Journal of Theoretical and Applied Information Technology
30th June 2022. Vol.100. No 12
© 2022 Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN OVERVIEW OF THE DATA AND USER REQUIREMENT OF RESIDENT'S SECURITY AND SAFETY APPLICATION ON SMARTPHONE

AMZARI ABU BAKAR[1] , NORHAYATI HUSSIN[2], ZAHARUDIN IBRAHIM[3], HASNAH HASHIM[4]

[1]Faculty of Information Management, Universiti Teknologi MARA Cawangan Selangor, Kampus Puncak Perdana, 40150 Shah Alam, Selangor, Malaysia
E-mail: [1]amzari1467@uitm.edu.my, [2]yatihussin@uitm.edu.my, [3]zahar347@uitm.edu.my, [4]hasnahhashim@uitm.edu.my

ABSTRACT

This paper discusses the crucial elements of developing a resident's security and safety application on the smartphone. The discussion focuses on identifying and determining the applicable requirement of the apps to be used by the residents. The collated data and user requirements will comprise security and safety parameters prevalent in the state and crucial features that residents would like to use when implementing the mobile application. This paper aims to construct an understanding of mobile apps and discuss the component that creates a firm foundation for advancing knowledge and facilitating based on the development of the apps. The method used is a literature survey. The secondary data source of information has been identified to explore the element in developing the security and safety of the mobile application for the large population. The information gained from the previous journal nationally and internationally ensures the right components are discussed. The paper's outcome will significantly contribute to and benefit potential mobile application developers, the communities, higher learning institutions, the federal government of Malaysia, academicians, and researchers. It can also contribute to the body of knowledge in the field of information management. Lastly, the execution of this study will help bolster the government's plan of the National Digital Economy Initiative (Digital Malaysia) towards strengthening the digital information economy of the nation.

Keywords: *Safety, Security, Mobile Application, Data Requirement, User Requirement*

1. INTRODUCTION

The security concerns that loom around Malaysia and Selangor particularly calls for consideration. The rising frequency of security concerns or cyber-attacks has become a worldwide acknowledged phenomenon, not only in Malaysia. Malaysia is especially vulnerable to cyber and internet-related security concerns due to its high internet penetration. This can be explained by several events that transpired over time (Mat et al., 2020). Eventually, cybercrime emerged as a significant economic worry in Malaysia. According to the Sophos Security Threat Report 2013, Malaysia is the sixth most endangered country in cybercrime. According to a CSIS analysis, the number of cybercrime in Malaysia is 0.18 per cent of GDP, or about RM 215 million each year. Malaysia is thought to have lost RM 179.3 million to cybercrime in 2015. Meanwhile, Malaysia's number of cybercrime incidents has climbed by 10,000 each year on average, with online frauds and hacking being the most common (CyberSecurity Malaysia, 2019).

Besides that, Malaysia places a premium on the security of its critical national information infrastructure, given the country's reliance on ICTs related to daily country activities, especially in the aspect of economics (Zahri & Sharifuddin, 2017). This type of improvement is critical. Currently, the majority, if not all, national critical infrastructures are being developed with network systems and information technology in mind. As a result, all of these vital assets must be well-protected. Lastly, the crisis in international politics shows Malaysia is one of the targets of Cyber-attacks from a geopolitical and strategic standpoint. Indeed, Southeast Asia is an area in flux, with significant powers such as the United States and China present and the potential for conflict that still exists, primarily in the South China Sea, making the country vulnerable to cyber attacks. Malaysia was one of the primary targets of malware assaults by overseas hackers between January and June 2015, according to research by FireEye (2015).

As profiting as it is, urbanization has created numerous social problems. Some of which are generally increased crime rates and insecurity (Ojo & Ojewale, 2019). On the one hand, cities are developing and thriving, and then, on the other hand, the growth comes with increased crime rates such as theft, fraud, kidnapping, robbery and other forms of terrorism. As an Urban habitation, Malaysia is not an exception to this dilemma. In fact, from a previous speech by the Minister of Home Affairs YB Dato' Seri Hishammuddin Tun Hussein, as stated by Bin & Soh (2012), "Crime affects all Malaysians, irrespective of race, religion, gender or income levels…" his speech signified the prevalence of this problem in the nation (Bin & Soh, 2012). Therefore, it is of no doubt that crime, insecurity and terrorism have begun eating the fabric tip of the nation gradually. Sadly, this isn't just true of peak urban cities such as Kuala Lumpur, but Selangor, as an urban state, is also in the same pot. In a previous order placed by the Inspector-General of Police (IGP), Tan Sri Khalid Abu Bakar said that he had proposed that about 1,000 CCTV cameras be mounted at strategic hotspot locations that have been susceptible to crime and terrorism (Malay Mail, 2013).

