. For instance, Singapore launched its Covid tracing application in March 2020 named "Trace Together". This app uses Bluetooth technology to collect data regarding users who have close to one another. These data are utilized by the health ministry to track and contact all individuals who have come in contact with a Coronavirus disease patient. The app uses dynamic ID which adds a layer of security. However, in this application, the temporary IDs are generated by the central server. Australia launched its digital contact tracing application named "Covidsafe" in April 2020. 2 million people downloaded in the first 24 h. It is the most adopted contact tracing application by the nation in the world for tracking Coronavirus disease in the pandemic. This application uses Bluetooth Low Energy technology and it takes a note of contact when it takes place through a digital handshake this application uses Bluetooth Low Energy technology and it takes note of contact when it takes place through a digital handshake. It records the other user's encrypted details reference code, date, time, Bluetooth signal strength, and proximity of the contact on the user's mobile and also records the phone's model. This information is encrypted using functional encryption and stored on the devices. This app stores users' details for 21 days and it automatically deletes the user's data.

New Zealand launched its Covid tracing application named "NZ Covid Tracer" for the ministry of health. This app uses Bluetooth technology to track the users who have been in proximity for more than 15 min. It allows users to scan the ministry of health QR codes at public buildings, businesses, and organizations for tracking purposes. People can also register their details on the NZCOVID tracer website. The user's data will be stored for 60 days on the user's device and then it automatically deletes the information. France launched a new contact tracing app named "TousAntiCovid" which is the enriched version of its previous application called Stop Covid. It uses Bluetooth technology to track user's movements and it is centralized. Aarogya Setu is a Covid tracing app "syndromic surveillance, self-assessment" developed and implemented by National Informatics Centre under the Ministry of electronics and information technology. It uses the smartphone's GPS and Bluetooth low energy technology to track the coronavirus infection. It generates static random IDs for each device to identify the user. It's mandatory to enable the Bluetooth all time, so it allows attackers to access Bluetooth devices through the technique called Key Negotiation of Bluetooth (KNOB). KNOB is done when the two devices talk to each other, they first generate an encrypted communication channel. Then the hacker can easily use the brute force technique to retrieve the key and Decrypt all communications. To do this technique, nearby attacker forces that device to use weaker encryption when it connects, making it easier for him to crack it. Germany launched its application named "Corona Warn App" which does not store the location of users by concerning the Privacy of every user and it works together

with Apple and Google. The exposure Notification System on the device transmits a rolling proximity identifier, while also regularly scanning for identifiers of phones using Bluetooth technology and storing the identifiers locally. Those identifiers are only valid for 20 min and derived using Cryptography from dynamic keys which changes every 24 h. A knock-on effect, England launched "The NHS COVID-19 app, running QR code-based systems to collect user's information. Every business venue was mandated to display QR code posters Users can scan these codes and register their names and mobile numbers, so that if the infected case of coronavirus disease was tracked to the venue and they would be informed by trace workers. The summary of the concerns over contact tracing applications has been depicted in Fig. 3.

Privacy Concerns-Contact Tracing

Since governments have been built contact tracing applications. In most apps, users were monitored and tracked without the user's consent. If such apps record the location history, the user's movement can be traced as well. Apart from tracing the location, there are many privacy issues, such as data breach, data collection, obscure data flow [3–8, 10–12, 16, 18].

Voluntary or Mandatory

The government should not mandate users to use these apps in any circumstances. It should be voluntary in using such tracing apps. Considering the concern over data privacy, unnecessary data collection, location tracking, and other issues, users must have free wills to decide by the users who installed the application.

Information Destruction

Mobile applications or a framework should automatically delete user records after a particular period (e.g., usually 14–21 days and no longer than 30 days). Otherwise, users should have manual control over data deletion from the app or the central server.

Transparency

The process of data collection, usage, and storing should be transparent to protect user privacy. The application should have policies, concise data flow, databases, and open-source code for transparency. While developing an application, one must follow the compliance and consent rules such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA).

Data Collection

Many applications collect excessive, unnecessary data from their users, for instance, an application named "Aarogya Setu" requires name, mobile number, age, gender, profession, and details of countries visited in the last 30 days Also, Geo-location tracing is unnecessary alongside Bluetooth or other similar wireless technologies.

