Analysis of Data's Privacy and Anonymity Aspects of Contact Tracing Apps via Smartphones – A Use Case of COVID-19

Haritha Akkineni[1,*], Madhu Bala Myneni[2], Budi Padmaja[3], Ananda Ravuri[4], CH. V. K. N. S. N. Moorthy[5] and Raviteja CMS[6]

[1]*PVP Siddhartha Institute of Technology, Vijayawada, India*
[2]*VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India*
[3]*Institute of Aeronautical Engineering, Hyderabad, India*
[4]*Software Engineer, Intel Corporation, USA*
[5]*Vasavi College of Engineering, Hyderabad, India*
[6]*Dreamplug Technologies Pvt Ltd, Bangalore*
E-mail: aharithapvpsit@gmail.com; baladandamudi@gmail.com; b.padmaja@gmail.com; ananda.ravuri@intel.com; krishna.turbo@gmail.com; hello@rtcms.dev
[*]*Corresponding Author*

Received 22 February 2023; Accepted 01 July 2023;
Publication 11 August 2023

Abstract

Privacy and anonymity aspects are playing a vital role in accessing smartphone apps. This is more evident in unexpected epidemic situations like COVID-19 while working with contact tracing apps. A human connectivity model is essential to analyse the widespread cases of viruses and vaccination patterns during the timeframe of March 2020 to May 2021. Smartphone apps that are supported by technologies like IoT and blockchain have already proven effective in tracing the Ebola epidemic. Thus, this technology, coupled with privacy-preserving features, would help to discover clusters with infectious contacts and alert the respective authorities. Besides, this can also allow us to understand the human connectivity model and the effectiveness of vaccines, which can aid in developing a plan of action for future epidemics.

Journal of Mobile Multimedia, Vol. 19_5, 1255–1276.
doi: 10.13052/jmm1550-4646.1956

Hence, this article focuses on the analysis of data collected from contact tracing apps and a number of affected cases. It includes a study on early solutions with existing technologies, an overview and analysis of existing COVID-19 apps with vulnerabilities, proposed solutions, and data analysis on privacy and anonymity aspects of smartphone apps using the ARIMA model. It is evaluated by correlating it with the usage of contact tracing apps. The results assured a positive correlation between the number of downloads and the number of cases. This infers that even though the Indian government released these contact tracing apps, it all depends on the citizens to utilise them to their fullest. As a policy suggestion, it is stated that regardless of the prevalence of contact tracing apps, people must follow the rules and regulations suggested by the local health authorities and maintain social distancing in public places.

Keywords: ArogyaSetu, ARIMA model, contact tracing, machine learning, RFID tags, smartphone apps, time series prediction.

1 Introduction

In December 2019, China experienced the spread of an unknown virus popularly known as COVID-19. In the early 2020s, the exact measures and precautions to stop the spread of the virus were still novel, which caused it to spread rapidly to other countries. As of March 14, 2021, 186 countries, territories, and areas had shared detailed data with the World Health Organization (WHO) about the situation of this virus, as depicted in Figure 1 [1]. Various technological innovations took place and led to the creation of new technology for efficient tracing and reducing its spread. According to the report published by WHO [1], COVID-19 confirmed cases continued to rise for a fourth consecutive week, with just under 3.3 million new cases reported in mid-March 2021. Despite the development of vaccines and effective tracing methods, COVID-19 cases continued to rise in India, particularly in Maharashtra, for a variety of reasons. The new stain of COVID-19 was not taken into consideration while tracing the infection.

As the number of technological developments rose, the privacy associated with such a massive amount of data played a vital role. Thus, according to William [3], the questions considered for defining the characteristics of a contact tracing app are as follows: The nature of the database; centralization versus distribution; the method of data collection, peer-to-peer or Bluetooth-based; the anonymity of the data; the open-sourced nature of the application The open-source nature of the application itself cannot determine its safety.

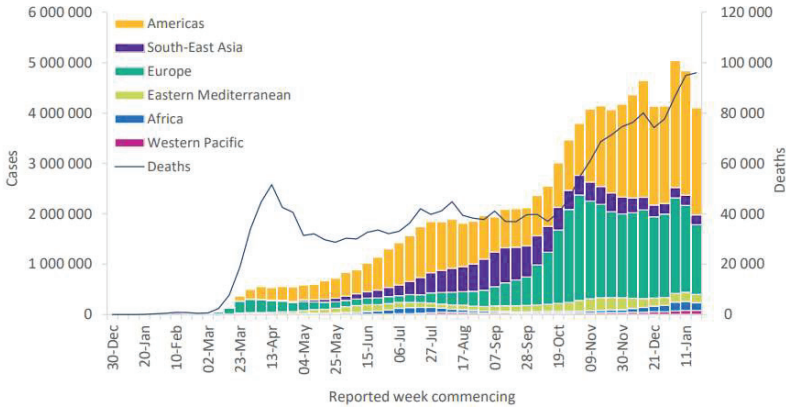

Figure 1 Weekly status of COVID-19 cases by WHO region, and global deaths, as of 21 March 2021 [1].

