A Review Of Security Concern On Covid-19 Tracing Application

Ebrahim Mubarak Abdulla Shml*[1], Siti Armiza Mohd Aris[2]

[1,2]Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia
[1]ebrahim20@graduate.utm.my, [2]armiza.kl@utm.my

Article history

Received:
13 July 2022

Received in revised form:
29 Aug 2022

Accepted:
12 Oct 2022

Published online:
15 Dec 2022

*Corresponding author
ebrahim20@graduate.utm.my

Abstract

The recent outbreak of COVID-19 has taken the world by surprise, forcing lockdowns, and straining public health care systems. In response, many governments have shown great interest in smartphone contact tracing apps that help automate the difficult task of tracing all recent contacts of newly identified infected individuals. However, tracing apps have generated much discussion around their key attributes, including system architecture, data management, privacy, security, proximity estimation, and attack vulnerability which cause reducing number of installations among individuals. In this research, we provide the first comprehensive review of the Saudi tracing app TABAUD. We also present an overview of many proposed tracing app examples, some of which have been deployed countrywide, and discuss the concerns users of TABAUD have reported regarding their usage. We close by outlining potential research directions for next-generation app design, which would facilitate improved tracing and security performance, as well as wide adoption by the population at large. The research used questionnaire methodology where all Participants completed an online survey that included thoughts and concerns about the application, status of use, and questions about whether the application was being used correctly. We performed multiple descriptive and frequency analysis to clarify the association between the use of the app and sociodemographic factors and user concerns.

Keywords: *Covid-19, tracing, Application, TABAUD, Concern*

1. Introduction

COVID-19 was designated a pandemic by the World Health Organization (WHO) on March 11, 2020, with its consequences likely determining the growth of our civilization since many generations to follow. The ability of human civilizationto quickly and collaboratively arrive at the greatest mitigation strategies will determine the path of this evolution. till a vaccination is developed or else the virus goes away on its own (Martin, Karopoulos, Hernández-Ramos, Kambourakis, & Nai Fovino, 2020).

Prevention and rapid detection of infected persons will be the most effective weapons in the hands of governments. Indeed, in the global battle to combat the spreading of COVID-19, nations, government and private corporations, academics, and many others have rapidly banded together to coordinate suitable responses, as a result of the epidemic, most health and social services will be closed down, and populations border controls will be implemented across the country. Technology and digital technologies had also facilitated the provision of critical services following the

* *Corresponding author. ebrahim20@graduate.utm.my*

introduction of certain stringent mitigation requirements(Whitelaw, Mamas, Topol, & Van Spall, 2020), On March 3, 2020, the first case of COVID-19 in Saudi Arabia was verified. In reaction to the epidemic, Saudi Arabia, like several other nations across the globe, shut down all retail and social activities, and the Saudis Ministry of Health has deployed numerous informatics systems to give public health information to people and the community.

To combat the spread of COVID-19, authorities in a number of nations are pressing for geographical monitoring. While digital surveillance may be the most efficient approach to stop the outbreak from spreading, the implications on privacy and security concerns should be addressed both now so as the epidemic progresses. Fear and anxiety frequently triumph over civil freedoms; yet, as previous crises have shown, regaining lost liberties may be difficult. As a result, it is important not just to accept the virus-response options afforded by technologies, but rather to assure that the right to security and privacy is protected (Sharma & Bashir, 2020).

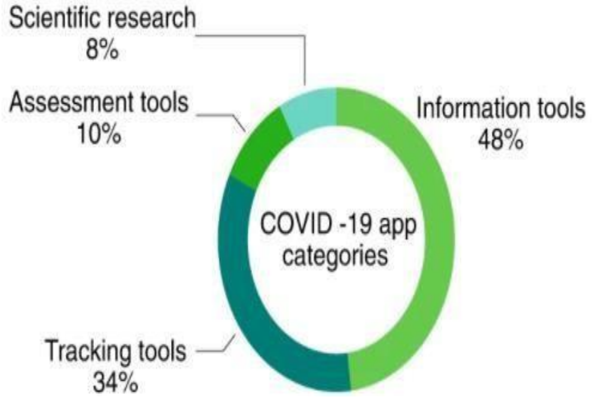

Figure 1. Distribution of COVID-19 apps from Nature Medicine(Sharma & Bashir, 2020).

Contact tracking applications obtain data from persons that have positive testsfor the disease and then utilize Geolocation, Bluetooth, or wireless technologies to locate and alert those that are in close contact with any of those people. All of the information of the user is used and collected and contact tracking applications operate with the user's data either in a centralized or decentralized manner.

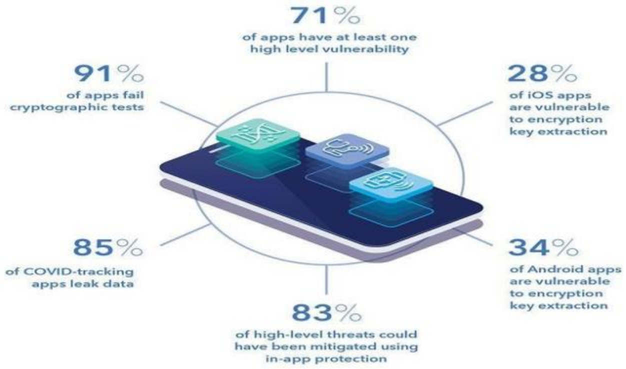
71%
of apps have at least one high level vulnerability
91%
of apps fail cryptographic tests
28%
of iOS apps are vulnerable to encryption key extraction
85%
of COVID-tracking apps leak data
34%
of Android apps are vulnerable to encryption key extraction
83%
of high-level threats could have been mitigated using in-app protection

Figure 2. COVID-19 tracing app security report analyzes (Nurgalieva, O'Callaghan, & Doherty, 2020).