As a foundation for future development, the study postulated the following objectives consist of; (1) to precisely identify the security challenges that beset Selangor, and (2) to garner and collate the User requirement, Data requirements and Features that pertain to the making of a security and safety mobile Application from Selangor locales. (3) To establish a groundwork for the potential development of intelligent security and safety mobile Applications tailored to function in Selangor. Other than that, this study also assists the government's plan of the National Digital Economy Initiative (Digital Malaysia) towards strengthening the digital information economy of the nation. The development of a security and safety mobile application will be further discussed to make sure the study's author has discussed the suitable component. This paper will significantly contribute to the body of knowledge on the security and safety of mobile applications that could be used.

2. LITERATURE REVIEW

2.1 Literature Survey

The literature survey has been used to explore and dig out the information related to security and safety mobile applications. A literature survey is defined as a documentation of the comprehensive published and unpublished work from the secondary data sources in the specific area of study of the researcher (Uma Sekaran, 2003). There are various sources of information that could be used for literature surveys, such as journal articles, government documents, newspapers, magazines, and any relevant sources available on the internet. These secondary data sources will assist the researcher in understanding and finding out the trends of the data based on the topic of the study. That information will be beneficial to the researcher in exploring and investigating the issue related to the current topic.

The secondary data sources represent the data that has already been collected for another purpose by the previous scholar but have some relevance to the current topic (Intellpost, 2020). The previous journal from various sources of information such as Google Scholar, Emerald Insight, and ScienceDirect has been explored and dug out by the researcher to ensure the correct information has been investigated based on the topic of study. Other documentation has been looked up, including articles on the website, newspapers, conference proceedings, and other secondary data sources. This is the most significant way to explore and dig out more information regarding the topic of study to ensure the researcher leaves behind no variable.

2.2 Defining Safety

The inverse of risk is widely used to describe safety: the smaller the risk, the higher the safety. Although safety as the antonym of risk captures some of the fundamental aspects of safety, it does not fully know the notion (Möller, Hansson, & Peterson, 2006). The product of likelihood and severity is frequently referred to as risk. Safety is increased by lowering both possibility and severity, which is the antonym or opposite of risk. Safety is nothing more or less than a condition or assessment of adequate control over hazards and dangers inherent in what an organization is doing now or plans to do in the future. The fundamental problem is controlling the inherent hazards in the business process, especially those not regulated to an acceptable level. An uncontrolled threat has the potential to harm (Montante, 2008).

Physical and/or nonphysical barriers prevent, regulate, or mitigate unfavourable events or incidents (Sklet, 2006). A frequent safety management method is to work toward having adequate barriers to prevent an incident or implementing extra barriers after an incident occurs. Defence in depth (barriers) is a simple linear system for evaluating and preventing accidents; nevertheless, it implies that barriers act independently of one another. While this may be true in some cases, it is a limited perspective given the complicated nature of safety management. Furthermore, the energy model argues that without addressing or enhancing other barriers, for example, implementing further training after an incident without reviewing and reinforcing accountability), one additional barrier will prevent an incident from occurring.

There have been many different definitions of safety over the years. By (Reason, 2000) mentioned that individuals' or organizations' ability to deal with risks and hazards in order to avoid harm or losses while still achieving their objectives. According to (Pierre, 2001), "a situation in which hazards and conditions that contribute to physical, psychological, or material harm are regulated to preserve the health and well-being of individuals and the community." Besides that, safety controls unintentional loss, according to Bird, Germain, and Clark (2003). In 2009, safety was the condition in which the risks were deemed to be tolerable (NSC, 2009). By (ANSI/ASSE, 2011), it is the freedom from unacceptable risk. Hollnagel (2014) mentioned that safety is the situation in which the quantity of adverse outcomes is kept as low as possible by attempting to ensure that things do not go wrong by eliminating or containing the causes of malfunctions and risks and also a state in which the quantity of successful outcomes is as great as feasible, the ability to succeed in a variety of situations by attempting to ensure that things go right rather than preventing them from going wrong. In 2015, there are several definitions, such as the management of known risks in order to attain an acceptable level of risk (ASSE, 2015), protection from dangers and hazards that arise from, are related to, or occur in the course of employment (CSSE, 2015) and also the presence of abilities, capacities, and competencies that allow things to run smoothly (Dekker, 2015).