Apps like ArogryaSetu are open-sourced but not actively maintained (from the Github repo released to the public [4]). Thus, the actual app might be completely different from the open-sourced version. But according to AarogyaSetup's Privacy Policy [5], they collect some sensitive information like age, sex, profession, and mobile number for tracing and generating a unique DDID. As the number of technological developments rose, the privacy associated with such a massive amount of data played a vital role. Thus, according to William [3], the questions considered for defining the characteristics of a contact tracing app are as follows: The nature of the database; centralization versus distribution; the method of data collection, peer-to-peer or Bluetooth-based; the anonymity of the data; the open-sourced nature of the application The open-source nature of the application itself cannot determine its safety. Apps like ArogryaSetu are open-sourced but not actively maintained (from the Github repo released to the public [4]). Thus, the actual app might be completely different from the open-sourced version. But according to AarogyaSetup's Privacy Policy [5], they collect some sensitive information like age, sex, profession, and mobile number for tracing and generating a unique DDID. As the number of technological developments rose, the privacy associated with such a massive amount of data played a vital role. Thus, according to William [3], the questions considered for defining the characteristics of a contact tracing app are as follows: The nature of the database; centralization versus distribution; the method of data collection, peer-to-peer or Bluetooth-based; the anonymity of the data; the open-sourced nature of the application The open-source nature of the application itself

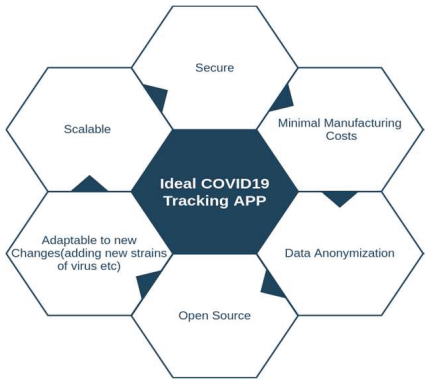

Figure 2 Ideal features for a COVID-19 tracing application.

cannot determine its safety. Apps like ArogryaSetu are open-sourced but not actively maintained (from the Github repo released to the public [4]). Thus, the actual app might be completely different from the open-sourced version. But according to the AarogyaSetu app's Privacy Policy [5], they collect some sensitive information like age, sex, profession, and mobile number for tracing and generating a unique DDID. The ideal features of the COVID-19 tracing app are given in Figure 2.

This paper analyses the existing solutions, including the IoT-based ones, and further understands the importance of smartphone-based COVID-19 tracing apps in terms of privacy and user safety measures. Further, it is extended with a major focus on the human connectivity model by taking data from crowd-sourced data sets and analysing the efficiency of the smartphone-based tracing app in terms of actual success. The rapid epidemic changes are noted from various sources.

Early solutions with existing technologies are discussed in Section 2. An overview and analysis of existing COVID-19 apps with vulnerabilities are discussed in Section 3. Proposed solutions and data analysis on privacy and anonymity aspects of smartphone apps using the ARIMA model are discussed in Section 4. The conclusion part goes in Section 5. The suggestions for further research are discussed in Section 6.

2 Backdrop of Solutions

In the early 2020s, there were many technological developments, and rapid prototyping took place. Initially, many existing technologies were used to

arrive at solutions. Various authors have studied this contact tracing problem to find a technological solution.

2.1 Lessons from Ebola Epidemic

Way back in 2014, the Ebola virus was spreading rapidly in countries like Liberia, Guinea, and Sierra Leone [6]. Thus, Lisa O. Danquah [6] proposed a technological proof-of-concept solution using smartphones to track this virus and mitigate it effectively. He inferred that the digitization of patient records proved the effectiveness of mobile health applications compared to paper-based infection tracing. This established the value of smartphone-based technology for tracking epidemics.

2.2 Contact Tracing Using Mobile Positioning

Mobile technology (GSM) is quite popular worldwide, which might be a prominent solution to tracking people. Many countries, including developed nations such as Israel [7], began to use this technology. Cecilia Panigutti [9] performed an extensive study on how CDR (Call Detail Record) can be used for one's own end. This data can be used to represent the commute links originating from or arriving at the most connected locations, which represent the busiest and most populated, as demonstrated by the correlation between node loyalty and its degree of traffic [9]. IniobongEkong [8] stated that even though the CDR data is very private, it follows the National Data Protection Regulation (NDPR) rules of Nigeria, promulgated in 2019. further concluded that the personal data must be handled safely and anonymized before analysis. There should be strict rules and regulations in place regarding the data handling procedures. Contact tracing using mobile positioning might be an instant technological solution, but it cannot be relied on for a long time due to various privacy factors and risks. According to the WHO, the contact definition for the COVID-19 virus is two metres [10]. Achieving high accuracy using this technology is not feasible. The above solutions didn't consider privacy an essential factor since they quickly solved the contact tracing problem. IniobongEkong [8] concludes by stating that more research is needed to efficiently anonymize and process this data. A long-term solution, considering privacy and the anonymization of data, is needed. The data collected from these apps might not be disposed of for a long period of time, which could create legitimate privacy concerns. Elkhodr et al. [30] reported after evaluating 30,000 reviews from 13 apps that the acceptance rate of these apps ranged from 5% to 30%. So people started trusting these apps.