Disclosure of Location

Location illustrates the interaction between individuals by representing the individuals as nodes and connection between the nodes as endpoints indicating that users may

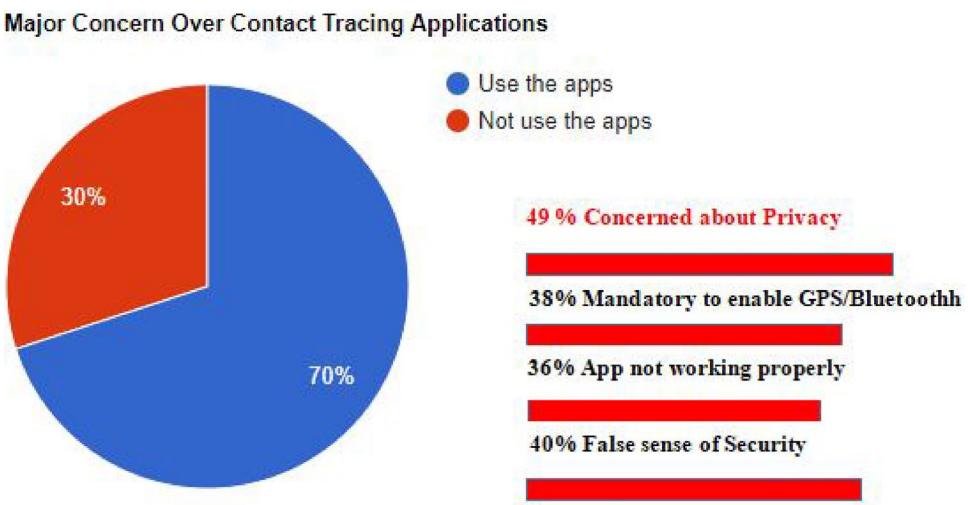

Fig. 3 Concerns of various existing solutions

have been in proximity. An adversary can build a social graph by mining the data to infer the user's contact profiles. Disclosure of the location or the social graph is undesirable, however, some countries such as India have done so despite concerns from civil society. Both centralized and decentralized architecture is vulnerable to the disclosure of location details.

Security Issues Associated with the cloud

Many security issues are existing in the cloud computing system. While believing the third party, users should query about seven safety issues: privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, and long-term viability. Several security issues have been identified in Covid tracing applications by Cloud Security Alliance (CSA) in different cloud domains and also provided security guidelines. Data Security breaches, data loss, outages that occurred in the cloud were reported by analyzing Covid tracing applications.

Security Attacks

There are some of the possible attacks that can be launched against different Covid tracing applications [19–29].

Bluesnarfing

Bluesnarfing is the security attack, which forces the connection with a Bluetooth-enabled device to gain access to sensitive data such as pictures, videos, emails, contact list, calendar and the International Mobile Equipment Identity (IMEI) stored in the memory. IMEI is a 15 digit unique identifier for devices and can be exploited by an attacker to divert all incoming calls from the user's device to the attacker's device. Sensitive information may be stolen from the devices through bluesnarfing without the owner's knowledge. Covid Tracing applications like Trace together, covidSafe, Arogya-Setu uses Bluetooth technology (which generates a random ID for each device) to identify the user and collect information regarding users who have been close to one another.

Playback Attack

A playback attack is also known as a replay attack in which the data transmission is delayed or maliciously repeated. This is done by the initiator who intercepts the data and re-transmits it, possibly as part of a masquerade attack by packet substitution. This attack is one of the lower-tier version of "Man in the middle attack". In these types of attacks, an adversary aims to force the users to store the misleading contact data, resulting in false messages. This is done by forwarding any type of message received from users at the same or different locations. The attacker requires minimal resources to launch this attack but he/she may use antennas to extend the area of its influence further. This playback attack is the simplest of the attacks that can be launched against users of the Covid tracing app.