2.3 Mobile Security

Wireless security and mobile security are inextricably linked. Simply said, mobile security is the process of protecting mobile services and devices from third-party attacks or vulnerabilities. Today's profit-making and non-profit-making institutions use a variety of tools and technology, the majority of which are mobile-based. Hence Mobile Security is a major problem. (Geneiatakis, 2017). IT security is divided into several sub-fields, like Web security, network security, database security, and other new fields such as these are important. Security in the cloud, mobile security, and so on. As a result, mobile security is a component of advanced IT security in many cases. Different companies apply various tactics for mobile security, one of which is allowing clients and employers to use just their respective or selected smartphones (Paul, 2019).

The fields of Mobile Security and Wireless Security are inextricably linked. However, the wireless security concept predates mobile security, and it is now inextricably linked to cloud security and mobile computing. (Nkosi, 2010). In today's age of information technology, mobile security is critical. With mobile computing, it's extremely close. In other words, it refers to the security of mobile devices such as smartphones. Attackers frequently link mobile security with smartphones, computers, and other devices. Short message service (SMS), multimedia messaging service (MMS), WIFI, Bluetooth, and other features are usually included. However, a few experts have issued warnings concerning operating system security, stating that attackers may leverage various objects provided by browsers, operating systems, or malicious Software (Paul,2019).

It's important to note that downloading apps might sometimes compromise cellphone security. Privacy and integrity programmes should be included with any smartphone or electronic device. According to network experts, the attackers' primary targets are:

a) Data: Credit card numbers, authentication indications, audio, visual material, call logs, and other sensitive or virtual information are all stored on smartphones or electronic gadgets. As a result, this is the main target.
b) Identity: The owner of an electronic device can be easily identified, and cyber attackers can use this identity for a variety of objectives.

As far as recent threads on mobile security are concerned, they are concerned with a variety of items such as:

a) Boot networks
b) Spyware is number two.
c) A harmful link
d) Peculiar applications

Operating Systems: Operating systems are at the heart of mobile devices, and there are various mechanisms in place to ensure and safeguard them from attack. Because smartphones may accommodate a variety of applications, there should be a sufficient process to detect vulnerabilities and any type of virus, malware, spyware, or other malicious software. Sandbox is an essential topic in mobile, and each phone must plan for its own

Sandbox in this regard. In this sense, a few key concerns (mostly in Android) are as follows:

The rootkit's penetration is critical, and hence a proper rootkit detection mechanism is critical.

a) Process isolation is also highly crucial in android-based systems, and this should be kept in mind for proper and scientific security. Furthermore, once each procedure has begun, it must be completed before proceeding to the next program. This method will lessen the risks of becoming vulnerable.
b) File system permission is a significant challenge for android-based systems, and the use of locking memory permission is also a concern.
c) Memory protection is an important feature and function of Android-based or comparable devices' operating systems.
d) Development in a runtime environment is a crucial consideration, and it's worth noting that high-level language-based products are ideal for this (Donald, 2013).

Hardware systems: In many conditions, the hardware system is vulnerable. Different sorts of attacks/vulnerabilities exist:

a) Electromagnetic waveforms constitute a significant cause of attacks, becoming more common by the day.
b) Juice jacking is a mobile security issue that can occur in various situations. This might be used in public venues such as the bus, airlines, trains, and other places where people charge their phones. This type of incidence can occur in a variety of locations. In this circumstance, a variety of malevolent attacks could occur. In this case, the USB charger is mostly used for assault victims.

