Toward a secure global contact tracing app for Covid-19

Muhammad Hamza
LUT University, Software Engineering, 53851 Lappeenranta, Finland
hamzajee541@gmail.com

Arif Ali Khan
M3S Unit, Empirical Software Engineering in Software, Systems, and Services, University of Oulu, Finland
arif.khan@oulu.fi

Muhammad Azeem Akbar
LUT University, Software Engineering, 53851 Lappeenranta, Finland
azeem.akbar@lut.fi

ABSTRACT

The outbreak of the covid-19 pandemic has devastated many sectors of each country and led to the development of contact tracing applications for controlling its spread. Contact tracing apps have been promoted to track infected contacts. However, contact tracing has gained significant debate due to its security and privacy concerns. The goal of this study is to examine the most popular contact tracing apps, their impact on pandemic control, as well security and privacy concerns. The multivocal literature review (MLR) brings the results from the state-of-the-art literature. We extracted 23 studies from both formal and grey literature to achieve the research objectives and found several security and privacy threats in the existing contact tracing applications. Additionally, the best practices to address these threats were also identified. We further proposed a preliminary structure of a secure global contact tracing app using blockchain technology.

CCS CONCEPTS

• Software and its engineering; **• Human-centered comput- ing;**; **• Computing methodologies**; **• Artificial intelligence;**;
• Philosophical/theoretical foundations of artificial intelligence;; **• Social and professional topics**; **• Empirical studies**;

KEYWORDS

Contact tracing apps, Multivocal literature review (MLR), Framework, Blockchain, COVID-19

1 INTRODUCTION

The global outbreak of Covid-19 has led the world toward the drastic loss of health, agriculture, and economic sectors [1]. The pandemic outbreak at the begging of January 2020 in China's most famous city Wuhan [1]. The rise in the Covid-19 cases increased the mortality rate worldwide. The surge in the cases forced governments to impose strict lockdown to prevent its spread, which eventually devastated many countries' economic and social activities. It has been predicted that more than 140 million people could face extreme poverty by losing their livelihood due to the pandemic. The contagious disease having predominantly pulmonary symptoms caused more deaths. However, few prevention measures include hand washing with a sanitizer, hydro-alcoholic methods, or social distancing that could limit the spread of Covid-19 [2]. Among all these measures, social distancing and contact tracing are considered significant for controlling the pandemic spread [2]. However, the unexpected spread of the pandemic failed the manual contact tracing platforms and forced governments and organizations to develop digital contact tracing systems [3, 4]. The rise in innovative technologies such as Internet of things (IoT) and Artificial Intelligence (AI) has significantly changed the medical field [34]. The IoT comprised several sensors, actuators, embedded systems, and machine learning-based software that allows the connection of different devices across the internet and sharing of information. These devices further obtain data by using wireless body area networks (WBANs), wireless sensor networks (WSNs), and radio frequency identification (RFID) [5]. The collected data is shared and stored across the cloud for analysis and then analyzed information is further used for obtaining meaningful data for rapid decision-making purposes [6-8]. The Internet of Things (IoT) can be evaluated and used as an essential technology in health management systems (e.g., mental health and global pandemic (COVID19)) as the drive to make healthcare more individualized, proactive, and cost-effective [9].

The increasing number of cases has triggered several measures to limit the pandemic, as scientists are working to develop vaccines and technologically sophisticated means to control its transmission. As a result, numerous apps such as Helathcode, Covidsafe, Coronawarn app, Aarogya setu, and NHS have been developed to minimize the possibility of transmitting SARS- CoV-2 after releasing lockdown precautions [10]. The possible transmission channels of a virus in the public can be investigated via contact tracing to isolate and aid individuals who may have come into touch with others who have COVID-19 infection [10]. By installing an app that tracks interactions with sick people and gives information on how to avoid infection, citizens can help limit the spread of COVID-19. Many governments have considered incorporating this type of tracing tool in their plans [10]. The focus of research has been on contact tracing and symptom tracking systems and the link between app usage and the virus epidemiological spread.

Various sorts of contact-tracing applications are being developed across the world, and many developed countries have already deployed (e.g., Singapore [11], Germany [12]). The willingness of users to utilize the app is important to the effectiveness of app-based contact tracking. According to Hinch et.al. [13] pandemic simulation data in the United Kingdom, the app decreases infections at all levels. For example, because the app would need to track user's interactions with others, privacy issues might impasse uptake and support [14].