The forerunner in digital rights management (DRM) new tech and largest provider of software information security, has published their 2020 security report onglobal mHealth apps, exposing that 85 percent of medical and healthcare applicationsin use for monitoring the Covid-19 have all been leaking information. The document evaluated 100 publicly accessible worldwide mobile healthcare applications along a range of subjects— incorporating COVID-19 tracking applications —to identify the most dangerous mHealth app threats (Nurgalieva et al., 2020).

As per the Ministry of Health in Saudi Arabia (TABAUD), it is among the most widely utilized application in Saudi Arabia to contain COVID-19, with much less than 5 million downloads, the Ministry of Health in Saudi Arabia has still been pressuring residents to download the app and is fining those who have not, people's concerns about security and privacy prohibit them from installing the app, which has a direct impact on the spread of the epidemic in the nation.

1.1 Centralized Approach

In terms of information sharing, apps may be divided into two categories: those that use a centralized method and those that use a decentralized one. The majority of presently implemented programs, such as the NHS COVID-19 in the United Kingdom, TraceTogether in Singapore, and COVIDSafe in Australia, are based on a centralized system.

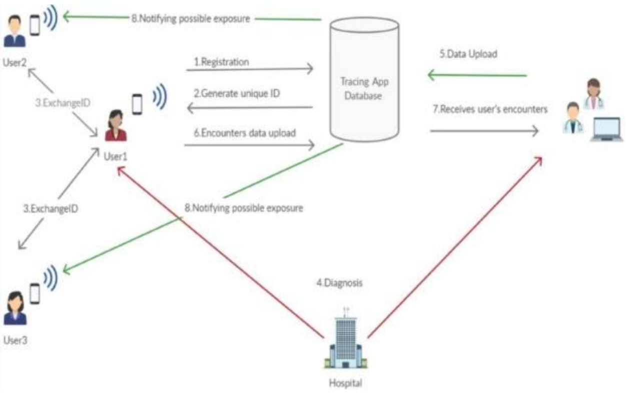

Figure 3. Centralized Approach architecture of Covid Tracing Apps (Sowmya et al, 2021).

The contact activities record is downloaded from the phone to a central database in a centralized method. Even when a user uploads information towards the database after being identified with coronavirus, the information is only kept and evaluated at the central database.

this not only offers authorities more ability to comprehend contact details and gain a better understanding of the virus's propagation, but it also allows them accessibility to sensitive information about the general public, including such specific places and who meets whom and when.

In the centralized method, irrespective over whether an individual is a virus spreader or not, all Bluetooth identification from each smartphone running the program are transferred to a central database.

1.2 Decentralized Approach

This is a much more data protection method, in which the phone activitieslog never leaves the smartphone and only limited data is downloaded to a central database, the implementation regularly uploads codes of positive diagnosed participants, and fits them against contact records stored on the device, this a methodis being used in the DP3T open protocol, and also in the Google and Apple-created "Exposure Notification" standard. The DP3T decentralized approach is used by Holland's Private Tracer.

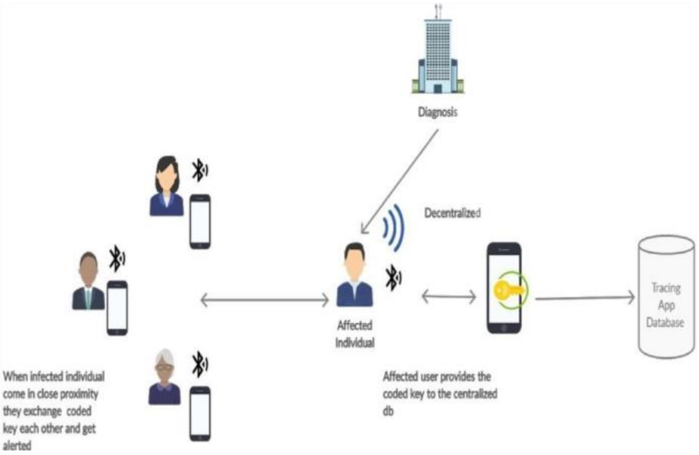
Diagnosis
Decentralized
Affected Individual
Tracing App Database
When infected individual come in close proximity they exchange coded key each other and get alerted
Affected user provides the coded key to the centralized db

Figure 4. Decentralized Approach architecture of Covid Tracing Apps (Sowmiya et al, 2021).

Figure 4 depicts a decentralized approach that delegated essential capabilities to the user's phones, leaving the server with little participation in the interaction tracking procedure. This method improves security and privacy by creating anonymized IDs on mobile networks and handling exposure notifications ondifferent devices rather than a centralized server, after testing positive for Covid-19, the individual can submit their encrypted key to a central database. This is in contrastto the centralized design, in which the user's whole profile is downloaded (Sowmiya et al., 2021).

1.3 TABAUD APP

TABAUD application is a way to notify those in contact with people infected with the emerging corona virus, where individuals can download the application and use it to achieve the health purpose for which it was developed.

The application sends camouflaged identifiers data to the smart phones used for the application, which were recorded during the period of contact with an infectedperson with the emerging corona virus, accompanied by data on the devices of infected people, according to the policies of the two global companies (Google and Apple), the application enables the user to obtain direct and proactive notifications ifany registered infection is detected, for the purpose of requesting direct health support from the Ministry of Health (in the Kingdom of Saudi Arabia).

2. METHODOLOGY

The study effort is divided into three parts that investigate Covid-19 tracing applications in Saudi Arabia and seek to analyze the behavior of users in Riyadh that influences the number of applications installed. The research strategy for this research paper reflects the general approach for linking the conceptual research difficulties to the research study's aim, this also implies that the research articulates what data is necessary, what techniques will be utilized to gather and evaluate the data, and how the data will be used to answer the research question.

The structure will attempt to solve the research issues stated before. This operational framework is a road map that provides consistency to the relevant question, the operational framework is shown in figure 5.