2.3 Other Technological Proposed Solutions

There were many solutions based on different technologies, not limited to IoT and artificial intelligence. Still, these solutions have to be scalable to the whole population and consider privacy. Many well-known organizations like the Allen Institute of Artificial Intelligence have publicly shared COVID-19 resources [13] for study and research, consisting of many articles and full-text journals. Generally, artificial intelligence and machine learning have shown some proven results in medicine and research. Therefore, advanced technology like AI and ML can be used to forecast and track the epidemic. Lalit [11] discusses the issues faced by existing technologies and proposed a solution, shown in Figure 3, which takes advantage of both smartphone apps and IoT coupled with Blockchain. The proposed architecture includes a DApp, also known as a "distributed application," in which the user or health system provider interacts with the application. Behind the scenes, the model connects to the Distributed Ledger, which takes advantage of blockchain at its core. As a result, the frontend DApp is designed in an adhoc phone-to-phone mesh network topology [11], with each phone connected to another via communication channels such as WiFi or Bluetooth. Further, to identify the exact movement of the people, they have also used RFID tags to uniquely identify vehicles at toll gates to track the location.

The Solidity smart contracts are used to perform operations like user registration. Whenever a new individual is registered, both public and private keys are generated, maintaining the individual's privacy. Various operations are carried out to sync the RFID chips with their unique identifier. This whole mode was simulated and run to generate results, costs, including the gas (for

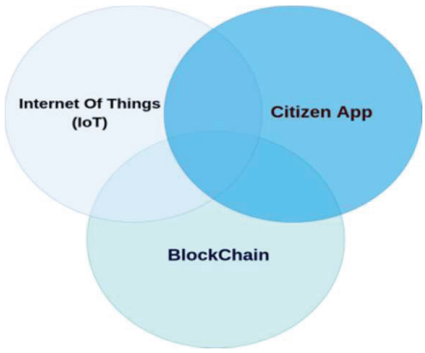

Figure 3 Diagrammatic representation of model proposed by LalitGarg [11].

making transactions on an Ethereum network), were calculated. The benign properties like decentralization, anonymity and traceability properties of blockchain using combined technique of non-interactive zero-knowledge proof and multi-signature with public key aggregation to achieve a privacy preserving model for contact tracing scenarios at a low cost [38].

2.4 Privacy Factors

The prominent works noted the privacy concerns of the CDR system. Their proposed model is more privacy-friendly since the app uses no sensitive information. Further, this model takes advantage of blockchain via smart contracts, making it censorship-resistant [11]. As the author states, "Blockchain is often an append-only ledger that is difficult to modify under normal conditions" [11], making it a challenging task to track the new strain of the COVID-19 virus, which was first discovered in December 2020 [14]. Furthermore, when compared to other variants, this new strain is found to be more dangerous and capable of spreading quickly and easily [14], making it an important factor in contact tracing. This model uses RFID chips to track objects. Manufacturing RFID tags during the lockdown situations is a big challenge. Hence, this model was less effective in practice. The author states that the "system stores data on a blockchain log, but at an average cost of $0.34 per log" [11], thus overall development and scalability of the model is a costly affair. SM Abu [12] analysed an IoT-based drug delivery platform that automatically places orders based on order history. It was stated that the SEIRS (Susceptible–Exposed–Infectious–Recovered–Susceptible) model, introduced as the result of research on the plague in the early 20th century. The authors used Artificial Intelligence Technology and derived at an extensive summary of results. Further, he outlines various techniques and technologies implemented by countries worldwide using IoT while preserving an individual's privacy. The conclusions of previous works and risks associated with IoT and AI technology are as follows: AI can be biased if erroneous data is fed into it, giving negative results that might have a destructive impact on decision-making. Technologies like GAN, which can create images using artificial intelligence, can be misused to develop fake CT scans and mislead the models. The authors in [32] developed a research model based on the unified theory of acceptance and use of technology (UTAUT), health belief model (HBM), focusing on privacy and security risks in the adoption of contact tracing apps. The authors in [33] focused on the multiple adoption considerations of the contact tracing apps. Major

parameters included the app's functionality, risks in data collection and privacy. The authors in [34] stated users experiences using New Zealand's contact tracing app. Supporting collective health has been the key motivator for the installation. The privacy features could be improved and the manually process of QR scanning could be replaced by autonomous collection of user location data. IoT devices are more vulnerable to severe attacks [15], making them a high risk in the whole infection tracing model. Moreover, a health data breach might have the worst impact since all personal data will leak online. As a result, it can be concluded that artificial intelligence and IoT technology should be carefully engineered, with privacy and security in mind, before being tested on a large scale to provide a more sustainable solution. More research is needed on effectively implementing decentralisation technologies like blockchain to enhance an individual's privacy in contact tracing.

The authors in this study proposed and validated an integrated a-b-c (Antecedent, behaviour, and consequence) and technology acceptance model of deploying the contract tracing app in four European countries. A quantitative approach was adopted achieving a positive outcome with citizens of the app was only 17.1% and negative consequent was 54.3% [36].

Authors researched on the individual's moral perspective on using Corona Warning App. They investigated on the reasons behind the gain of this app and how it can be promoted. They found a strong influence of moral intensity on app download [37].

2.5 Mobile Based COVID-19 Tracing Applications

Today's mobiles are equipped with many sensors, including but not limited to Bluetooth, proximity sensors, and other sensors like an accelerometer, GPS with high precision, and a camera. These sensors can be used to navigate a citizen's movement and efficiently track the spread of the COVID-19 virus.