Wireless Device Tracking

Applications that use the centralized architecture, temporary ID, and device model information can be used to identify the device easily. Since the temporary ID is changed after a short time (approximately 10–15 min), tracking the device beyond the point where the device starts advertising a new Temp ID would require extra intelligence to link the two Temp ID to the same device, advertising the same phone model. In the case of a decentralized approach, architecture provides only limited opportunities for tracking. The tracking server can still enumerate the total number of users in a particular area; however, it is difficult to track the movements of the device without the device model. In this case, tracking would apply to limited scenarios.

Denial of Service

This attack aims to utilize the resources available in the system (user, mobile, server). In this regard, we discuss the issue of an adversary injecting bogus encounter messages/chirps into the contact tracing environment. This attack is done with the following intentions such as consuming device storage and battery in both centralized and decentralized architectures. An adversary may cause an upload of this misinformation to the server once the user tested positive in a centralized approach. This may increase the processing timestamp at the server in both centralized architecture and decentralized architecture.

Enumeration

The purpose of this attack is to count the number of users who have tested positive for the covid-19 in the centralized architecture. In this attack, an attacker can estimate the number of users infected with the Covid-19, who have been volunteered to upload their contact tracing data to the Centralized architecture.

Carryover Attack

In this attack, an attacker aims to continue the device tracking period beyond the anonymous ID expiration time. Most of the application randomize their Bluetooth MAC addresses to avoid device tracking. The temporary identifiers get changed after a short time. An address attack is done when

the change over time of the Bluetooth MAC address and the temporary identifier have not coincided. For an instance, let us consider that the Temp ID gets changed every 20 min, while Bluetooth MAC changes every 10 min. An observer can easily link the multiple Bluetooth MAC addresses released within the lifetime of the same Temp ID. Contrarily Temp ID change can be connected to the same Bluetooth address. Complete synchronization of temporary transient identifiers and the Bluetooth random MAC address change are proposed in some Covid tracing applications.

State of the Art

In this section, existing works related to privacy preservation issues in contact tracing are discussed. Table 2 provides the comparison of existing work with respect to methodology and inference.

Whaiduzzaman et al. [9] proposed a fog-based IoT healthcare Contact Tracing Application. It ensures data privacy, security, optimization of data communication, low power consumption, and also enhances efficiency in terms of cost, network delay, and energy consumption. Authors have introduced Automatic Risk Checkers (ARC) and Suspected User Data Uploader Node(SUDUN) which is the fog nodes for tracing purpose. Rotational Unique Encrypted Reference Code (RUERC) which is the unique ID will be transmitted through Bluetooth Low Energy (BLE). The concept of implementing ARC's at the business venues, and other organizations, which will instantly detect the individuals if they are infected. If the positive case found in proximity, ARC will transmit the pre-cautionary messages to nearby people. The implementation of SUDUNs at Hospitals and health centers will report the test results to the cloud.

Wenzhe et al. [13] proposed a peer-to-peer system of a blockchain protocol, provides users with a unique ID, transparent data storage, location proofing, and zero-knowledge proof-based data ownership authorization. The concept of introducing the Delegated Proof of Stake (DPoS) consensus mechanism is based on the virtual electronic field to enhance the location proofing service. Implementing these types of measures does not need a trusted third party and a centralized server.

Garg et al. [2] proposed an Internet of Things (IoT) model which captures information on patient' movements and contact of objects. This solution ensures that this is anonymously executed until users have tested positive for a COVID-19 disease. The concept of implementing a proof-of-concept will utilize a passive Radio Frequency Identification (RFID) transceiver for the IoT component. Users can wear passive RFID tags without having mobile phones with them. This is the first solution proposing IOT with specifically RFID for anonymized RFID