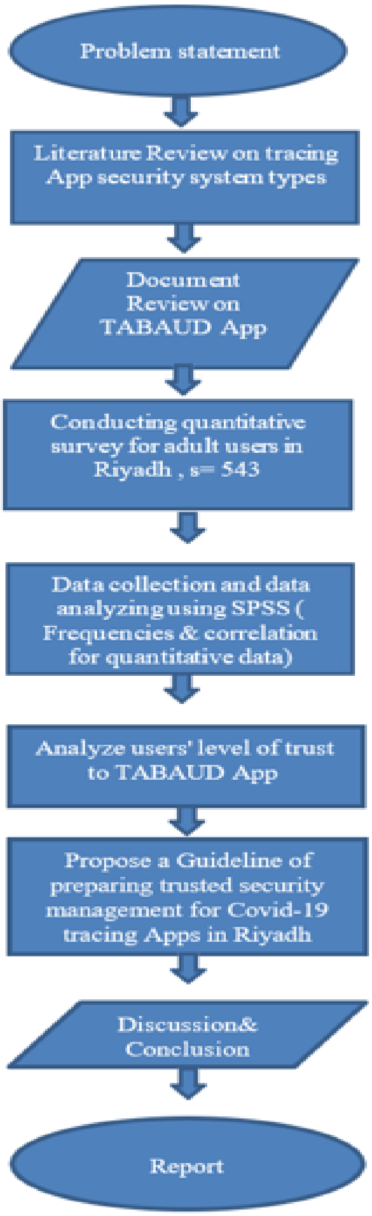
Problem statement
Literature Review on tracing App security system types
Document Review on TABAUD App
Conducting quantitative survey for adult users in Riyadh , s= 543
Data collection and data analyzing using SPSS (Frequencies & correlation for quantitative data)
Analyze users' level of trust to TABAUD App
Propose a Guideline of preparing trusted security management for Covid-19 tracing Apps in Riyadh
Discussion& Conclusion
Report

Figure 5. Flow chart

For this research study there are estimated about 543 samples of adult users for the tracing app TABAUD in Riyadh will be collected. to respond to questions about the key issues drawn from the literature review, Data obtained from the questionnaire would be evaluated using a statistical software program (Statistical Packages for Social Sciences) (SPSS).

The study population consisted of all adult users of the MOH mhealth app TABAUD in Riyadh aged 15 years or older. Based on the report of the General authority of Statistics (GAS) for the Saudi population and the estimated percent of smartphone users, the total study population was approximately 7.6 million (Alghamdi 2016). In the absence of a sampling frame, a convenience sampling method was used to collect the study data from the study population. other factors that encouraged the researchers to use convenience sampling included its low cost and the quick and easy selection of individuals. A sample of 543 individuals was determined as appropriate for the study according to the guidelines for choosing a sample size using non-probability sampling.

Based on the related literature, a questionnaire was developed to collect the data from the study population. The questionnaire comprised two parts: demographic characteristics, awareness and use of mhealth apps, and a list of items to evaluate the purpose, concerns, understanding, and satisfaction with TABAUD app. The demographic variables included nationality, gender, age. The second part included questions to assess the level of knowledge of TABAUD security system and the methods by which they came to know about the apps and their use. in addition to evaluating the perceived concerns and trust (third party concerns); (I find the app to be beneficial); for TABAUD mhealth app by rating the items on a five-point Likert scale ranging from 1=strongly disagree to 5=strongly agree. An electronic questionnaire was developed using Google Form and then distributed via WhatsApp during March 2022 to the study population. Total of 543 responses were found valid for analysis.

For this research study there are estimated about 543 samples of adult users for the tracing app TABAUD in Riyadh will be collected. to respond to questions about the key issues drawn from the literature review.

The purpose of this questionnaire survey is to accomplish objective number two. In carried out to examine the elements influencingconfidence in tracing apps and how this affects the apps' capacity to reduce the onset of the Covid-19 epidemic. The questionnaire would be in the format of a multiple- choice test. Multiple-choice questions necessitate anticipating the entire number of alternative answers and structuring options accordingly.

3. Results

3.1 Demographic data of the respondents

3.1.1 Gender

Table 1 and figure 6 show the gender distribution of the respondents. The results indicated that (61.9%) of the respondents were females and (38.1%) males.

Table 1. Gender Distribution of The Respondents

Characteristics		Frequency	Percent %
Gender	Male	207	38.1%
	Female	336	61.9%
Total		543	100%

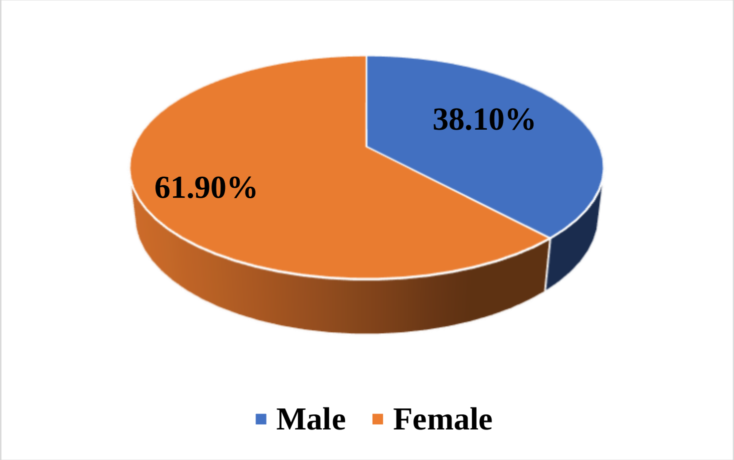

Figure 6 .The Gender Distribution Of The Respondents

3.1.2 Age

Table 2 and figure 7 present the age distribution of the respondents. The results showed that most of the respondents (62.6%) were in the age category within 26-64 years, (33.7%) of the respondents were in the age category within 15-25 years, and (3.7%) of the respondents were in the age category within 65 years and older.