2.5.1 Basic overview

Figure 4 depicts smart phone device contact tracing. Many smart phone apps ask for explicit permission to use their on-device sensors during the installation process. Let us assume that two people exist: Alice and Bob. A unique ID is generated for both Alice and Bob whenever they come into contact. If any one of them is infected with COVID-19, then the match takes place in an anonymous fashion, and the other person will be alerted that they have been in contact with the infected person. This tracing of an individual is done via GPRS, Bluetooth, or proximity-based technologies.

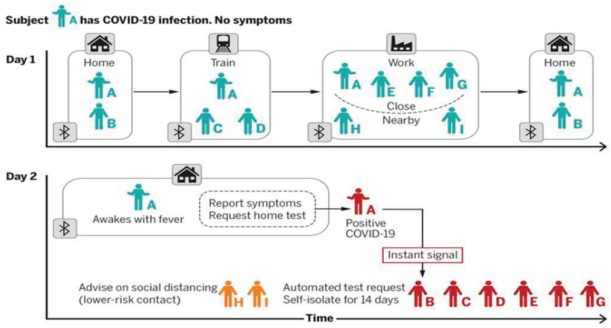

Figure 4 Basic overview of how contact tracing via smartphones works from Muhammad [16].

Table 1 Summary of methods

Contact Tracing Approaches					
Authors	Broadcasting	Selective Broadcasting	Unicasting	Participatory Sharing	Private Kit
Ramesh [19]	✓	✓			✓
Shahroz [18]			✓	✓	
Y. Bengio [35]	✓			✓	

2.5.2 Methods of contact tracing

Different methods to support contact tracing approach are presented in Table 1.

Broadcasting: A central authority would share locations that diagnosed carriers have visited within the timeframe of the contagion. Maps and text messages were used by some governments to alert citizens. The authors in [35] proposed a decentralized architecture that captures less personally identifiable information. Citizens with privacy concerns prefer a hybrid or decentralized model. The leak of PII would be a major concern.

Selective Broadcasting: The specific groups or target audiences are shared with the locations that diagnosed carriers have visited within the time frame of the contagion. The privacy component of the process is at stake, as personal information like mobile numbers and user sign-ups are essential.

Unicasting: This only alerts people who were in close contact with a diagnosed infection carrier. According to Shahroz [18], this method requires information about every citizen who crosses paths with each other and is usually ineffective in terms of privacy.

Participatory Sharing: This is a method by which users voluntarily submit their information. Still, there is a breach of privacy and trust if any central authority, like the government, is involved. This method might also be prone to abuse by bad actors [18].

Private Kit: MIT designed this as a free and open-source project wherein the location data is encrypted and then sent to devices based on the requests. This method is safer since the information is only shared with the respective government authorities when identified as COVID-positive. Ramesh [19] thoroughly examined these methods and then tabulated the associated risks and challenges in their research based on various parameters, such as accuracy.

3 Overview and Analysis of Existing COVID19 Apps

Many countries have started developing apps for various platforms like Android, iOS, and the Web for contact tracing as early as March 2020. Further, many countries have released their apps while taking privacy and security into consideration. Despite this, this study was able to uncover some serious trackers within these COVID-19 contact tracing apps, which share data with third parties. Contact tracing apps available at the time of this research were analyzed, taken from the list of COVID-19 apps available at Wikipedia [20]. Also, there were many contact-tracing apps developed for a particular country. In such cases, we have eliminated them based on the following criteria:

- Apps that are not directly related to the government bodies of that country.
- Apps that aren't available publicly for analysis, for example China.

Many apps were developed in the USA, out of which the ones with the highest number of permissions and trackers were considered for analysis.

3.1 Analysis of Number of Trackers and Permissions

The advantage of the Exodus project [21] is that it allows one to determine the number of trackers and permissions requested by a specific contact tracing app. Exodus is an open-source framework that looks for embedded trackers and lists them. A "tracker" can be defined as software that collects data on the person using the app, how they are using it, or the smartphone they are using. Permission is a request for access to on-device sensors such as

the geolocation, contacts, files, microphone, vibrate function, camera, etc. According to the Exodus Project [21], some permissions are considered dangerous. But, for this research, we have considered the total number of permissions requested since many contact tracing apps require some sensitive permissions, like access to location, to function correctly and avoid false positives. From the research done by Muhammad [16], this study observes that the NHS App, developed for the United Kingdom with over 500,000+ installs, requests some sensitive permissions like microphone and device ID access, which are irrelevant for the process of contact tracing. The T DE OLHO app developed for Brazil has dangerous trackers like One Signal and requests a lot of permission, including dangerous ones like WRITE_SETTINGS, which may pose a privacy threat. Countries like China haven't published their apps used for contact tracing publicly for further analysis. But William [18] states that since the app is mandatory to be used by citizens, there might be a breach of privacy and security. In India, many contact-tracing apps exist, among them all the state-developed apps such as COVID Punjab by the Punjab government and GoK Direct by the government of Kerala. The AAROGYA SETU App, developed by the National Informatics Center, became popular. According to India Today [22], the AAROGYA SETU App is the most downloaded COVID-19 tracing app in the world. It uses GPRS and Bluetooth to track people and identify who has been in close contact with the infected person. Even though the app's source code is made public [4], there is no active development of the app in the public domain, and hence it can be considered a closed-sourced app. Nadeem [28], as a part of his research, studied various types of security attacks that might be possible by an attacker and found that the ArogyaSetu app was vulnerable to the following:

Replay/Relay Attack: An attacker can force malformed data to be fed into the system, thus inducing false positives.