However, information sharing is a problem while executing contact tracing apps in a country and this privacy and security threat becomes harmful while scaling it in a global context. Seeking the importance of security and privacy threats, this study explores the top contact tracing apps, their impact on controlling the spread of Covid-19, and the main security and privacy concerns that it offers. Furthermore, we purpose a secure contacting tracing app globally. This study presents an initial idea for scaling secure contact tracing apps in the global context.

2 BACKGROUND AND MOTIVATION

The global outbreak of the pandemic has led to a public health emergency that devasted the economy of several countries [1, 35]. The virus outbreak has changed people's lives all over the world, governments levy lockdowns, recommend self-isolation, obligate social distancing, and deploy emergency health responses. Furthermore, a COVID-19 carrier might be infectious even if no symptoms are present. As a result, by the time the carrier tests positive, the virus has likely spread to many others who have come into contact with them. This demands a method known as 'contact tracing,' which identifies persons who had intimate touch with the positive carrier and may now be infected themselves.

Medical Internet of Things (m-IoT) or smart healthcare system is a network of objects like sensors and actuators that converse with each other in a diverse network with or without the assistance of a computer. The rise in these smart devices is predicted to reach 2.1 trillion by the end of 2025 [15]. The use of the IoT in the pandemic has shown remarkable results in controlling its spread. Governments and researchers are looking forward to a technological solution to control the rapid spread of pandemics by automating the contact tracing process. Contact tracing is considered a crucial control measure for covid-19 spread [4]. Apart from contact tracing, several other recommendations include isolation, immediate diagnosis, and rigorous care of the infected carrier [5]. The infected person is advised to keep himself in quarantine, and contact is traced to control its spread known as contact tracing. However, contact tracing can be successful if the efforts by the community, health workers, and researchers are made.

Digital contact tracing apps store the data of infected individuals who came in contact with others and store it in their memory. However, the research identifies that in several circumstances infected person does not remember close contact or does not know the contacted person [16]. Contact tracing applications based on technology can help to simplify and automate the procedure, allowing contact tracers to alert users of a COVID-19 victim's contact information. The digital contact tracing app can work using Wireless Fidelity (Wi-Fi) or global positioning system (GPS) and other technologies [17].

However, these contact tracing apps are prone to several privacy and security threats as these apps trace the location of the infected person [18]. There is a great need to protect against health data loss and unauthorized access when implementing emerging technologies in tackling Covid-19. Most COVID-19 contact tracing apps such as *TraceTogether, COVIDSafe, and BeAware App* support concurrent access to health data and remote motoring of COVID-19 infected people and suspects in self-isolation (or in isolation centers), which poses serious security threats to public health data [18]. Similarly, tracking COVID-19 patients and contact persons' activities could entail a breach of their privacy.

The ultimate objective of this research study is to analyze the top contact tracing apps considering their security and privacy vulnerabilities. We further aim to propose a preliminary idea to develop a secure global contact tracing app.

3 RESEARCH METHODOLOGY

The ultimate objective of this research work is to develop a secure global contract tracing app. This is an initial study conducted considering the evidence from multivocal literature studies to achieve the mentioned objective [32, 33]. The complete MLR [19, 26, 27] study process followed in this study is given in Figure 1

3.1 Study selection criteria

A multivocal literature review is a form of systematic literature review comprised of peer-reviewed and grey literature (i.e., blogs, white papers) studies. The literature studies are extracted from the available scientific database and digital libraries. The search string is developed to search the available literature studies that specifically covered the research aims of this study. The search string is developed by the notion of the contact tracing app and its list of synonyms. The search keywords are linked using OR and, AND operators. We used the following search string for this study as reported in other studies [20-21].

("Contact tracing app" OR "digital contact tracing" OR "close contacts" OR "exposure notification" OR "digital contacts" OR "blockchain-based contact tracing" OR "blockchain-based digital contacts") AND ("security and privacy" OR "trust" OR "legal use") AND ("Benefits" OR "Success" OR "Advantages").