Malicious Software-based Vulnerability: When it comes to mobile devices, several types of vulnerabilities can be found in harmful Software. These days, smartphones are frequently used for internet purposes, and we are all aware that malware is a program that harms the system. According to a study, the virus strain has surged by 54 per cent in the recent past. In this category, worms and viruses are essential (Varshney,2000). Malicious assaults can be classified into three categories:

a) Infection of systems, which can be characterized as Explicit Permission, Implied Permission, Common Interaction, and No Interaction—all of this malicious Software is necessary to attack a mobile device.
b) The achievement of its purpose, which includes harming systems after installing malicious Software, is done through monetary damage, data and/or device damage, and hidden damage.
c) Another critical technique to make systems vulnerable is spreading malware to other systems. Wi-Fi, Bluetooth, and infrared, and remote networks such as phone calls, SMS, and emails, can be used to spread information.

2.4 Mobile Application

Mobile applications are defined as software/sets of programmes that function on a mobile device and assist users in completing their daily tasks. Nowadays, mobile applications rapidly grow, especially with the advancement of technology within the ICT industry. The criteria of mobile applications include easy, user-friendly, low cost and could run on mobile phones. The mobile application has various components of applications because of its extensive functionality, including calling, texting, browsing, chatting, social network communication, audio, video, and games, among others (Rashedul, 2010). In the year 2000, mobile application developers began discussing web-based mobile applications. People can use those mobile applications to connect to the internet for their daily needs. In some world places, such as EUA, the mobile sector is behind schedule. The mobile network in that part of the world was not very advanced. As a result, having high expectations for the mobile application from that section is a weird thing. (Rashedul, 2010).

However, if we consider Europe, where the world's largest mobile companies, such as Nokia, Ericsson, and others, have their headquarters, mobile innovation has emerged from that region. The fundamental issue is that such companies produce both cell phones and mobile applications for mobile operators. They may, however, slow things down. As a result, there was a disconnect between the developer and the consumer. It created a source of frustration for the developer, regardless of what they made, when it would arrive or whether it would ever arrive (Rashedul, 2010). Consider internet browsing, voice chat, Facebook, Twitter, and other forms of communication. Every ordinary cell phone now has a Facebook application. Users can share with their friends and family from any location, such as in a car or train. People can utilize messenger to communicate with one another. Using a VoIP program and the internet, we may make low-cost calls to any part of the world. Then we can discuss the GPS. The most common applications for GPS systems include locating current locations on a map, road navigation, and vehicle tracking. Google Maps assists us in finding any location.

We can view products, pick products, and place orders for products via mobile commerce. The mobile application Mobile Wallet is used to complete payments in some restaurants and markets. People can use mobile applications to do business. Another feature of the mobile application is mobile banking and eTicketing. We can sometimes use a smartphone application with an internet connection to control a home gadget from a distance. People are conducting business outside of the office. People can watch videos and movies directly from YouTube on their mobile devices. They have the ability to play both video and audio. Kids can play games on their phones, a type of mobile application.

The first usually contains malware sent to users via email attachments. The term "boot net" is a mix of the words "robot" and "network," and it usually refers to harmful activities. Here, attackers from the network can take control of the device and cause damage to the entire system. Spyware can be used to highjack a phone, listen in on calls, read text and content, and track the device's location using GPS. Backdoors can propagate malicious links on social networking sites for more excellent circulation. Malicious apps can be found on a variety of platforms. It can be used to obtain personal information or log into a system. The majority of these assailants are from various communities. Many of them are unethical hackers, while others are professionals who work for businesses or the military. There are numerous tools and defense mechanisms available for security management; however, the following are a few of the most significant:

2.5 Data Requirement

Data requirements consist of several main processes, including identifying, prioritizing, precisely formulating, and validating the data required to meet organization objectives. Data should be referred to in business terminology when establishing data requirements, if possible, using recognized standard business terms. If business terms for the data in scope have not yet been standardized and authorized, the data requirements process provides an opportunity to do so. Governance should be included in assessing data requirements for patient demographic data, with representation from supplying and consuming business areas throughout the life-cycle to ensure that their needs are met (Data operation, 2021).

The discovery and decomposition of data requirements should be made systematically and sequentially. The logical design of the destination datastore should be created in parallel with the business rules for system behaviour; this process is bi-directional and iterative. Data requirements should be reflected in the data store's logical design and should be consistent across projects.

Before populating the new data store with data that already exists elsewhere and will be migrated, profiling should be done to ensure that it fulfil the business expectations and requirements. This may positively impact the design process by highlighting the need for new quality rules or specifications, as well as increasing the proportion of criteria met and reducing rework for future releases.