Wireless Tracing: The ArogyaSetu app emits Bluetooth signals that an adversary like a shopping mall can take advantage of to track its customers' movements.

Location Confirmation: An attacker confirms the presence of a user in a particular location.

Enumeration: An attacker can enumerate and get the total count of users tested for COVID positivity.

DOS: An attacker can do things like upload malformed data to the server when a user is tested positive, making the server unusable for everyone.

According to the privacy policy [5], the app collects sensitive information like name, age, gender, phone number, address, and ID proof information. This app contains third-party trackers like Google Crash Analytics and Google Firebase Analytics, thus making the privacy and security of this app questionable. To break the chain of infections, the German Corona-Warning-App (CWA) was introduced. In the beginning, there were privacy concerns that prevented its use by many people. To increase the number of users of this app, a positive relation between CWA download and moral intensity must be derived from parameters like social norms about app use, the magnitude or seriousness of consequences, individual proximity to COVID-19 cases, and the probability of the app's positive effect [31].

4 Proposed Solution and Analysis

4.1 Apple and Google API's

Amidst this COVID-19 spread, Google Inc. and Apple Inc. have collaborated and announced [17] an API that takes advantage of Bluetooth technology. It is an opt-in-only feature, and anyone can voluntarily participate. We collect no location data from the users. William [18] describes this process as highly secure since it was later upgraded to work with AES keys for enhanced encryption. When two or more people get together within Bluetooth's proximity range, their unique IDs will be exchanged. They can self-report in the app that they are infected, and then all previous contacts with the infected person will be notified. This process ensures that privacy and anonymity are taken care of. Open-source apps like Patch Check take advantage of this exposure notification protocol developed by Apple and Google [17]. Naresh [25] performed an extensive study of the Autoregressive Integrated Moving Average (ARIMA) model and the Facebook Prophet model for time series forecasting of COVID-19 cases and reported the efficiency of ARIMA. Patch Check is thoroughly audited for the privacy threat model for COVID-19 by using various techniques like static and dynamic code analysis. All these documents can be found in their Github [27] repository. The advantages of the existing open-source project and ability to trace new coronavirus variants to better understand the spread of new dangerous variants such as 20C, 20J, and 20C/S:452R are specified in the WHO report [1]. As a result, we will be able to conduct further analysis and research into how the new variant is spreading, as well as track the number of people who have been vaccinated, in order to make better decisions.

4.2 Data Analysis on Privacy and Anonymity Aspects

The data collected for this work is taken from smartphone apps to analyse the data's privacy and anonymity aspects. But, due to privacy and integrity reasons, no such datasets are made available publicly. So the Google Mobility dataset [23], which contains data collected from mobile devices in a privacy-preserving manner, is chosen. But this has the limitation that it could only work in places like grocery stores, pharmacy stores, parks, transit stations, retail stores, and workplaces. To further analyse the actual impact of these contact tracing apps, a crowdsourced dataset is considered to predict the COVID-19 cases for a particular period in India. The effect of contact tracing apps on the number of cases is analysed. This work includes using another dataset, which is crowdsourced and maintained by COVID-19 India [24, 25]. These datasets provided by organisations like the ICMR are not constantly updated and thus do not provide the latest information. This information is derived from official announcements in state bulletins. Further, crowd-sourced datasets have a lower error rate as they are verified by volunteers before being pushed into the public domain. There are various datasets made available by COVID-19 India, but case_time_series is considered the best way to understand the number of COVID-19 cases over time. Further, the data having attributes such as Date of Reporting Date_YMD (date in YY-MM-DD format), Daily Confirmed (number of COVID-19 cases), and Total Confirmed (total number of cases confirmed until the given date) (cumulative of daily confirmed cases) are taken. Similarly, other fields like daily recovered, total recovered, daily deceased, and total deceased are also assessed.

For this analysis, Date_YMD and Total Confirmed attributes are considered. The ARIMA model to perform predictions for the next 30 days of COVID-19 cases in India is illustrated in Figure 5.

A comparative study of COVID-19 cases and the number of AROGYASETU app downloads is performed to better understand how the contact tracing apps were successful in practice.

The data was collected from sources using the Play Store's Web Archive [26] feature to find the number of downloads, and a graph is plotted as illustrated in Figure 6. The number of AROGYASETU app downloads (only from the Play Store) rose in April, and thus the COVID-19 infection rate was meager. Further, from May to November, even though the number of downloads of the app grew, the COVID-19 infection rate grew more rapidly. When the cases are more numerous, the number of downloads of the contact tracing apps also increases. This gives a basic understanding of the human

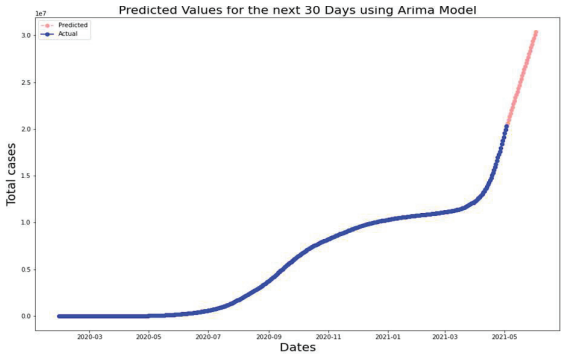

Figure 5 COVID-19 prediction model response using ARIMA model.