The search string was applied to the title, abstract, and keywords of the papers available in the scientific databases and digital libraries. The selected digital databases include ScienceDirect, SpringerLink, ScienceDirect, JSTOR, Scopus, JSTOR, IEEE Xplore, and ACM Digital Library and the grey literature (i.e., white papers and blogs). We supplemented automatic search with backward and forward snowballing manual search using the Google Scholar search engine to ensure a comprehensive sample of studies. A total of 48 studies were found based on the search string. All the available studies were further reviewed based on the inclusion and exclusion criteria. The inclusion criterion was applied to study the title, abstract, and keywords that meet the primary objective of this research study. We further excluded the irrelevant studies by considering the exclusion criteria. The exclusion criteria assist us in excluding the papers which do not cover the core theme of this study. The inclusion and exclusion criteria are described as:

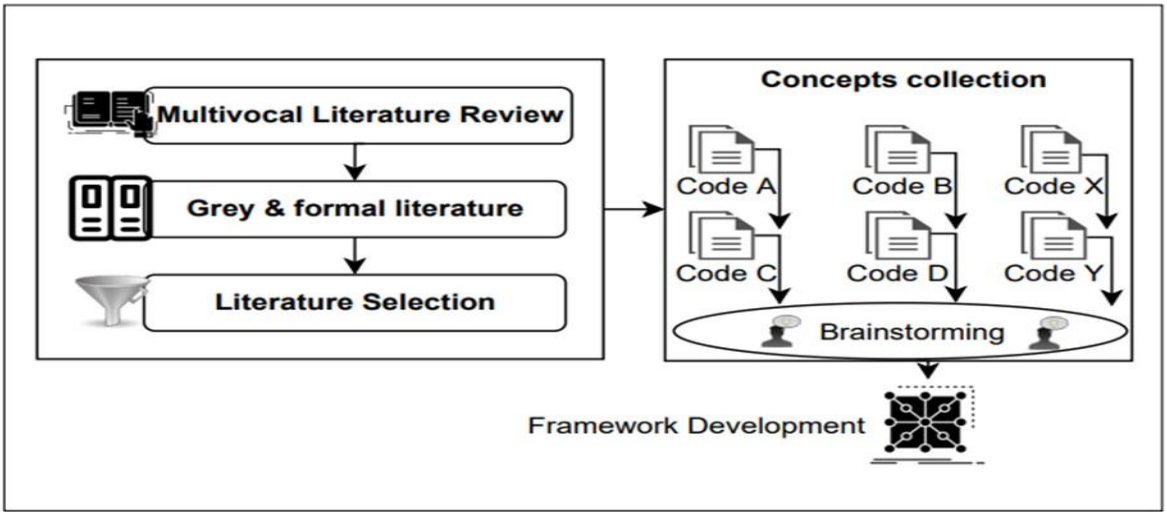

Figure 1: Steps used in MLR

3.1.1 Inclusion criteria: The following criteria were utilized to decide which type of literature (article, technical reports, etc.) was searched by the search strings [22-23].

- The study's full text is available.
- Every paper should be in a journal, conference, or book chapter.
- Papers that define Covid-19 contact tracing apps and their significance during a pandemic.
- Papers that define contact tracing apps' security and privacy concerns.
- Studies that are published between (January 2020 and February 2022).
- Research goals and approaches are clearly defined.
- Papers should be in English.

3.1.2 Exclusion criteria: To exclude the irrelevant studies from the total selected literature, the following criteria will be used [24-25].

- Papers that are not related to the research objective.
- Papers that do not discuss contact tracing apps and their security and privacy concerns.
- In the case of duplicate papers, the most complete version was published.
- The exclude the irrelevant studies from the total selected literature

We followed a similar approach to collect "grey" literature in the second step. We repeated the same search query using the Google search engine instead of scientific databases and only considered the top 30 results. Each extracted literature was manually checked to decide the inclusion and exclusion according to prescribed criteria. The total number of items in the "grey" literary collection is, with content that meets the following criteria.

- Is publicly available (i.e., not behind a paywall/registration).
- Discuss certain aspects of the contact tracing app and its security and privacy concerns.
- Is a standalone material written under a real name or published under the organization's name?
- The material content is original.

We have finalized 23 studies from both formal and grey literature and are available at https://tinyurl.com/2eftxen3.

3.2 Data extraction

A multistage formal content analysis procedure was used to extract data for contact tracing applications, followed by further analysis and reporting [28].

We gathered the following data from both literature sources: Title, Author(s), Year of Publication, Type of Publication, Application, Country, and Key Findings. We also extracted bibliographic data: publication venue, research approach, research aim, and research questions for the grey literature studies. Company/project, analytical approach, and web Address are among the additional fields available for "grey" literature.

4 RESEARCH FINDINGS

This section focuses on the most effective contact tracing apps used in different countries that assist in the pandemic spread control. We further discussed the pros and cons of security and privacy vulnerabilities in these apps.