Table 2 Comparison of existing works

Work	Methodology	Inferences
[9]	Application using mobile and fog computing, privacy-preserving e-government framework to trace and prevent COVID-19 community transmission	Ensures data privacy, security, optimization of data communication, low power consumption, and also enhances efficiency in terms of cost, network delay, and energy consumption
[2]	IoT-based tracing framework. Anonymized RFID contact tracing of Infection spread. Blockchain technology is used for data storage to ensure privacy	Secure and efficient for contact tracing The identity privacy problem is protected by the combination of zero-knowledge proof and key escrow. By the connection of unique cryptographic identity and on-chain proof-of-location commitment is decoupled such that it is almost impossible to track and identify the person
[13]	A peer-to-peer system of a blockchain protocol, used for contact tracing. Provides users with a unique ID, transparent data storage, location proofing, and zero-knowledge proof-based data ownership authorization	Does not require trusted third-party services and centralized servers and ensures the anonymity of users
[14]	A decentralized approach for contact tracing	Secure storage and Efficient for contact tracing. APIs used to support applications developed by governments, health workers intended to work seamlessly
[15]	Machine learning used for screening, prediction, forecasting, contact tracing, and drug development for SARS-CoV-2	Requires large amounts of data to achieve higher efficiency Training of data might take a long time

contact tracing of Infection spread. Blockchain technology is used for data storage to ensure privacy through distributed ownership and management of stored data. Smart Contract (SC) is used for storing captured proximity information.

Apple and Google have joined to enhance privacy-preserving contact tracing by introducing an exposure notification system [14]. Their tracing mechanism is the decentralized approach for contact tracing system. The system consists of two phases. In the first phase on 20th May 2020, Application Program Interface (API) methodologies were released to support applications developed by governments, health workers intended to work seamlessly on IOS and Android devices. This measure helps to manage issues related to Bluetooth Low Energy (BLE) scanning and advertisements faced by current applications. During the exposure notification service, the system utilizes the proposed Associated Encrypted Metadata (AEM). AEM is the privacy-preserving encrypted metadata that includes power transmission to aid in collecting more accurate proximity estimation reports. Once the individual downloads a contact tracing application that uses the exposure notification API released by Apple and Google and opts in to contact tracing applications. The users who installed such applications their devices start generating "Proximity identifiers" which is dynamic, changed every 15 min (approximately). Through BLE, those proximity identifiers are periodically shared with nearby devices whose users have also opted into the same contact tracing application. The proximity identifier is then processed on the device and does not reveal the data about the user's location or other personal details. Once the user confirms a positive diagnosis of coronavirus disease, they can share their diagnosis details with the application they installed, which will then inform other users who have come into proximity with them in the last 14 days.

Hao et al [17] proposed solutions combined with the use of blockchain, encryption, and anonymization technologies to ensure the user's privacy. Blockchain is non-regional, transparent, and provides a suitable Global access platform for COVID-19 pandemic tracing and control. The transparent feature can prevent the public from intentional misinformation by authorities or third parties. Samuel et al [15] used a significant method in the field of screening, prediction, forecasting, contact tracing, and drug development for SARS-CoV-2. The assessment of information on the research was executed on the databases related to the application of Machine Learning (ML) and Artificial Intelligence (AI) on Covid-19. It also addresses challenges while using some algorithms for storing the user data in the Covid tracing application.

Proposed Solution

Several Covid-19 tracing apps store user's data using weaker encryption standards. User's data can be encrypted using a secure algorithm. The cryptographic encryption algorithms can be mainly categorized into two types: symmetric key encryption. In symmetric key encryption, a single secret is used for both encryption and decryption. In contrast to the symmetric key, an asymmetric key, encryption is performed using two different keys namely public key and private key. The public key is used for encryption and the private key s used for decryption. There are three encryption standards namely Advanced Encryption standards (AES), Data Encryption Standards (DES), and Rivest-Shamir-Adleman (RSA). Advanced Encryption Standard (AES) algorithm is the symmetric block cipher. It has a particular structure to encrypt and decrypt the sensitive data or files which is applied in hardware and software all over the world. It is very difficult for hackers to retrieve the original data while the application using the AES algorithm. AES was published by the National of Standards and Technology (NIST) in 2001. It is the symmetric block cipher that replaces the Data Encryption Standards (DES). Table 3 provides the feature comparison of AES and DES.