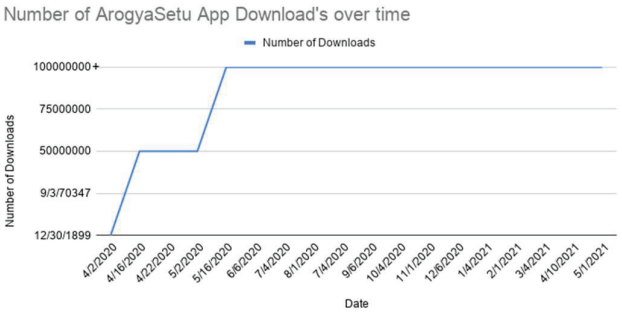

Figure 6 Plot of number of downloads for ArogyaSetu app over time.

connectivity model. There is a positive correlation between the number of downloads and the number of cases. Thus, we can infer that even though the Indian government released this contact tracing app, it all depends on the citizens to utilize it to its fullest.

5 Conclusion

This study includes the contact tracing apps proposed by other researchers using various technologies such as IoT and Blockchain prior to the Ebola outbreak. Furthermore, we examined contact tracing apps via smartphones, as well as the privacy practices used in designing and developing the app around the world. Further, this work has predicted how COVID-19 cases might grow in the coming days using the ARIMA model on a crowdsourced dataset. Furthermore, an analysis of the effect of contact tracing apps on the number of COVID-19 cases is conducted. This work concludes that even though contact

tracing apps exist, people must follow the rules and regulations suggested by the local health authorities and maintain social distancing in public places.

6 Further Research

The proposed two new features are the ability to track new variants and book vaccine slots via the smartphone app. These suggestions will help with further research, as follows:

- Study how different COVID-19 strains are spreading across the population.
- Analyze the rate of vaccination throughout the country.
- Study the effect of vaccines on the new strains of the COVD-19 virus.

Thus, these patterns enable the decision-makers to understand the ground situation and make decisions like the number of funds allocated to a particular area, etc.

References

[1] World Health Organization (WHO). "Weekly epidemiological update on COVID-19-23 March 2021 [Internet]." Geneva: WHO, 2021.

[2] Dong Y, Yao Y. D., "IoT Platform for COVID-19 Prevention and Control: A Survey," in IEEE Access, vol. 9, pp. 49929–49941, 2021, doi: 10.1109/ACCESS.2021.3068276.

[3] Buchanan, William J., Muhammad Ali Imran, Masood Ur-Rehman, Lei Zhang, Qammer H. Abbasi, Christos Chrysoulas, David Haynes, Nikolaos Pitropakis, and Pavlos Papadopoulos. "Review and critical analysis of privacy-preserving infection tracing and contact tracing." Frontiers in Communications and Networks 1 (2020): 583376.

[4] Nagori, V. "AarogyaSetu": The mobile application that monitors and mitigates the risks of COVID-19 pandemic spread in India. Journal of Information Technology Teaching Cases, 11(2), 66–80, 2021.

[5] Mankar, Vikrant, M. Naravane, and Swarupa Chakole. "The rise and impact of Covid-19 in India: Aarogyasetu App." Europ J Molec Clin Med 8.1, 2021.

[6] Tellier, R., Li, Y., Cowling, B. J., and Tang, J. W., Recognition of aerosol transmission of infectious agents: a commentary. BMC infectious diseases, 19(1), 1–9, 2019.

[7] Stedman, I. Colleen M. Flood, Vanessa MacDonnell, Jane Philpott, Sophie Thériault, and Sridhar Venkatapuram, eds. Vulnerable: The Law, Policy and Ethics of COVID-19. Ottawa, ON: University of Ottawa Press, 630 pp. Canadian Journal of Law and Society/La Revue Canadienne Droit et Société, 36(1), 185–187, 2021.

[8] Ekong I, Chukwu E, Chukwu M, "COVID-19 Mobile Positioning Data Contact Tracing and Patient Privacy Regulations: Exploratory Search of Global Response Strategies and the Use of Digital Tools in Nigeria", JMIR MhealthUhealth 2020;8(4):e19139. doi: 10.2196/19139.

[9] Cecilia Panigutti, Michele Tizzoni, Paolo Bajardi, Zbigniew Smoreda, Vittoria Colizza. Assessing the use of mobile phone data to describe recurrent mobility patterns in spatial epidemic models. Royal Society Open Science, 2017, 4(5), pp. 160950. ⟨10.1098/rsos.160950⟩. ⟨hal-01534854⟩.

[10] World Health Organization, Coronavirus disease 2019 (COVID-19): situation report, 73, 2020.

[11] Garg L., Chukwu E., Nasser N., Chakraborty C., G. Garg, "Anonymity Preserving IoT-Based COVID-19 and Other Infectious Disease Contact Tracing Model," in IEEE Access, vol. 8, pp. 159402–159414, 2020, doi: 10.1109/ACCESS.2020.3020513.

[12] S. M. Abu Adnan Abir, Shama Naz Islam, Adnan Anwar, Abdun Naser Mahmood, AmanMaung Than, "Building Resilience against COVID-19 Pandemic Using Artificial Intelligence, Machine Learning, and IoT: A Survey of Recent Progress", 2020, DOI: 10.3390/iot1020028.