4.1 Five most effective contact tracing apps

4.1.1 Health code (China). China developed "health code" systems that allocated unique health codes to the citizens to indicate their risk of being exposed to COVID-19. The most commonly utilized health code systems are hosted on WeChat and Alipay, two major apps with billions of users worldwide. Health Code was inspired by a feature on Alibaba's DingTalk app, allowing companies to monitor their employees' health information. In early February 2020, the Hangzhou city government in Zhejiang collaborated with Alibaba to extend the Health Code function to its inhabitants, incorporating the Zhejiang province Health Code into Alipay. Users' WeChat and Alipay services are automatically updated with Health Code programs, making them unable to deactivate the function without abandoning the service. The health code further monitors the individual's health status and assigns color coding, i.e., red code for quarantine, yellow for self-isolation, and green code for the healthy person.

4.1.2 Security and privacy concerns. The health code app has shown significant results to reduce the spread of covid-19. However, according to reports, there is a lack of certainty about how the app works and what data it stores. Some people have complained about being unable to reverse erroneous "red" classifications and have questioned the government's dependence on the internet and monitoring. Furthermore, the user was monitored and tracked without the user's agreement. If such apps record the user's location history, the user's movements can be tracked as well. Apart from pinpointing the location, there is a slew of privacy concerns, including data breaches, data gathering, and a lack of transparency in the data flow.

4.1.3 Corona Warns app (Germany). When COVID-19 infections spread throughout the globe and the World Health Organization (WHO) declared the outbreak a pandemic in early 2020, German research institutes and government organizations began looking into the possibilities of exploiting mobile phone location data for contact tracing. After months of contentious debate, the German Corona-Warn-App became launched in the app stores of the two major mobile platforms on June 16, 2020. The app was downloaded over 14 million times in the first two weeks, with that number expected to climb to 24.2 million by mid-December 2020. The open protocol "Decentralized Privacy-Preserving Proximity Tracing" is used in the German app (DP-3T or DP3T). The German government app does not collect any location data because it is not required for the system to function. In addition, the software does not know the user's identity. Instead, for each user, the software creates a pseudonymized I.D. number. The software identifies other phones in your vicinity using the app and stores their I.Ds via Bluetooth. This data transmission is performed regularly to track how long the encounter lasted. A contact is saved after 15 minutes. There is a problem with the infrastructure that supports the Corona-Warn-App on Android and iOS.

4.1.4 Security and privacy concerns. The official German Corona-Warn-App (CWA) program for tracing contacts with patients with coronavirus infection has a significant vulnerability, according to experts at GitHub Security Labs (COVID- 19). Its vulnerability might allow an attacker to run arbitrary code from afar. Centralized Bluetooth with added location functionality has low privacy and security, while non-streaming GPS scored high in security and medium in privacy.

4.1.5 Aarogya setu (India). The National Informatics Centre designed the Aarogya Setu App, a COVID-19 (coronavirus) mobile tracking tool (NIC) . English, Tamil, Hindi, Telugu, Kannada, Malayalam, Punjabi, Bengali, Oriya, Gujarati, Marathi, and Assamese are among the 12 Indian languages supported by the app. If a user meets up with a COVID-positive person, the program will notify them via notification. The tracking is done via Bluetooth technology and location-based social graphs or GPS, which indicates the user's interactions with anyone who has tested positive for the coronavirus and alerts them. With GPS and Bluetooth sensors, it identifies and monitors the user's movement. It will also detect other nearby cellphones that have the app loaded and, using its database and algorithms; it will send out a notice if they encounter infected persons.

4.1.6 Security and privacy concerns. Bluetooth has always been subject to security attacks (such as sniffers), and the odds of replay assaults are very significant, resulting in erroneous information and public panic. Furthermore, it is impossible to disguise the hardware device coupled with Bluetooth technology, which might lead to the disclosure of user identification. Moreover, Bluetooth's proximity limit is set. Furthermore, numerous authorities suggested that data obtained by the Aarogya Setu app on millions of Indians might be subject to threats from unfriendly state and non-state actors, posing a national security risk.

4.1.7 NHS (UK). The United Kingdom government developed the NHS Covid-19 app as a tool to do conventional contact tracing, which involves alerting the contacts of someone who has been infected using technology. The contact tracing app for England and Wales, like many others, uses Bluetooth to locate nearby users. If a user comes into close contact with someone who has tested positive, they are notified and advised to separate themselves. However, when Covid instances are on the rise in the United Kingdom, this has been contentious for companies. During the epidemic's early stages, the app was marketed as a critical component of measures to relax England's lockdown restrictions. However, the administration has recently attempted to downplay its relevance.