The cipher takes plaintext of size 18 bit. The key length can be 128,192,256 bits. The algorithm is referred to as AES-128, AES192, and AES-256 depending on key length. The cipher consists of N rounds depends on key length: 10 rounds for a 128-bit key, 12 rounds for a 192-bit key, and 14 rounds for a 256-bit key. First N-1 rounds consist of 4-transformation functions permutation (ShiftRows) and three substitutions (Substitute bytes, MixColumns, AddRoundKey). The final round of both encryption and decryption consists of three stages namely substitution bytes, MixColumns,

Table 3 Comparison between AES and DES

Features	AES	DES
Developed by	Vincent Rijmen	Horst Feistel
Length of the Key	128,192,256 bits	56bits
Block Size	128bits	64bits
Rounds	10,112,114 rounds	16 rounds
Algorithm type	Symmetric Key	Symmetric Key
Encryption Time	Fast	Medium
Decryption Time	Fast	Medium
Power Consumption	Less	Less
Security	High	meet-in-the-middle attack *(MITM)*
Scalability	No	Yes
Efficiency	High	Medium

and AddRoundKey. Substitute bytes use the S box for byte by byte substitution. MixColumns makes the use of modular arithmetic of four-term polynomials over GF (2^8). AddRoundKey is a bit-wise Xor operation of the current block with a portion of the expanded key.

Cloud Storage and Security

Cloud Security is also referred to as cloud computing security refers to a line of policies, technologies, and controls deployed to safeguard data, applications, and associated infrastructure of cloud computing (Fig. 4).

Registration

Users can register through hospitals /Labs /health centers or Self-assessment (Fig. 5). Through hospitals user's details like name, Phone number, and further details can be collected and uploaded in the cloud for storage.

Storage

For storing user's information, we cloud with secure symmetric encryption standards (Fig. 4). AES is secure symmetric encryption than DES. It is a process that is at least six times faster than triple DES. The encryption consists of 10 rounds for 128-bit keys. User's Details will be split into different blocks based on collected details. Then individual blocks are encrypted separately. After block-wise encryption, each block was uploaded to the cloud at different locations with user-encrypted _id and block_id. For contact tracing, it is enough to use the User's encrypted id to alert the nearby person.

Tracing

iBeacon (Bluetooth low-level Energy) is a compatible hardware transmitter. This device consistently broadcasts a Bluetooth 4.0 signal (BLE) and its unique identifier to nearby portable electronic devices. iBeacon's communication is one-way, that an iBeacon could transfer information to a receiver device (such as a mobile phone, a laptop, etc.) without the need for pairing, making the process significantly more transparent. The ID (which is to be changed for every 1 min like google authenticator) sent with it can be used to determine the device's physical location, track users on the device. Users are notified whenever they're too close to a person infected from coronavirus or someone who is at high risk.

Data Privacy and Security

The model consists of 128bit AES encryption. The encryption consists of 10 rounds for 128bit keys. The fields in the user's data were split into different blocks and then individual blocks are encrypted separately. After block-wise encryption, each block is uploaded to the cloud at different locations in encrypted form. If anybody tries to access the user's data directly from the server, they cannot get the whole data since it is stored at different locations. The person who knows secret data-id can retrieve data concerns regarding the collection and use of data and its security.

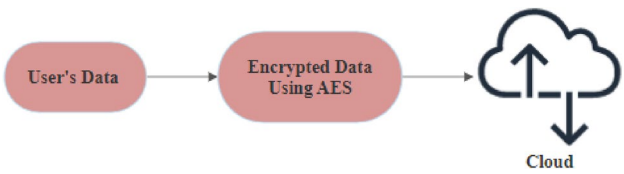

Fig. 4 Architecture for storing user's data

Future Scope

Hence a mobile application should be user-centric and should protect users from unwanted intervene. Future work remains to build an application by adding high security and feasibility in tracing and storing the user's data. It is also designed with an automatic generation of reports by self-diagnosis with a high rate of accuracy. These types