Minimizing data complexity over time requires establishing and implementing solid processes for specifying data requirements. The following advantages will result from effectively applying this process:

a) Ascertains that informed people determine what data is required;
b) Increases the ability to communicate data within and outside of the organization;
c) Ensures that systems and data repositories have proactive data quality procedures in place;
d) Enhances the connection between data and business processes;
e) Enhances the business vocabulary, generates metadata assets, and establishes data ownership, governance, and lineage.

2.6 User Requirement

User requirements, also known as user needs, explain how a user interacts with a system, such as what tasks they must be able to complete. User needs are typically recorded using narrative prose in a User Requirements Document (URD). User requirements are usually signed off by the user and utilized as the primary source of information for developing system requirements. Determining what the user genuinely wants a software product to achieve is a crucial and challenging phase in the design process. This is due to the user's inability to articulate their entire set of needs and desires, as well as the fact that the information they supply may be incomplete, erroneous, or contradictory. The business analyst is in charge of adequately comprehending what the customer wants.

This is why user needs and system requirements are usually considered separately. The business analyst thoroughly evaluates user requirements before carefully constructing and documenting high-quality system requirements that meet specified quality characteristics. One sort of stakeholder need is user requirements (Geis, 2018). They serve as a foundation for system requirements from the perspective of the interactive system's user (Parker, 2012). To meet one or more user needs, user requirements outline what a user should be able to do and/or experience with the system in each specific context of use. User requirements were defined as enabling the design of a system that would allow users to attain high levels of usability, accessibility, user experience, and/or avoidance of harm from use (referred to as human-centred quality in ISO 9241-220).

Other sorts of criteria were included in the NIST Specification for Usability Requirements (NST,2007), in addition to the components of usability (effectiveness, efficiency, and satisfaction). These kinds of criteria are now referred to as "user requirements". Table 1 show the components in NIST Specification for Usability Requirements:

Table 1: NIST Specification for Usability Requirements

No.	Main Components	Sub-Component
1.	Design advice	a) Design principles b) Human factors and ergonomics c) Style guides d) Standards
2.	Usability features	a) Accessibility b) Understandability c) Learnability d) Operabilityity e) Attractiveness
3.	Content and functions	a) Functionality b) Content c) Complete, accurate, up-to-date, style d) Effectiveness (for learning) e) Trust f) Platform independence

2.7 A previous study on Mobile Security Application

Miriyala et al. (2016) used the android OS to develop a mobile security application to protect women who face social harassment and violence in India. The system was systematically designed to function with hardware wearable gadgets such as wrist bands and spectacles. Although the mobile application proved to be a success in India, its success could be traced to the fact that the mobile application was developed to address the specific security and safety concern, which is rape and harassment. Implementing this application in another society would be a great idea; however, its success would depend on the prevalence of rape and sexual harassment.

Yarrabothu & Thota (2015) developed "Abhaya": An Android App for women's safety. This app was developed in Delhi, India. The application works remotely by enabling users (not necessarily women) to input four different emergency contacts that would be reached in potential danger scenarios. In place of danger or emergency, the user can turn on the application, and with a single click, the app will be activated. It would begin sending emergency alerts to the registered contacts on the app while simultaneously calling the first registered number on the application. The location URL of the victim is sent to the emergency contacts at an interval of 5 minutes until it is disabled by the victim; this is to enable emergency contacts to know the location update of the potential victim in case of movements. As of its success, the mobile app did prevail in that society, seeing that the insecurity targeted towards women was particularly identified and added as a security parameter in the Mobile application.

Saigh et al. (2015) developed a Personal Safety Mobile Notification System to help users in emergency and dangerous situations. The application was developed and patented in the United States with extensions to Canada also, which means that the application is made available to the user from the US and Canada only. Like many other security apps, this personal safety mobile Notification system uses GPS and SMS alerts to send emergency alerts to friends and loved ones of victims. The system does not have any hardware components. Emergency alerts are only sent when the victim of a potentially dangerous situation turns on the app and taps an emergency button.