Table 2 The Age Distribution of The Respondents

Characteristics		Frequency	Percent %
Age	15-25 years	183	33.7%
	26-64 years	340	62.6%
	65 years and older	20	3.7%
Total			100%

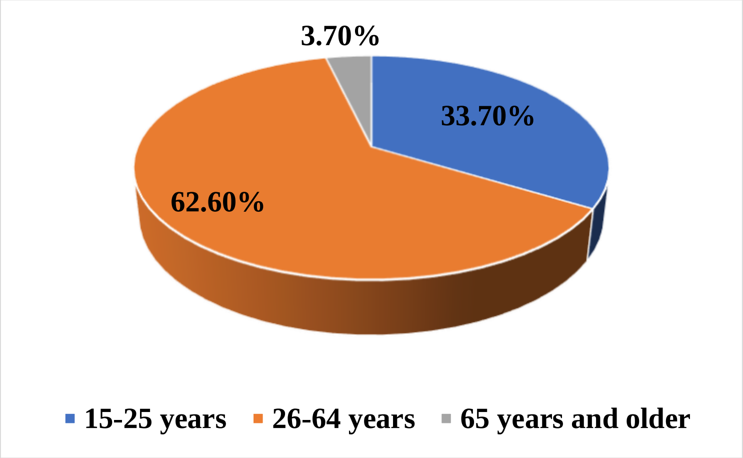

Figure 7. The distribution of the respondents

3.1.3 Nationality

Table 3 and figure 8 show the nationality distribution of the respondents. The results reported that most of the respondents (72.9%) of the were Saudis and (27.1%) of the respondents were non-Saudi.

Table 3 The Nationality Distribution Of The Respondents

Characteristics		Frequency	Percent %
Nationality	Saudi	396	72.9%
	Non-Saudi	147	27.1%
Total		543	100%

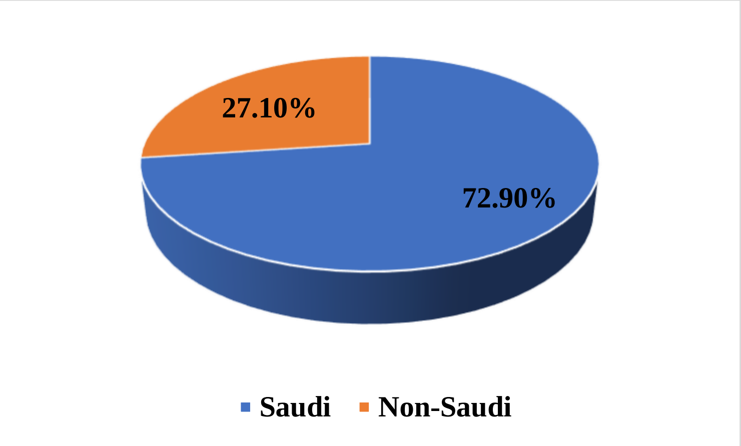

Figure 8. The Nationality Distribution of The Respondents

3.2 Analyzing the Covid-19 TABAUD App security challenges

This study used descriptive statistics such as frequencies and percentages to analyze the Covid-19 TABAUD App security challenges. This study applies the three-point Likert scale (always, sometimes, and never). The questionnaire respondents were asked to indicate the personal degree of agreement toward the scale's statements.

3.2.1 Do you know what security system used for TABAUD App?

The results presented in Table 4 and figure 9 showed that the more than half of the respondents (56%) of the respondents didn't know what security system used for TABAUD App, (42.2%) of them stated (Yes), and only (1.8%) of them stated (Maybe).

Table 4. The Answers Of The Respondents About (Do You Know What Security System Used For TABAUD App?)

Characteristics		Frequency	Percent %
Do you know what security system	Yes	229	42.2%
	Maybe	10	1.8%

used for TABAUD App?	No	304	56 %

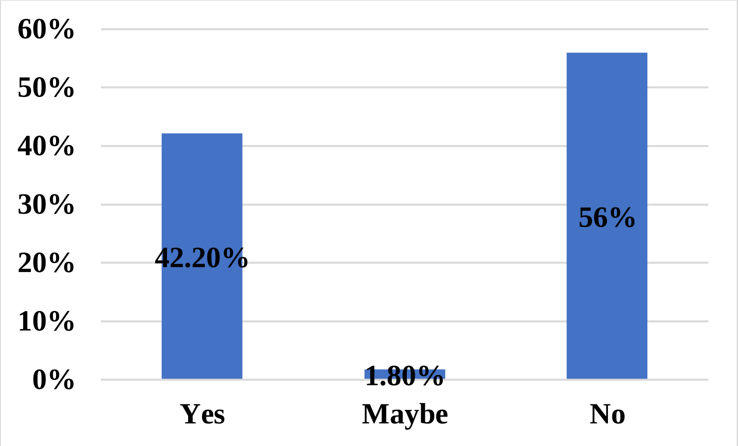

Figure 9. The answers of the respondents about (do you know what security system used for TABAUD App?)

3.2.2 If yes, do you understand what notification exposure system is?

The results presented in Table 5 and figure 10 showed that (31.1%) of the respondents who did know what security system used for TABAUD App they also, understand what notification exposure system is, while (11.6) of them stated (No), and (1.8) of them stated (Maybe).

Table 5 the answers of the respondents about (If yes, do you understand what notification exposure system is?