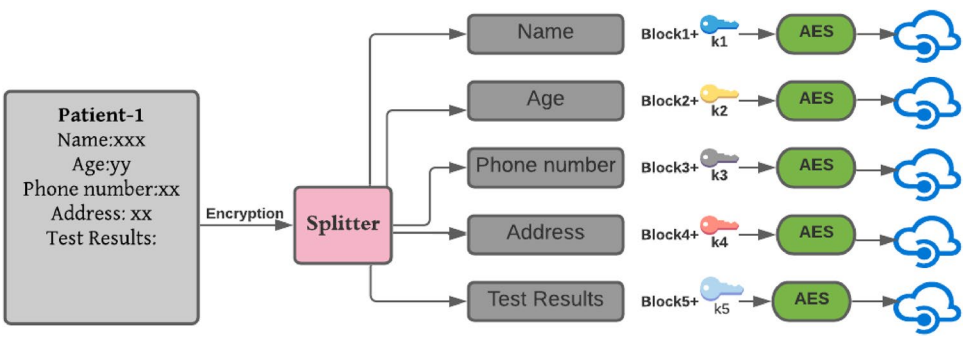

Fig. 5 User's Data Encryption and Storage

of measures will increase the privacy of the snoopers, adversaries.

Conclusion

As Coronavirus spreads through close social interaction, contact tracing has become vital for containing its spread. Mobile devices present an ideal platform to introduce contact tracing software due to their ease of use, widespread ownership, and personalized usage. Therefore, several smartphone apps have been developed by governments, international organizations, and other parties to mitigate the virus spread. However, there is an increasing concern regarding the collection and use of data and its security. In this paper, we analyzed a huge set of contact-tracing apps implementing different security and privacy measures. Specifically, we analyzed contact-tracing apps for privacy, data storage, and data security. From our survey, we conclude upon the AES encryption standard and random cloud storage for protecting the collected data.

Compliance with Ethical Standards

Conflict of Interest The authors declare that they have no conflict of interest.