[13] Wang, L. L., Lo, K., Chandrasekhar, Y., Reas, R., Yang, J., Eide, D., ... and Kohlmeier, S. Cord-19: The covid-19 open research dataset. ArXiv, 2020.

[14] COVID, U., About Variants of the Virus that Causes COVID-19, 2021.

[15] Ahmad, M., Riaz, Q., Zeeshan, M., "Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set", Journal of Wireless Communication Network 2021, 10, 2021.

[16] Azad, M. A., Arshad, J., Akmal, S. M. A., Riaz, F., Abdullah, S., Imran, M., and Ahmad, F., A first look at privacy analysis of COVID-19 contact-tracing mobile applications. IEEE Internet of Things Journal, 8(21), 15796–15806, 2020.

[17] Leith, D. J., and Farrell, S. Measurement-based evaluation of Google/Apple Exposure Notification API for proximity detection in a commuter bus. Plos one, 16(4), e0250826, 2021.

[18] Ahmad, Maged N Kamel Boulos, Ricardo Vinuesa, Junaid Qadir, "COVID-19 digital contact tracing applications and techniques: A review post initial deployments." Transportation Engineering, vol. 5 (2021): 100072.

[19] Elissa M. Redmiles,"User Concerns & Tradeoffs in Technology-facilitated COVID-19 Response", Digital Government: Research and Practice, vol. 2, issue 1, pp. 1–12, 2021.

[20] Kondylakis, H., Katehakis, D. G., Kouroubali, A., Logothetidis, F., Triantafyllidis, A., Kalamaras, I., ... and Tzovaras, D, COVID-19 mobile apps: a systematic review of the literature. Journal of medical Internet research, 22(12), e23170, 2020.

[21] Berthome, P., Fecherolle, T., Guilloteau, N., and Lalande, J. F., Repackaging android applications for auditing access to private data. In 2012 Seventh International Conference on Availability, Reliability and Security (pp. 388–396). IEEE, 2012.

[22] Gupta, R., Bedi, M., Goyal, P., Wadhera, S., and Verma, V, Analysis of COVID-19 tracing tool in India: case study of AarogyaSetu mobile application. Digital Government: Research and Practice, 1(4), 1–8, 2020.

[23] Aktay, A., Bavadekar, S., Cossoul, G., Davis, J., Desfontaines, D., Fabrikant, A. and Wilson, R. J. (2020). Google COVID-19 community mobility reports: anonymization process description (version 1.1). arXiv preprint arXiv:2004.04145, 2020.

[24] Roy, A., and Kar, S. Nature of transmission of COVID-19 in India. Medrxiv, 2020-04, 2020.

[25] N. Kumar, S. Susan, "COVID-19 Pandemic Prediction using Time Series Forecasting Models," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020, pp. 1–7, doi: 10.1109/ICCCNT49239.2020.9225319.

[26] Acker, A., and Chaiet, M, The weaponization of web archives: Data craft and COVID-19 publics. Good Systems-Published Research, 2020.

[27] Wang, L., Li, R., Zhu, J., Bai, G., and Wang, H, When the open source community meets covid-19: Characterizing covid-19 themed github repositories. arXiv preprint arXiv:2010.12218, 2020.

[28] Nadeem Ahmed, Regio A. Michelin, WanliXue, SushmitaRuj, Robert Malaney, Salil S. Kanhere, ArunaSeneviratne, Wen Hu, Helge Janicke, Sanjay K. Jha, "A Survey of COVID-19 Contact Tracing Apps", 2020, IEEE Access.

[29] B Padmaja, Madhu Bala Myneni, E Krishna Ro Patro, "A Comparison on Visual Prediction Models for MAMO (Multi Activity-Multi Object) Recognition using Deep Learning," in Journal of Big Data, Springer, 2019.

[30] M. Elkhodr, O. Mubin, Z. Iftikhar, M. Masood, B. Alsinglawi, S. Shahid and F. Flnajjar, "Technology, privacy, and user opinions of COVID-19 mobile apps for contact tracing: Systematic search and content analysis," Journal of Medical Internet Research, vol. 23, no. 2, e23467, 2021.

[31] Sarah Zabel, Michael P. Schlaile, Siegmar Otto, Breaking the chain with individual gain? Investigating the moral intensity of COVID-19 digital contact tracing, Computers in Human Behavior, Volume 143, 2023, 107699, ISSN 0747-5632.

[32] Chopdar, P. K., Adoption of Covid-19 contact tracing app by extending UTAUT theory: Perceived disease threat as moderator. Health Policy and Technology, 11(3), Article 100651, 2022.

[33] Eugene Y Chan 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.

[34] Alexei Tretiakov and Inga Hunter. 2021. User Experiences of the New Zealand COVID Tracer App: Thematic Analysis of Interviews, 2021.

[35] Y. Bengio, D. Ippolito, R. Janda, M. Jarvie, B. Prud'homme, J.-F. Rousseau, A. Sharma and Y. W. Yu, "Inherent privacy limitations of decentralized contact tracing apps," Journal of the American Medical Informatics Association, vol. 28, no. 1, pp. 193–195, 2021.

[36] Michael D. Dzandu, Antecedent, behaviour, and consequence (a-b-c) of deploying the contact tracing app in response to COVID-19: Evidence from Europe, Technological Forecasting and Social Change, Volume 187, 122217, 2023.