3 PROPOSED FRAMEWORK OF DATA AND USER REQUIREMENTS FOR SAFETY AND SECURITY OF MOBILE APPLICATION

In assessing the previous study on the data and user requirements, the proposed framework on data and user requirements has been identified and constructed. After careful assessment based on the Malaysian environment, these data and user requirements have been taken. Several variables have been identified in constructing the framework on data and user requirements consisting of data requirements, user requirements, and components of safety and security for mobile applications.

Data Requirement

Data requirement will contribute to the creation and validation of core business definition and term that includes the metadata, data standard, and business process. The component shows the data required for the security and safety application for the smartphone consisting of business terminology, resident demographic data, consuming business process, profiling, data repositories, and safety and security processes. This requirement must be included in the safety and security mobile application to ensure the application will collect the right and appropriate application for the safety and security of the resident.

The business terminology means the elements refer to the data elements within your field. In contrast, resident demographic data refer to the process of creating the data, such as resident registration information. At the same time, consuming business processes related to the operation or processes that use data (Office of National Coordinator for Health Information Technology, n.d). While data repositories will collect all the resident data and store it in the data archive. This is important to ensure the location's history will be stored within the data archive. While profiling residents will also be kept in the data repositories, this application will record any information and data related to the resident's knowledge. It will be held in the data repositories. The safety and security process will be collected, particularly on the confidential information associated with the resident. These components have been taken from the previous studies discussed earlier to make sure the component that will be developed is equivalent to the data requirement required by the user of this safety and security mobile application.

User Requirement

In terms of user requirements, NIST Specification for Usability Requirements has been adopted in identifying the user requirement for the resident's security and safety for the smartphone. There are three main components of user requirements consist of design advice, usability feature and content and function. The first component that has been mentioned is design advice. The design advice refers to the design principle, ergonomic criteria, style guide and standards. The design principle will follow the user's requirement to ensure the application is easy to use and valuable without any complex feature that hinders the user from using that software. Besides that, the ergonomic feature is important to ensure those applications will never have a health effect on the user itself.

In terms of usability features, those applications should be accessible easily, understandable as well as attractive. The attractive component in the mobile application will attract the user's interest to use it. Last but not least, the component of user requirements in mobile applications for residents' safety and security are content and function. The content and function of the application should be straightforward; for example, the emergency button should be designed and placed on the areas for victims easily click on it to begin sending emergency alerts to the registered contacts on the app.

Security and Safety Mobile Application

The mobile application will secure the resident in terms of security and safety within the area of their living or workplace. These security and safety mobile applications should consist of several components: confidentiality, integrity, authentication, authorization, availability, and no-repudiation (Yusop et al., 2014). This security mobile application aspect is used to ensure the high quality of the software is developed by the developer. Besides that, it also secures the confidential data and information in this application to make sure the resident's personal information will not leak to others.

The first aspect that needs to highlight in the safety and security mobile application is confidentiality. Thus, the data requirement that has been collected consisting of detailed information on the resident, including their identification card (IC), address, telephone number and other required information, should be kept appropriately. The high security of the mobile application is necessary to make sure the integrity and authentication of the application are preserved. This mobile application requires high security because it requires authorization from the user when they want to access it. Besides that, this application is only available to the user who registers. This application also provides the feature that will prove the origin, authenticity, and integrity of data within the application (Awati, 2021).

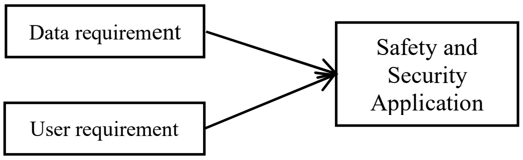

Figure 1: Proposed Conceptual Framework

The proposed framework of data and user requirement application for the smartphone will be assessed and evaluated based on the Malaysian environment among residents to explore the perception of Malaysian towards security and safety mobile applications that existed in this country. The result will be different based on the type of the safety and security mobile application that has been developed like in Bangladesh, where the android technology is a solution for the safety of women (Hossain et al., 2019). While, India has developed the Safetipin mobile application as a personal location guide for public places using the Global Positioning System for the safety of females (Manazir, Govind and Rubina, 2019). While it contradicts Mata et al. (2016), which has developed a mobile application for the Mexico city's residents to provide safe routes based on crowd-sensed crime data and this mobile application does not focus on the women but the whole city's residents. Thus, the proposed framework will focus on Malaysia because based on different country has different kind of criminal occur; therefore, it is necessary to develop the safety and security of mobile application based on the appropriate environment of that country.