4.1.8 Security and privacy concerns. The NHSX COVID-19 Track, and Trace app use a centralized database. However, this central database will contain anonymized records of those reporting symp- toms.

Privacy campaign groups have raised concerns that this centralized database model could be extended to monitor individuals' movements and contacts. It's also impossible to ignore the fact that a large database containing the general public's personal information will be a prime target for hackers with malicious intents. The centralized based database could be vulnerable Hackers to gaining access to highly sensitive personal information, including names, national IDs, health statuses, and location data of users.

Furthermore, In the presence of an untrusted TLS server, the registration process does not properly guarantee either the integrity of the authority public key or the privacy of the shared secrets established at registration. The result completely undermines the

core security goals of the protocol, including its privacy and its resistance to spoofing and manipulation. Similarly, the storing and transmitting of unencrypted interaction logs facilitates the recovery of installationsIDs without requiring access to the Authority Private Key. Long-lived BroadcastValues undermine BLE specified privacy protections and could reveal additional lifestyle attributes about a user who submits their data.

4.1.9 Covidsafe App (Australia). Australia launched the COVIDSafe app as a contact tracing tool. The smartphone software, which was created in collaboration between the Health Department and the Digital Transformation Agency, employed the same Bluetooth technology as Singapore's TraceTogether contact tracing tool. There is a registration step once people download it to their smartphone. Individual personal information is required for registration. According to reports, this personal information is subsequently sent from the registrants' phones to a "very secure information storage system housed in Australia," according to reports. Since the storage system is geo-locked, the data can't be taken out of Australia. The National COVIDSafe Data Store (Data Store) is a "database operated by or on behalf of the Commonwealth to store safe information".

4.1.10 Security and privacy concerns. The program does, however, include several security and privacy vulnerabilities. According to the empirical study, people have many concerns about security, privacy, and legal difficulties. Few people believe that their phone is too old to be updated.

5 SECURITY AND PRIVACY CONSIDERATIONS

Since the establishment of governments, contact tracing applications have been developed. Contact tracing applications employ either a centralized or decentralized technique to operate with the user's information. In most of the apps, users were monitored without their consent. The user's movements can be traced if such programs maintain track of the user's location history. Apart from locating the location, there are many privacy problems, including data breaches, data collection, and a lack of data flow transparency [18].

Users should not be forced to use these applications by the government under any circumstances. The use of such tracking apps should be optional. Furthermore, mobile apps or frameworks should destroy user records after a set time (often 14–21 days and no more than 30 days). The mechanism for collecting, utilizing, and storing data should be transparent to protect user privacy. The program should incorporate regulations, a clear data flow, databases, and open-source code for transparency.

Many programs take excessive and useless data from their users; for example, "Aarogya Setu" requests names, cellphone numbers, age, gender, occupation, and information about countries visited in the last 30 days. Furthermore, geolocation tracking is unneeded when using Bluetooth or other comparable wireless technologies. Furthermore, several privacy and security vulnerabilities exist in the cloud computing system. Before trusting a third party, users should ask about seven safety considerations: privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, and long-term sustainability. Cloud Security Alliance (CSA) discovered many security concerns in Covid tracking apps in several cloud domains and issued security advice.

6 SECURITY ATTACKS ON CONTACT TRACING APPS

The contact tracing apps are more vulnerable to several security and privacy threats as described.

Bluesnarfing: can steal confidential information, i.e., pictures, emails, videos, and calendars.

Playback or replay attacks: halt data transmission or mali- ciously repeat the data frequently.

Denial of service (DoS): is another attack that uses all the system's resources by sending multiple requests eventually slowing down the system or dead. Similarly, an attacker can estimate the number of users infected with Covid-19 who have consented to submit their contact tracing data to the Centralized architecture using enumeration.

Other types of attacks include blue gagging, proximity app, resource drain, jamming, resource drain, reply, resource drain proximity app, spoofing, backend imprisonment, ransom, false injection, and jamming.

7 BEST PRACTICES

We have identified the following best practices from the state-of-the-art literature.

- Applications should be cautious and transparent about how users' private data will be stored and utilized.
- Various COVID-19 apps should be consolidated, in order to cut down on the number of necessary apps that users have to download.
- Apps should be developed before, and not after, disease outbreaks occur (for future preparedness).
- Apps should take into account regional differences. Applications servicing rural areas may need to work differently from applications servicing urban areas.
- Steps should be taken to minimize the number of times users have to interact with these applications on a daily basis.
- Apps should be made easy to use and accessible to people who do not have much prior experience using mobile applications. Government agencies and community committees should allocate resources toward teaching citizens how to effectively use these apps.