[37] Sarah Zabel, Michael P. Schlaile, Siegmar Otto, Breaking the chain with individual gain? Investigating the moral intensity of COVID-19 digital contact tracing, Computers in Human Behavior, Volume 143, 107699, 2023.

[38] Momeng Liu, Zeyu Zhang, Wenqiang Chai, Baocang Wang, Privacy-preserving COVID-19 contact tracing solution based on blockchain, Computer Standards & Interfaces, Volume 83, 103643, 2023.

Biographies

Haritha Akkineni is currently an associate professor in Information Technology at PVP Siddhartha Institute of Technology, Vijayawada. She received her Ph.D in Computer Science and Engineering. She is working in the area of Opinion Mining and Data Sciences. She has twelve years of academic and research experience. Her research interests are Data Science, Image Mining, Artificial Intelligence, Data Analytics, Deep Learning and Machine Learning. She has published about 38 papers in reputed Journals like SCOPUS UGC etc. She has published 2 patents. She has received grants from AICTE for organizing Short Term Training Programs. She is a reviewer for SCOPUS indexed journals. She authored a book on Opinion Mining. She acted as Workshop/tutorial chair for various International Conferences. She delivered various invited talks.

Madhu Bala Myneni is working as a Professor of computer science and engineering at VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India. She received her Ph.D in Computer Science and Engineering from JNTUH. She has Twenty-one years of academic and research experience. Her research interests are Data Science frameworks, Image Mining, Text mining, Machine learning, Artificial Intelligence, Deep Learning, and Data Analytics. She has published 57 articles in reputed Journals indexed

in SCOPUS, SCI, etc. She has published 2 patents. She is the Principal Investigator of DST funded project on sustainable smart city development. And has received variousgrants from AICTE for organizing Short Term Training Programs; Infrastructure Development; and Faculty Development Programs. And selected a part of AICTE national mission programs such as Student Learning Outcomes Assessment (SLA); Technical Book Writing (TBW). She is a reviewerfor Elsevier, Springer, and more indexed journals. She acted as session chair, organizing member, and advisory member for various International Conferences. She delivered various invited talks on Data Modelling, Data Science, and Analytics. She is a Life member of professional bodies like CSI and ISTE, Sr. Member for IEEE, WIE & International association IAENG, ICST, and SDIWC.

Budi Padmaja is currently working as an Associate Professor of CSE (Artificial Intelligence and Machine Learning), Institute of Aeronautical Engineering, Hyderabad, Telangana, India. She has received her B.Tech from the North Eastern Regional Institute of Science and Technology (NERIST), Arunachal Pradesh, India in May 2001. She completed her M.Tech from the School of IT, JNTUH, and Hyderabad, India in 2010. She was awarded the Ph.D. degree in Computer Science and Engineering in 2021 by JNTUH, Hyderabad. She has vast teaching and research experience of 20 years. She has published more than 25 research papers in various International journals and presented more than 15 papers in various International conferences. She is also a reviewer for 08 International journals. Her current areas of research interest include Machine Learning, Deep Learning, Computer Vision, and Social Network Analysis. She is a life member of ISTE, CSI, IAENG and CSTA.

Ananda Ravuri has obtained his B.Tech Degree from SV University Andhra Pradesh, and M.Tech (Electrical Machines and Industrial drivers) from NIT Warangal, Telangana. He is having nearly 20+ years' experience in Information Technology Software Architectural Design, Development and Integration of software Applications, Middleware, Device drivers and Hardware on Windows and Linux OS. His area of research includes Intel Field Programmable Gate Arrays (FPGAs) Open Stack (OFS), Smart NIC and Infrastructure Processing Unit (IPU), Workload acceleration. Presently he is working as Sr Software Engineer at Intel Corporation, USA.

CH. V. K. N. S. N. Moorthy is working as Director R&D, Vasavi College of Engineering, Hyderabad, Telangana, India. He is a multidisciplinary and cross domain researcher having experience in the fields of Computer Science and Mechanical Engineering. He received Master of Technology both in the fields of Computer Science Engineering and Heat Power Refrigeration & Air Conditioning. He received Doctoral degree for research in the field of Thermo-Nano Fluid Heat Transfer from GITAM University, Vishakhapatnam and pursuing his Doctoral degree in the field of Machine Learning too. He has nearly two decades of teaching and research experience with a total research grant of 424.46 K USD from Department of Science and

Technology, Ministry of Science and Technology, Government of India for various projects under cross domain research, more than 40 research publications, International Research Collaborations, Awards and Patents to his credit. He is a Chartered Engineer and Fellow Member of Institution of Engineers, India (IEI), a Life Member of Indian Society for Technical Education (ISTE), Member of American Society of Mechanical Engineers (ASME) and Institute of Electrical and Electronics Engineers (IEEE). His thrust areas of research include Cognitive Science, Data Analytics and Data Science, Machine Learning, Artificial Intelligence, Thermo-Nano fluid Heat Transfer, Nanotechnology, Carbon Nano Tubes, Computational Fluid Dynamics.

Raviteja CMS his B.Tech. in Computer Science and Engineering from the Institute of Aeronautical Engineering, Hyderabad in 2021. His areas of interest are Machine Learning, Deep Learning and Computer Vision. Currently he is working with Dreamplug Technologies Pvt Ltd, Bangalore as of July 2023.