4. CONCLUSION

In conclusion, this paper discussed the data and user requirements on security and safety mobile applications for safeguarding the community nowadays. The comprehensive overview purposely explores the significance of data and user requirements of the security and safety mobile application. The supporting evidence from the previous study has been researched and investigated to know the actual security and safety of mobile application situations. Various countries started to develop this kind of mobile application to protect women and risk groups of the community from a crime or other harmful situation in their daily lives. This kind of mobile application could be a platform for people to avoid any danger around them. Other than that, this application should be linked with other authorities such as police, fireman or any other agency that could help safeguard the community from danger.

Malaysia's government should force certain agencies to develop the security and safety mobile application to protect the community from emergencies and dangerous situations. The security and safety mobile application required to develop should follow the data and user requirements from the user's perspective rather than the developer. The user-friendly and easy mobile application will assist the community in overcoming any emergency or dangerous situation getting worse. The police or authorities quickly get informed by the apps related to the emergency reported by the community and take action more quickly. Thus, this security and safety mobile application are essential to develop, mainly to protect the society, either rural or city.

ACKNOWLEDGEMENT

This paper is funded by *Geran Dalaman Fakulti Pengurusan Maklumat*, Universiti Teknologi Mara (UITM). Reference Number: 600-TNCPI 5/3/DDF (FPM) (006/2020)

REFERENCES:

[1] ANSI/ASSE. (2011). Prevention through design: Guidelines for addressing occupational hazards and risks in design and redesign processes. (ANSI/ASSE Z590.3-2011). Des Plaines, IL: Author.

[2] ASSE. (2015). Dictionary of terms used in the safety profession. Safety, Health and Environmental Body of Knowledge. ASSE. Retrieved from www.safetybok.org/ resources/dictionary_of_terms

[3] Bin, M., & Soh, C. (2012). Crime and Urbanization: Revisited Malaysian Case-review under responsibility of Centre for Environment-Behaviour Studies (cE-Bs), Faculty of Architecture, Planning & Surveying, Universiti Teknologi MARA, Malaysia. Procedia-Social and Behavioral Sciences, 42, 291–299. https://doi.org/10.1016/j.sbspro.2012.04.193

[4] Bird, F.E., Germain, G.L. & Clark, M.D. (2003). Practical loss control leadership (3rd ed.). Duluth, GA: Det Norske Veritas.

[5] Canadian Society of Safety Engineering (CSSE). (2015). Hiring a health and safety practitioner: A guide for employers and OH&S practitioners. Toronto, Canada: Author. Computer, 33(10), 32-38..

[6] CyberSecurity Malaysia (2019). "Reported Incidents based on General Incident Classification Statistics 2019," (November 25,

2019). Retrieved from https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=733c3a52-bcb1-43e5-8bee-03837a0ccf16.

[7] Data requirements definition. (2020, September 14). The Office of National Coordinator for Health Information Technology. https://www.healthit.gov/playbook/pddq-framework/data-operations/data-requirements-definition/

[8] de Winter, J. C. F., Dodou, D., & Wieringa, P. A. (2009). Exploratory factor analysis with small sample sizes. Multivariate Behavioral Research, 44(2), 147–181. https://doi.org/10.1080/00273170902794206

[9] Dekker, S. (2015). Safety differently: Human factors for a new era (2nd ed.). New York, NY: CRC Press, Taylor & Francis Group.

[10] Donald, A. C., Oli, S. A., & Arockiam, L. (2013). Mobile cloud security issues and challenges: A perspective. International Journal of Engineering and Innovative Technology, 3(1), 401.

[11] Geis, T, Polkehn K.: Praxiswissen User Requirements - Nutzungsqualität systematisch, nachhaltig und agil in die Produktentwicklung integrieren, dpunkt.verlag Heidelberg Germany (2018).

[12] Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017,May). Security and privacy issues for an IoT based smart home. In 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1292-1297). IEEE.

[13] Hollnagel, E. (2014). Safety-I and Safety-II: The past and future of safety management. Burlington, VT: Ashgate Publishing Co.

[14] Islam, Dr MD Rashedul & Mazumder, Tridib. (2010). Mobile application and its global impact. International Journal of Engineering & Technology. 10. 72-78.