If yes, do you understand what notification exposure system is?	Yes	169	70%
	Maybe	10	4%
	No	63	26%

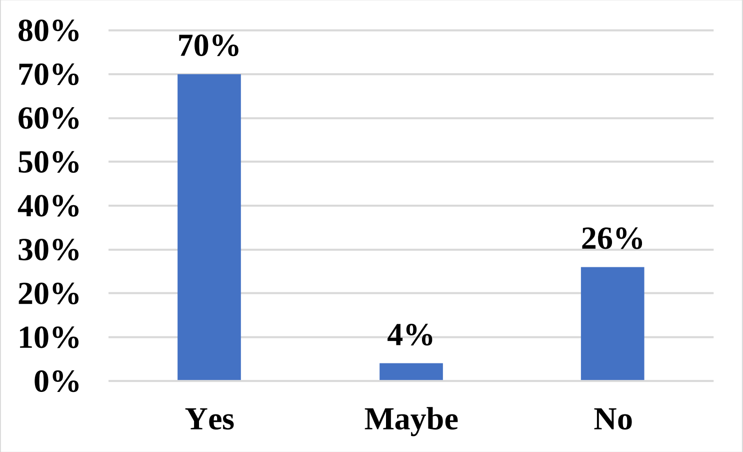

Figure 10. The Answers Of The Respondents About (If Yes, Do You Understand What Notification Exposure System Is?

3.2.3 I think it is an invasion of privacy

The results presented in Table 6 and figure 11 indicated that the majority of the respondents (70.9%) sated that Sometimes TABAUD App is an invasion of privacy, however it is necessary, (20.6%) of them stated (Never), and only (8.5%) of them stated (Always).

Table 6. the answers of the respondents about (I think it is an invasion of privacy)

Characteristics		Frequency	Percent %
I think it is an invasion of privacy	Always	46	8.5%
	Sometimes, however it is necessary	385	70.9%
	Never	112	20.6%

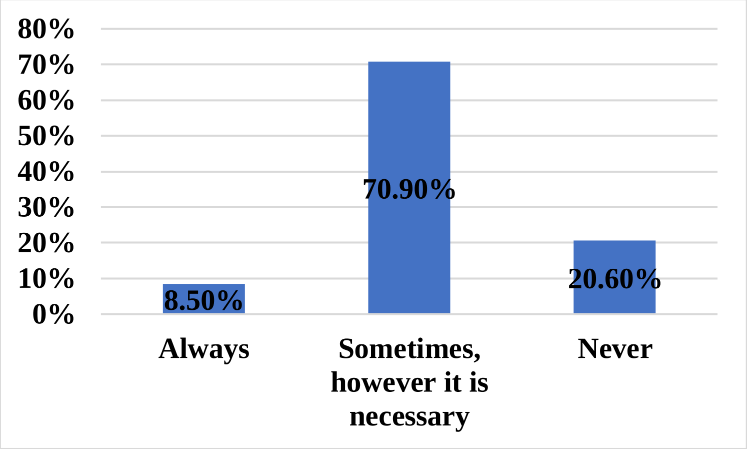

Figure 11. The answers of the respondents about (I think it is an invasion of privacy)

3.2.4 Security concerns about covid-19 TABAUD app

The results presented in Table 7 and figure 12 reported that most of the respondents (68.5%) sated that always have security concerns about covid-19 TABAUD app, (20.4%) of them stated (Sometimes), and only (11%) of them stated (Never).

Table 7. the answers of the respondents about (Security concerns about covid-19 TABAUD app)

Characteristics		Frequency	Percent %
Security concern about covid-19 TABAUD app	Always	372	68.5%
	Sometimes	111	20.4%
	Never	60	11%

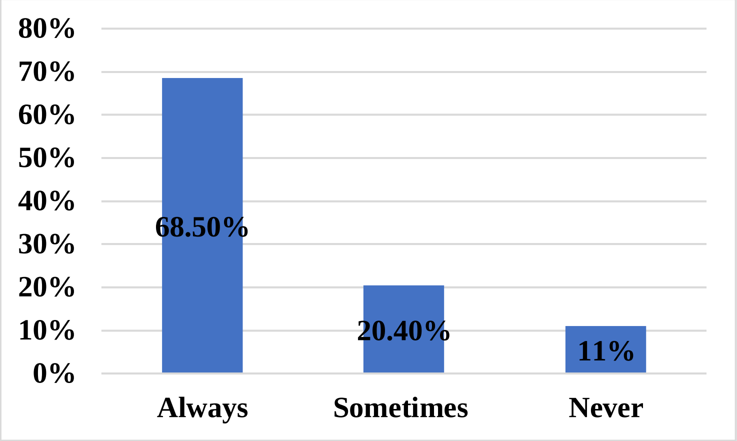

Figure 12 the answers of the respondents about (Security concerns about covid-19 TABAUD app)

3.2.5 Doubt about effectiveness of app for preventing spread of the pandemic

The results presented in Table 8 and figure 13 showed that (44.4%) of the respondents sated that always have Doubt about the effectiveness of the app for preventing spread of the pandemic, (29.5%) of them stated (Sometimes), and only (26.2%) of them stated (Never).

Table 8. The answers of the respondents about (Doubt about the effectiveness of the app for preventing spread of the pandemic)

Characteristics		Frequency	Percent %
Doubt about the effectiveness of the app for preventing spread of the pandemic	Always	241	44.4%
	Sometimes	160	29.5%
	Never	142	26.2%

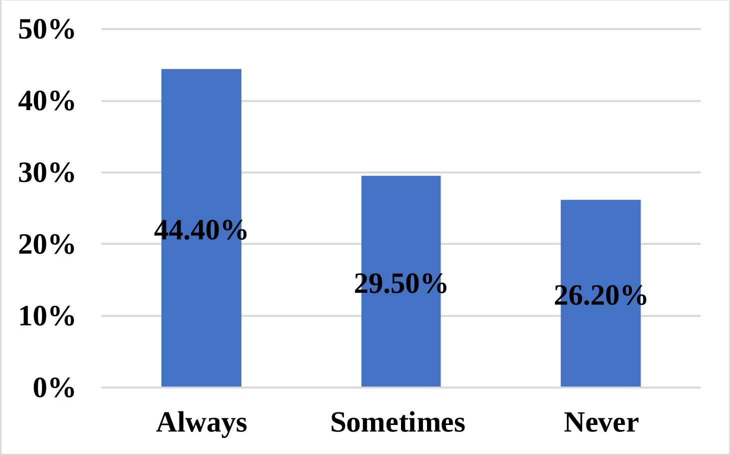

Figure 13. the answers of the respondents about (Doubt about the effectiveness of the app for preventing spread of the pandemic)

3.2.6 Trust in the Ministry of Health strategy for Covid-19

The results presented in Table 9 and figure 14 revealed that almost half of the respondents (49.2%) sated that always have Trust in the Ministry of Health strategy for Covid-19, (39%) of them stated (Sometimes), and only (11.8%) of them stated (Never).