8 IMPORTANCE OF CONTACT TRACING APP AT THE GLOBAL LEVEL

Contact tracing can reduce viral transmission by quickly identifying, isolating, and treating patients and enabling assisted quarantine of contacts. Contact tracing app has shown a significant impact in controlling the spread of Covid-19. The architecture of the contact tracing apps is different in different countries. Germany implemented a contact tracing app using smartwatches that monitor the temperature, pulse, and sleep pattern. Similarly, patients who have tested positive for COVID-19 and have elected to get treatment at home are tracked using mobile network operators and GPS coordinates in Moscow's patient-tracking app.

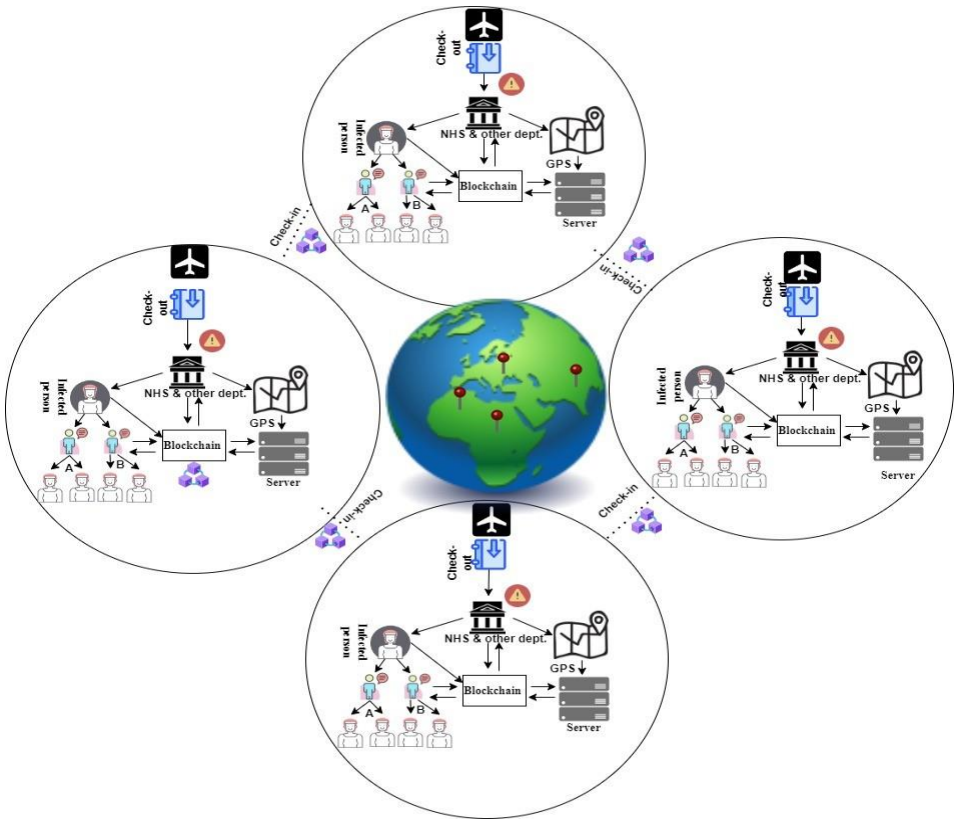

Figure 2: proposed structure of secure global contact tracing app

8.1 Proposed global contact tracing app

However, no app work globally for controlling the spread of covid-19. It has been noticed that individuals with fake covid negative reports are traveling to other countries [29]. The spread of new variants could be increased if controlled at the global level and managed manually. Thus, a more generic and effective global contact tracing app is needed. The single globally recognized app could be used for domestic and for international purposes. The initial framework is presented in Figure 2. The global contact tracing app will follow the following scenarios:

- The national health department will be able to know the covid history of a traveler through airport control authority when entered.
- The airport control authority would know the covid and contact tracing the history of travelers.
- The traveler could know the situation when arriving in another country i.e., who is the infected and with whom he has contacted.
- The data of travelers could easily be synced with other countries.

The global contact tracing app would significantly limit the spread of covid-19 and also possible new variants.