[15] Intellpost website (2020). Secondary Data: Advantages, Disadvantages, Sources, Types. Retrieved September 2021, from: https://www.intellspot.com/secondary-data/

[16] Kirkpatrick, J., & Kirkpatrick, W. K. (2009). A Kirkpatrick White Paper. Retrieved from http://www.kirkpatrickpartners.com/Portals/0/ Resources/White Papers/Kirkpatrick Four Levels white paper 2012.pdf

[17] Malay Mail. (2013). Selangor cops to add 1,000 CCTV cameras statewide next year, says IGP | Malaysia | Malay Mail. Retrieved from https://www.malaymail.com/news/malaysia/2013/12/13/selangor-cops-to-add-1000-cctv-cameras-statewide-next-year-says-igp/581279

[18] Mat, Bakri & Mohamed Pero, Siti Darwinda & Wahid, Ratnaria & Shuib, Md. Shukri. (2020). Cyber Security Threats to Malaysia: A Small State Security Discourse.

[19] Maurice, Pierre & Lavoie, Michel & Laflamme, Lucie & Svanström, Leif & Romer, Claude & Anderson, Ragnar. (2001). Safety and safety promotion: Definitions for operational developments. Injury Control and Safety Promotion. 8. 237-240. 10.1076/icsp.8.4.237.3331.

[20] Möller, N., Hansson, S.O. & Peterson, M. (2006). Safety is more than the antonym of risk. Journal of Applied Philosophy, 23(4), 419-432. doi:10.1111/j.1468-5930 .2006.00345.x

[21] Montante, W.M. (2008). The essence of Safety: Do you really know safety. Safety 2008 Professional Development Conference Proceedings (Session 684). Des Plaines, IL: ASSE

[22] NIST: Common Industry Specification for Usability—Requirements. (2007) https://www.nist.gov/itl/iad/iusr-papers-and-publications, last accessed August 2021.

[23] Nkosi, M. T., & Mekuria, F. (2010, November). Cloud computing for enhanced mobile health applications. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (pp. 629-633). IEEE.

[24] NSC. (2009). Accident prevention manual for business and industry, engineering and technology (13th ed.). Itasca, IL: Author.

[25] Parker, J. (2012, August 18). Business, User, and System Requirements. Enfocus Solution. https://enfocussolutions.com/business-user-and-system-requirements/

[26] Paul, P.K. & Aithal, Sreeramana. (2019). Mobile Applications Security: An Overview and Current Trend. 10.5281/zenodo.3516738.

[27] Reason, J. (2000). Safety paradoxes and safety culture. Injury Control and Safety Promotion, 7(1), 3-14. doi:10.1076/1566-0974(200003)7:1;1-v;ft003

[28] Sklet, S. (2006). Safety barriers: Definition, classification and performance. Journal of Loss Prevention in the Process Industries, 19(5), 494-506. doi:10.1016/j.jlp.2005 .12.004

[29] Uma Sekaran (2003). Research Method for Business: A skill building approach. United States of America: John Wiley & Sons, Inc.

[30] Varshney, U., Vetter, R. J., & Kalakota, R. (2000). Mobile commerce: A new frontier.

[31] Yusop, N., Kamalrudin, M., Sakinah, S., & Sidek, S. (2014). Validation Of Security Requirements For Mobile Application: A Study. Science International, 26(4), pp 1451 - 1454.

[32] Office of National Coordinator for Health Information Technology (n.d). Data Operation: Data requirement definition. Retrieved May 2022, from: https://www.healthit.gov/playbook/pddq-framework/data-operations/data-requirements-definition/

[33] Awati, R. (2021). Non repudiation. Techtarget website Retrieved May, 2022, from: https://www.techtarget.com/searchsecurity/definition/nonrepudiation

[34] Hossain, M. E., Rahman, M. W., Islam, M. T., & Hossain, M. S. (2019). Manifesting a mobile application on safety which ascertains women salus in Bangladesh. International Journal of Electrical and Computer Engineering, 9(5), 4355.

[35] Manazir, S. H., Govind, M., & Rubina. (2019). My Safetipin Mobile Phone Application: Case Study of E-Participation Platform for Women Safety in India. J. Sci. Res., 8(1), 47-53.