Table 9 the answers of the respondents about (Trust in the Ministry of Health strategy for Covid-19)

Characteristics		Frequency	Percent %
Trust in the Ministry of Health strategy for Covid-19	Always	267	49.2%
	Sometimes	212	39%
	Never	64	11.8%

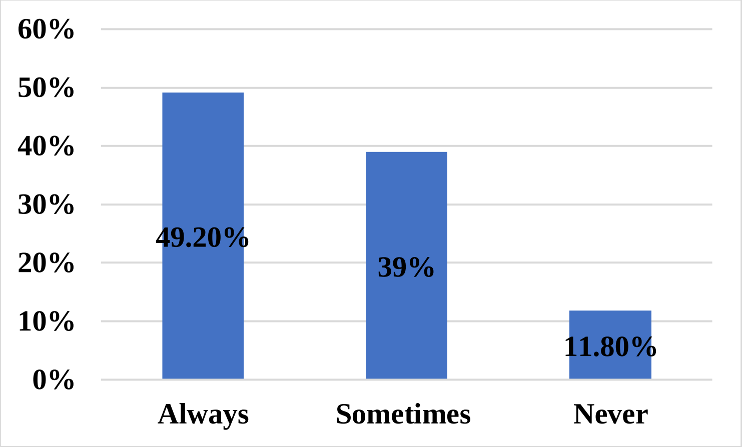

Figure 14 The answers of the respondents about (Trust in the Ministry of Health strategy for Covid-19)

3.2.7 I don't want the government to have access to my location data

The results presented in Table 10 and figure 15 indicated that most of the respondents (65.6%) sated that never want the government to have access to their location data, (25.2%) of them stated (Sometimes), and only (9.2%) of them stated (Always).

Table 1.0 the answers of the respondents about (I don't want the government to have access to my location data)

Characteristics		Frequency	Percent %
I don't want the government to have access to my location data	Always	50	9.2%
	Sometimes	137	25.2%
	Never	356	65.6%

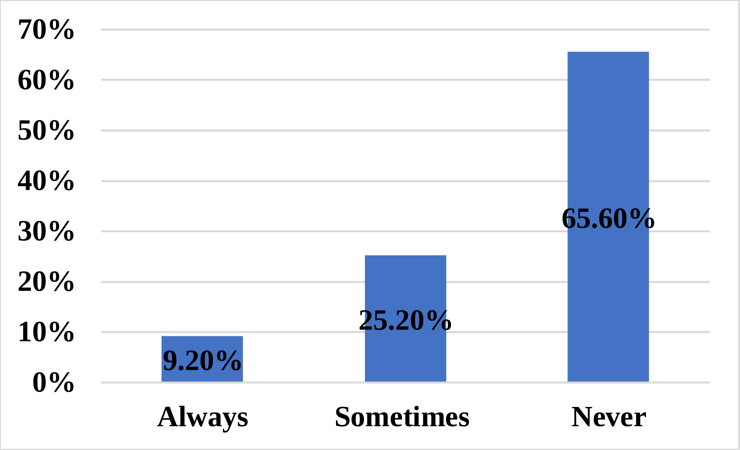

Figure 15. the answers of the respondents about (I don't want the government to have access to my location data)

4.2.8 Concerned about third-party groups having my data and location

The results presented in Table 11 and figure 16 showed that most of the respondents (63%) sated that Always they are concerned about third-party groups having their private health data and location, (21.9%) of them stated (Sometimes), and only (15.1%) of them stated (Never).

Table 11. the answers of the respondents about (I'm concerned about third-party groups having my private health data and location)

Characteristics		Frequency	Percent %
I'm concerned about third-party groups having my private health data and location	Always	342	63%
	Sometimes	119	21.9%
	Never	82	15.1%

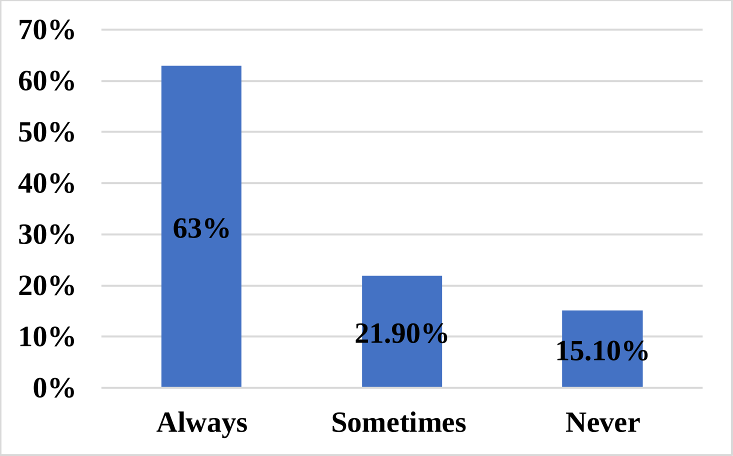

Figure 16. the answers of the respondents about (I'm concerned about third-party groups having my private health data and location)

4.2.9 I don't believe enough people will install it

The results presented in Table 12 and figure 17 reported that (30.4%) of the respondents sated that Always don't believe enough people will install it, (35.2%) of them stated (Sometimes), and (34.4%) of them stated (Never).