8.2 Security concerns

Besides the significant advantage of global contact tracing, the disclosure of privacy and data security is one of the main concerns. Traditionally, to address security and privacy concerns, cryptographic approaches are used. In the current era, blockchain is one of the key tools to manage data security and privacy-related issues [30-31]. The proposed global contact tracing app is fundamentally based on a blockchain-based distributed network.

The privacy and security of users' personal information are some of the impediments raised by digital contact tracking applications. It is crucial to preserve the confidentiality of individual identity when the data is collected from different sources and broadcast to the network. In most apps, users are asked for their approval, which gives them some control over their data. Furthermore, there is a lake of verification of the information shared in the network for contact tracing purposes. The blockchain has introduced several benefits. The distributed peer-to-peer connectivity of network nodes that bridges the gap between users and app management is supported

by blockchain technology, which can play a vital role in contact tracing. The technological capabilities of blockchain enable people to share information while maintaining their anonymity.

9 IMPLICATIONS

This is an initial study of contact tracing across borders. The objective of this study is to make a secure global health care system with the usage of blockchain technology. This study has implications for both the research community and industry practices. The research community can consider this idea and contribute to making this proposed idea more flexible and adoptable by suggesting different tools, techniques, and technologies. The practitioners also need to adopt this proposed idea in a real-world environment and contribute to making an effective and secure global contact tracing system by applying blackchin technology.

10 CONCLUSION AND FUTURE WORK

The surge in the covid-19 cases the breakdown the normal life and devastated the economy of several countries. Various measures have been proposed, including social distancing, frequent hand washing, and contact tracing to control the spread of the pandemic. The use of technology such as digital contact tracing methods has helped in controlling the spread of the pandemic. The contact tracing app assists in identifying the person who has been in contact with the infected people. This app works by sharing personal information with the national healthcare department and others, leading to security and privacy concerns. This research study analyzes the most used contact tracing app, their influence on controlling the spread of the pandemic, and key security and privacy vulnerabilities that exist in the apps. The multivocal literature review (MLR) approach was used to extract the data from formal literature and grey literature, and a total of 23 studies were identified that meet the objective of this research study. We have analyzed the five most used contact tracing apps as health code (China), Corona warns (Germany), Aarogya setu (India), NHS (UK), and Covidsafe (Australia) from the existing state-of-the-art literature. Several countries have implemented their own contact tracing app. However, there is no single contact tracing app that works globally. We have proposed an initial idea for developing a secure generic global contact tracing app using blockchain technology.

The global contact tracing app would offer several security and privacy vulnerabilities as data of individuals is being shared with different departments of other countries. Therefore, blockchain is one of the key tools to manage data security and privacy-related issues. The proposed global contact tracing app is fundamentally based on a blockchain-based distributed network. We would expand our idea to its real implementation for controlling pandemics in the future.

REFERENCES

[1] Priya, S. Shanmuga, Erdem Cuce, and K. Sudhakar. "A perspective of COVID 19 impact on global economy, energy and environment." International Journal of Sustainable Engineering 14.6 (2021): 1290-1305.

[2] GÜNER, HATİCE RAHMET, İmran Hasanoğlu, and Firdevs Aktaş. "COVID-19: Prevention and control measures in community." Turkish Journal of medical sciences 50.SI-1 (2020): 571-577.

[3] Kleinman, Robert A., and Colin Merkel. "Digital contact tracing for COVID-19." CMAJ 192.24 (2020): E653-E656.

[4] Lo, Bernard, and Ida Sim. "Ethical framework for assessing manual and digital contact tracing for COVID-19." Annals of Internal Medicine 174.3 (2021): 395-400.

[5] Landaluce, Hugo, *et al.* "A review of IoT sensing applications and challenges using RFID and wireless sensor networks." Sensors 20.9 (2020): 2495.

[6] Jahmunah, Vicnesh, *et al.* "Future IoT tools for COVID-19 contact tracing and prediction: A review of the state-of-the-science." International journal of imaging systems and technology 31.2 (2021): 455-471.

[7] Hu, Peng. "IoT-based contact tracing systems for infectious diseases: Architecture and analysis." GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, 2020.

[8] Tedeschi, Pietro, Spiridon Bakiras, and Roberto Di Pietro. "IoTrace: a flexible, efficient, and privacy-preserving IoT-enabled architecture for contact tracing." IEEE Communications Magazine 59.6 (2021): 82-88.

[9] Darshan, K. R., and K. R. Anandakumar. "A comprehensive review on usage of Internet of Things (IoT) in healthcare system." 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT). IEEE, 2015.