Ethical Approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. AM Arshad, J Akmal, A Abdullah, S Ahmad, F Imran, M Riaz, F (2020) A first look at contact tracing apps. Url https://arxiv.org/pdf/2006.13354.pdf
2. Garg L, Chukwu E, Nasser N, Chakraborty C, Garg G. Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model. IEEE Access. 2020;8:159402–14. https://doi.org/10.1109/ACCESS.2020.3020513.
3. D. Zeinalipour-Yazti and C. Claramunt (2020) COVID-19 mobile contact tracing apps (MCTA): a digital vaccine or a privacy demolition?, 2020 21st IEEE International Conference on Mobile Data Management (MDM), Versailles, France https://doi.org/10.1109/MDM48529.2020.00020.
4. Jaiswal R, Agarwal A, Negi R. Smart solution for reducing the COVID-19 risk using smart city technology. IET Smart Cities. 2020;2(2):82–8.
5. Ahmed N, Michelin R, Xue W, Ruj S, Malaney R, Kanhere S, Seneviratne A, Hu W, Janicke H, Jha S. A Survey of COVID-19 contact tracing apps. IEEE Access. 2020;8:134577–601. https://doi.org/10.1109/ACCESS.2020.3010226.
6. Michael K, Abbas R. Getting behind COVID-19 contact trace apps: the google-apple partnership. IEEE Cons Electr Mag. 2020. https://doi.org/10.1109/MCE.2020.3002492.
7. Abbas R, Michael K. COVID-19 contact trace app deployments: learnings from Australia and Singapore. IEEE Cons Electr Mag. 2020;9(5):65–70. https://doi.org/10.1109/MCE.2020.3002490.
8. Hernández-Orallo E, Manzoni P, Calafate CT, Cano J. Evaluating how smartphone contact tracing technology can reduce the spread of infectious diseases: the case of COVID-19. IEEE Access. 2020;8:99083–97. https://doi.org/10.1109/ACCESS.2020.2998042.
9. Whaiduzzaman M, Hossain MR, Shovon AR, Roy S, Laszka A, Buyya R, Barros A. A privacy-preserving mobile and fog computing framework to trace and prevent COVID-19 community transmission. IEEE J Biomed Health Informat. 2020;24(12):3564–75. https://doi.org/10.1109/JBHI.2020.3026060.
10. Dubov A, Shoptawb S. The value and ethics of using technology to contain the COVID-19 epidemic. Am J Bioethic. 2020;20(7):W7–11. https://doi.org/10.1080/15265161.2020.1764136.
11. Basu S. Effective contact tracing for COVID-19 using mobile phones: an ethical analysis of the mandatory use of the aarogya setu application in India. Camb Quarter Healthcare Ethics. 2020. https://doi.org/10.1017/S0963180120000821.
12. J Bay, J Kek, A Tan, CS Hau, L Yongquan, J Tan, and TA Quy (2020) BlueTrace: a privacy-preserving protocol for community-driven contact tracing across borders. Govt Technol Agency-Singapore Tech Rep. https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf. Accessed 31 Jan 2021.
13. W Lv, S Wu, C Jiang, Y Cui, X Qiu, Y Zhang (2020) Decentralized blockchain for privacy-preserving large-scale contact tracing Url: https://arxiv.org/abs/2007.00894
14. DJ Leith, S Farrell (2020) Measurement-based evaluation of google/apple exposure notification API for proximity detection in a commuter bus. Url: https://arxiv.org/abs/2006.08543
15. Lalmuanawma S, et al. Applications of machine learning and artificial intelligence for Covid-19 (SARS-CoV-2) pandemic: a review. Chaos Solitons Fractals. 2020;139:110059. https://doi.org/10.1016/j.chaos.2020.110059.
16. Bassi S, Chaudhary A. Cloud computing data security-background and benefits. Int J Comp Sci Commun. 2015;6(1):34–40.
17. Xu H, Zhang L, Onireti O, Fang Y, Buchanan WJ, Imran MA. BeepTrace: blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond. IEEE Int Things J. 2020. https://doi.org/10.1109/JIOT.2020.3025953.
18. A Ako. (2017) Advanced encryption standard (AES) algorithm to encrypt and decrypt data. Url: https://www.researchgate.net/publication/317615794. Accessed 31 Jan 2021
19. Jonker M, et al. COVID-19 contact tracing apps: predicted uptake in The Netherlands based on a discrete choice experiment. JMIR mHealth uHealth. 2020;8(10):e20741. https://doi.org/10.2196/20741.
20. O'Dowd A. Covid-19: app to track close contacts is launched in England and Wales. BMJ (Clin Res ed). 2020;370(m3751):25. https://doi.org/10.1136/bmj.m3751.
21. Apple Covid 19 App and Website (2020) Url: https://www.apple.com/newsroom/2020/03/apple-releases-new-covid-19-app-and-website-based-on-CDC-guidance/. Accessed 31 Jan 2021
22. Y Gvili (2020) Security analysis of the covid-19 contact tracing specifications by apple inc. and google inc., Url: https://eprint.iacr.org/2020/428.pdf. Accessed 31 Jan 2021
23. Currie DJ, et al. Stemming the flow: how much can the Australian smartphone app help to control COVID-19? Public Health Res Pract. 2020;30(2):3022009. https://doi.org/10.17061/phrp3022009.
24. Susanto H, Leu F-Y, Caesarendra W, Ibrahim F, Haghi PK, Khusni U, Glowacz A. Managing cloud intelligent systems over digital ecosystems: revealing emerging app technology in the time of

the COVID19 pandemic. Appl Syst Innov. 2020;3:37. https://doi.org/10.3390/asi3030037.
25. Whitelaw S, Mamas MA, Topol E, Van Spall HGC. Applications of digital technology in COVID-19 pandemic planning and response. Lancet Digit Health. 2020;2(8):e435–40.
26. Simmhan Y, Rambha T, Khochare A, Ramesh S, Baranawal A, George JV, Bhope RA, Namtirtha A, Sundararajan A, Bhargav SS, Thakkar N, Kiran R. GoCoronaGo: privacy respecting contact tracing for COVID-19 management. J India Instit Sci. 2020. https://doi.org/10.1007/s41745-020-00201-5.
27. G Magklaras, LNL Bojorquez (2020) A review of information security aspects of the emerging COVID-19 contact tracing mobile phone applications. Url: https://arxiv.org/abs/2006.00529
28. Tropea M, De Rango F. COVID-19 in Italy: current state, impact and ICT-based solutions. IET Smart Cities. 2020;2(2):74–81.
29. Veale M (2020) Privacy is not the problem with the Apple-Google contact-tracing toolkit. Url: https://www.theguardian.com/commentisfree/2020/jul/01/apple-google-contact-tracing-app-tech-giant-digital-rights. Accessed 31 Jan 2021