Table 12. The answers of the respondents about (I don't believe enough people will install it)

Characteristics		Frequency	Percent %
I don't believe enough people will install it	Always	165	30.4%
	Sometimes	191	35.2%
	Never	187	34.4%

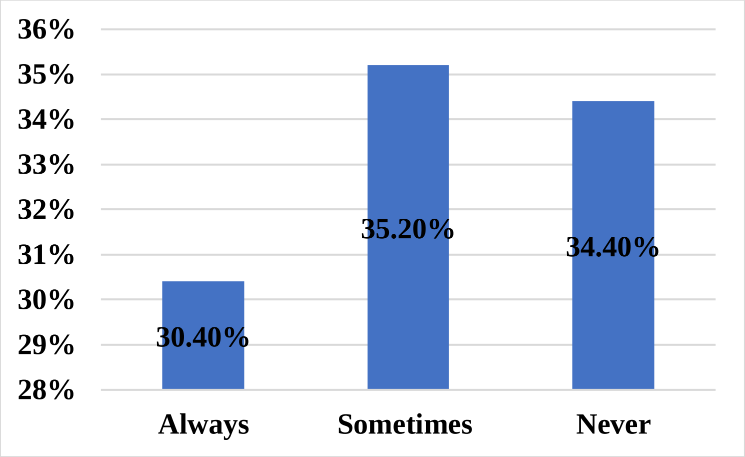

Figure 17. the answers of the respondents about (I don't believe enough people will install it)

3.2.10 I don't believe the virus is as big of a threat as it's been said to be

The results presented in Table 13 and figure 18 revelated that (29.5%) of the respondents sated that always don't believe the virus is as big of a threat as it's been said to be, (31.7%) of them stated (Sometimes), and (38.9%) of them stated (Never).

Table 13. The answers of the respondents about (I don't believe the virus is as big of a threat as it's been said to be)

Characteristics		Frequency	Percent %
I don't believe the virus is as big of a threat as it's been said to be	Always	160	29.5%
	Sometimes	172	31.7%
	Never	211	38.9%

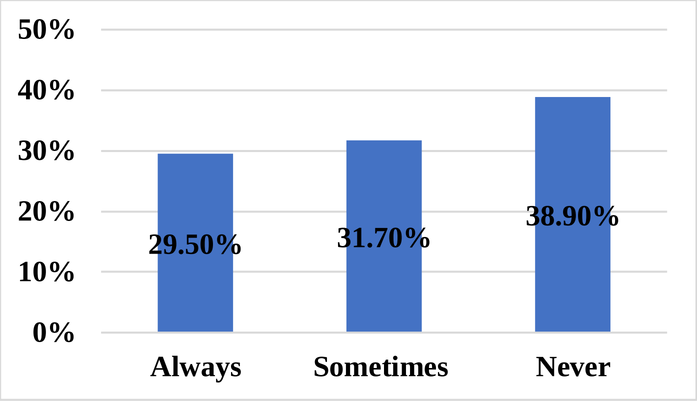

Figure 18. the answers of the respondents about (I don't believe the virus is as big of a threat as it's been said to be)

4.3 Discussion

In this study, we evaluated the usage of the COVID-19 Contact Application (TABAUD), a COVID-19 contact tracing application developed by the Saudi Ministry of Health. TABAUD uses Bluetooth like many other COVID-19 contact tracing applications. TABAUD does require registration of personal information and does record personal information, the application will record anonymous contact information from the opposite smartphone when one TABAUD-installed smartphone comes in close proximity (within 1 m) with another TABAUD-installed smartphone for 15 min or more. If COVID-19 is diagnosed in one of the smartphone owners, a notification is sent via the Internet to the recorded contact persons in the app with whom the smartphone owner has been in contact. Although the health centre and government do not know who received the notification, if a person who received the notification contacts a local health centre it is possible to get tested for COVID-19 if the health centre decides that it is necessary.

Regarding concerns for contact tracing applications, the question item was developed based on concerns from the general population which were listed on the website of the Saudi Ministry of Health, as frequently asked questions about this application. All participants rated their concerns for the following items regarding the TABAUD on a 4-point bipolar scale (1 = strongly disagree, 4 = strongly agree): 1) insufficient knowledge of how to use the application, 2) concerns about privacy, 3) security concerns, 4) doubts about the effectiveness of apps for preventing spread of infection, 5) . For the current study, a response of 3 or 4 was defined as “having concern” about that matter.

In the first wave of the survey, participants provided their sex, age, nationality. In the second wave of the survey, participants indicated their level of trust in the Saudi Ministry of Health COVID-19 strategy using a 4-point bipolar scale (1 = very low, 4 = very high. This question was adapted from the behavioural insights research for COVID-19 questionnaire published by the World Health Organization regional office in Europe. In the current study, a response of 1–3, 4, 5–7, was defined as having low, middle, and high level of trust in the Japanese Ministry of Health respectively.

the purpose of this study was to clarify the concern, implementation, and correct usage of a COVID-19 contact tracing application among Saudi citizens and factors inhibiting implementation and correct use of the application. We defined participants who responded that they were aware of the TABAUD security system as 'COVID-19 contact tracing application users. Participant characteristics, level of trust in the Saudi Ministry of Health, and concerns regarding the contact tracing app were compared between COVID-19 contact tracing application users and non-users. Regarding correct usage of the COVID-19 contact tracing application, we clarified the percentage of app users who were partially understood hoe security system works and those who were not aware of security system process for TABAUD.