[10] Ahmed, Nadeem, *et al.* "A survey of COVID-19 contact tracing apps." IEEE access 8 (2020): 134577-134601.

[11] Huang, Zhilian, *et al.* "Performance of digital contact tracing tools for COVID-19 response in Singapore: cross-sectional study." JMIR mHealth and uHealth 8.10 (2020): e23148.

[12] Amann, Julia, Joanna Sleigh, and Effy Vayena. "Digital contact-tracing during the Covid-19 pandemic: an analysis of newspaper coverage in Germany, Austria, and Switzerland." Plos one 16.2 (2021): e0246524.

[13] Hinch, Robert, *et al.* "Effective configurations of a digital contact tracing app: a report to NHSX." Retrieved July 23 (2020): 2020.

[14] Chan, Eugene Y., and Najam U. Saqib. "Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high." Computers in Human Behavior 119 (2021): 106718.

[15] Singh, Pawan. "Internet of things based health monitoring system: opportunities and challenges." International Journal of Advanced Research in Computer Science 9.1 (2018): 224-228.

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

[17] Mbunge, Elliot. "Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls." Diabetes & Metabolic Syndrome: Clinical Research & Reviews 14.6 (2020): 1631-1636.

[18] Hatamian, Majid, *et al.* "A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps." Empirical software engineering 26.3 (2021): 1-51.

[19] Ogawa, R.T. and B. Malen, Towards rigor in reviews of multivocal literatures: Applying the exploratory case study method. Review of educational research, 1991. 61(3): p. 265-286.

[20] Akbar, Muhammad Azeem, *et al.* "A Multicriteria Decision Making Taxonomy of IOT Security Challenging Factors." IEEE Access 9 (2021): 128841-128861.

[21] Hamza, Muhammad, *et al.* "Decision-Making Framework of Requirement Engineering Barriers in the Domain of Global Healthcare Information Systems." Mathematical Problems in Engineering 2022 (2022).

[22] Akbar, Muhammad Azeem, *et al.* "Toward successful DevSecOps in software development organizations: A decision-making framework." Information and Software Technology 147 (2022): 106894.

[23] Hamza, Muhammad, *et al.* "SIOT-RIMM: Towards secure IOT-requirement imple- mentation maturity model." Proceedings of the Evaluation and Assessment in Software Engineering. 2020. 463-468.

[24] Akbar, Muhammad Azeem, *et al.* "Prioritization-based taxonomy of global software development challenges: a FAHP based analysis." IEEE Access 9 (2021): 37961-37974.

[25] Akbar, Muhammad Azeem, *et al.* "A fuzzy analytical hierarchy process to prioritize the success factors of requirement change management in global software development." Journal of Software: Evolution and Process 33.2 (2021): e2292.

[26] Akbar, Muhammad Azeem, *et al.* "Barriers of managing cloud outsource software development projects: a multivocal study." Multimedia Tools and Applications (2021): 1-24.

[27] Hamza, Muhammad, *et al.* "Identification of Privacy and Security Risks of Internet of Things: An Empirical Investigation." Review of Computer Engineering Research 6.1 (2019): 35-44.

[28] Akbar, Muhammad Azeem, *et al.* "Requirements change management challenges of global software development: An empirical investigation." IEEE Access 8 (2020): 203070-203085.

[29] India, T.T.o., Lab issuing fake Covid reports raided in Gurugram. 2022.

[30] Akbar, Muhammad Azeem, *et al.* "Towards efficient and secure global software development using blockchain." Proceedings of the Evaluation and Assessment in Software Engineering. 2020. 493-498.

[31] Taiyaba, Ms, *et al.* "Secure V2X Environment using Blockchain Technology." Proceedings of the Evaluation and Assessment in Software Engineering. 2020. 469-474.

[32] Akbar, Muhammad Azeem, *et al.* "Success factors influencing requirements change management process in global software development." Journal of Computer Languages 51 (2019): 112-130.
[33] Akbar, Muhammad Azeem, *et al.* "A multivocal study to improve the implementation of global requirements change management process: A client-vendor prospective." Journal of Software: Evolution and Process 32.8 (2020): e2252.
[34] Riaz, Muhammad Tanveer, *et al.* "A wireless controlled intelligent healthcare system for diplegia patients." Mathematical Biosciences and Engineering 19.1 (2022): 456-472.
[35] Sang, Jun, *et al.* "Joint image compression and encryption using IWT with SPIHT, Kd-tree and chaotic maps." Applied Sciences 8.10 (2018): 1963.