In Saudi Arabia, the adoption of mhealth applications has become a priority for improving healthcare services, particularly during pandemics. To contain the spread of the COVID-19 pandemic, the Saudi MOH has developed and launched many mhealth apps. This study aimed to evaluate the users' awareness, use, and security concerns toward the leading mhealth app TABAUD and propose an enhanced guideline for developers. In addition, the study assessed the inter-relationships in users' perceptions and tested the differences in the users' evaluations across the demographic variables. The study findings revealed that most of the Saudi population do not know the mhealth app TABAUD security system. The results show that even though most people do not know the privacy and security system used for TABAUD there still quite big number of do know the system and how it works. The high knowledge of the Tabaud app could be attributed to a large number of services it provides and its mandatory use to get services from private and public organizations. Moreover, the study results show that most of users who is aware security system used for TABAUD are actually well aware notification exposure system and how it works in addition to its security issues.

There is an approximate consensus that privacy is not a priority, but rather the important thing is to take advantage of the application, which means the users who are not aware of the applications that they use, they also prefer the application be a centralized or government-controlled software over decentralized them since the trust between the users and the government is somewhat high.

4. Conclusions

This study aims to examine the Covid-19 TABAUD App security challenges. A descriptive analysis was used to address the objective of the study. The study found that most of the users didn't know what security system was used for TABAUD App, however, slightly lower than half of the users have knowledge about the security system used for TABAUD App and understand what notification exposure system is. The study found that the majority of the users think TABAUD App is an invasion of privacy, however, they considered it a necessary application.

The study found that the users who are familiar with the security and protection program of TABAUD App often have greater confidence in the effectiveness and benefit of the application, but at the same time, they are the most fearful of the security aspects of the application and prefer that the application be centralized or controlled by the government even there is a violation of privacy from the government, but they think it is safer for them since the trust between the users and the government is somewhat high.

The study found that the users who don't have an idea about the privacy and protection program used in TABAUD App often doubt the benefit and effectiveness of the application and at the same time there are various fears in terms of the application security and privacy.However, there is an approximate consensus that privacy is not a priority, but rather the important thing is to take advantage of the application, which means the users who are not aware of the applications that they use, they also prefer the application be a centralized or government-controlled software over decentralized.

The study found that most of the users think that not enough people will install TABAUD App during the pandemic because it is not effective enough for preventing the spread of the pandemic, and because security issues since it is a decentralized app.The experimental data of UTM-LST VFE-2 model at high angle of attack is presented here. More experiments are needed to verify this complicated flow topology.

References

[1] Alghamdi, K. A. (2016). Designing geodatabases for the general authority for statistics of the Kingdom of Saudi Arabia.

[2] Almufarij, A. (2022). Perceptions of Using Mobile Health Apps (mHealth) During Covid-19 Pandemic In Saudi Arabia: A Cross-Sectional Study. 1Journal of Health Informatics in Developing Countries.

[3] Bajaj, R., et al. (2002). "GPS: location-tracking technology." Computer 35(4): 92-94.

[4] Bashshur, R. and G. W. Shannon (2009). History of telemedicine: evolution, context, and transformation, Mary Ann Liebert New Rochelle, NY.

[5] Bhatraju, P. K., et al. (2020). "Covid-19 in critically ill patients in the Seattle region—case series." New England Journal of Medicine 382(21): 2012-2022.

[6] Ferretti, L., et al. (2020). "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing." Science 368(6491): eabb6936.

[7] Halpern, N. A. and K. S. Tan (2020). "United States resource availability for COVID-19." Society of Critical Care Medicine 3.

[8] Hassounah, M., et al. (2020). "Digital response during the COVID-19 pandemic in Saudi Arabia." Journal of medical Internet research 22(9): e19338.

[9] Li, T., et al. (2020). "Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing apps." arXiv preprint arXiv:2005.11957.

[10] Martin, T., et al. (2020). "Demystifying COVID-19 digital contact tracing: A survey on frameworks and mobile apps." Wireless Communications and Mobile Computing 2020.

[11] Mbunge, E. (2020). "Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls." Diabetes & Metabolic Syndrome: Clinical Research & Reviews 14(6): 1631-1636.

[12] Nurgalieva, L., et al. (2020). "Security and privacy of mHealth applications: a scoping review." IEEE Access 8: 104247-104268.

[13] Sampat, B. H. and B. Prabhakar (2017). "Privacy risks and security threats in mHealth apps." Journal of International Technology and Information Management 26(4): 126-153.

[14] Sharma, T. and M. Bashir (2020). "Use of apps in the COVID-19 response and the loss of privacy protection." Nature Medicine 26(8): 1165-1167.

[15] Shukla, M., et al. (2020). "Privacy guidelines for contact tracing applications." arXiv preprint arXiv:2004.13328.

[16] Sowmiya, B., et al. (2021). "A survey on security and privacy issues in contact tracing application of COVID-19." SN computer science 2(3): 1-11.

[17] Tomar, A. and N. Gupta (2020). "Prediction for the spread of COVID-19 in India and effectiveness of preventive measures." Science of The Total Environment 728: 138762.

[18] Uğurel, O. M., et al. (2020). "An updated analysis of variations in SARS-CoV-2 genome." Turkish Journal of Biology 44(7): 157-167.

[19] Vaudenay, S. (2020). "Centralized or decentralized? The contact tracing dilemma." Cryptology ePrint Archive.

[20] Wang, D. and F. Liu (2020). "Privacy risk and preservation for COVID-19 contact tracing apps." arXiv preprint arXiv:2006.15433.

[21] Wen, H., et al. (2020). A study of the privacy of covid-19 contact tracing apps. International Conference on Security and Privacy in Communication Systems, Springer.

[22] Whitelaw, S., et al. (2020). "Applications of digital technology in COVID-19 pandemic planning and response." The Lancet Digital Health 2(8): e435-e440.

[23] Wosik, J., et al. (2020). "Telehealth transformation: COVID-19 and the rise of virtual care." Journal of the American Medical Informatics Association 27(6): 957-962.

[24] Zhao, Q., et al. (2020). On the accuracy of measured proximity of bluetooth-based contact tracing apps. International Conference on Security and Privacy in Communication Systems, Springer.