Security and privacy awareness of smartphone users in Indonesia

M Amin¹, Tasmil¹, Herman¹, Bahrawi¹, N Alam¹, D F Dhahir¹ and Y D Hadiyat¹

¹ BBPSDMP Kominfo Makassar, Ministry of Communication and Information Technology, Republic of Indonesia, Prof. Abdurrahman Basalamah street 25, Makassar, Indonesia

E-mail: mukhlis.amin@kominfo.go.id

Abstract. The number of smartphone users in Indonesia is increasing every year and has been growing rapidly since Covid-19 hit Indonesia. Smartphones store a lot of personal and information data, such as photos, videos, contact lists, e-mails to social media accounts. A large amount of personal data on smartphones causes an increasing number of threats to information security and privacy. This study aims to measure the knowledge and level of awareness of smartphone users in Indonesia on information security and privacy. This study modifies the existing measurement methods. The results showed that there are still many Indonesians do not know the information security and privacy on their smartphones. The results also show that the level of information security awareness among Indonesians is still low.

1. Introduction

Smartphone technology continues to increase every year, especially after Covid-19 strikes. The number of smartphone users is increasing along with the implementation of learning from home [1]. Of the total 272.1 million population of Indonesia, internet users reach 175.4 million. Interestingly, the number of connected smartphones reached 338.2 million units, almost double the number of internet users. This means that almost Indonesian people have more than one smartphone. Meanwhile, the number of social media users has reached 160 million [2]. Apart from phone calls and SMS, smartphones also provide internet services, data sharing, life support applications, games etc. Smartphones also allow us to store various data, documents, photos and videos. This can increase security and privacy risks.

Nowadays, almost all human activities are connected to the internet, therefore security and privacy awareness are very important. Several studies have shown that smartphone users have done the right thing in keeping their smartphone safe. User has used authentication such as different pattern usage, fingerprint password, face password, pin password, etc. [3,4,5]. This is not sufficient to protect us from security related problems [6]. Smartphones are devices that can store various information including personal information. Users must ensure the safety of each other's personal information. They often neglect to protect personal information due to a lack of awareness, whereas if that information falls into bad hands, there will be problems.

Recent studies show that the total number of applications downloaded in the first quarter of 2020 was 31.5 billion globally. Of these, 22.5 billion came from the Google Play Store and 9 billion from
the Apple App Store. This number increased 20% compared to the same period the previous year [7].

Another study released that more than 29,000 malicious Android applications circulated in the first quarter of 2020. That number is up dramatically from the range of 14,500 malicious applications recorded in the same period last year. Nine out of ten malicious applications at the top had stopped at the Android Play Store application store. This means that they can penetrate the Play Store security system, which should be able to filter out malicious programs. According to newly available data, Indonesia, has seen dramatic spikes in fraudulent activity. Of the 161 million transactions in Indonesia that were processed, more than 157 million of them were blocked as fraud [8].

This paper discusses the results of an information security and privacy awareness survey of smartphone users in Indonesia. This study aims to measure the level of awareness of information security and privacy of smartphone users. Several previous studies have discussed information security awareness in Indonesia [9-12]. However, all of them specifically discussed information security awareness among teenager. In addition, all of them only use descriptive analysis to show the level of information security. Neither one has proposed a method of measuring information security awareness. Likewise, what was done in Budapest [13]. Previously, we have also conducted research on information security and privacy among civil servants in Makassar. We use Multi Criteria Decision Analysis (MCDA) to measure the level of information awareness [14] by adopting a prototype of the information security awareness measurement proposed by Krugger & Kearney [15].

In 2019, Noor [12] propose a method of measuring security awareness and privacy of smartphone users. The study conducted a security and privacy awareness survey among college students and proposed a method of measuring the level of awareness. It uses previous research results that divided attacks on smartphones into old attacks and new attacks [17]. They compiled question related to security and privacy based on the attack. Similar to computers, smartphones also have same challenges. Security and privacy-related threats on smartphones are divided into four [16] including: Data protection and privacy [17,18], Attacks [19,20] Authorization [21], and Vulnerabilities [22].

Next, we refer to Noor method as the existing method. In our research, we measured the level of security and privacy awareness of smartphone users in Indonesia using the modified existing method. An explanation of the existing method and its modifications is discussed in the next section. Then proceed with a discussion of the results of the security and privacy awareness survey and the measurement results, then close with a conclusion.

2. Method

The purpose of this study is to measure how much security and privacy awareness of smartphone users. Data collection is carried out through a user survey. This method is most commonly used for research activities, but this process takes a long time to complete [23]. In fact, it is expensive, especially if the survey coverage area is very large. The use of technology in collecting data by survey can be used to overcome this problem [24], it can even be used to analyze data automatically (e.g. Google forms). Online data collection is a very popular to use in many researches [25].

In this study, we prepared a questionnaire using Google Form, then collected data using the crowdsourcing method [26]. We invite smartphone users in Indonesia aged 12 years and over to fill out questionnaires by distributing links via Facebook, Whatsapp, Telegram and SMS.

We compiled a questionnaire based on a modified method design. The existing methods raise several questions regarding security and privacy. However, it only took the six questions that were most influential. They formulate easy-to-understand question sentences in simple language. We have modified the existing methods in several sections. the first is that we changed the first question (Q1: For what purpose do you use Smartphone?) because almost all smartphone users today use it for activities other than communicating so this question will potentially result in unsafe answer choices. We replace this question with the question: "Do you save some information on your smartphone (perhaps as a reminder or for personal consumption)?". This question also has the potential to be answered by smartphone users who do not use it to access internet applications. We changed some of the question redaction to make it easier to understand.
We also add one question related to security (Q7) although the addition of the question is not that significant in calculating the level of awareness using Equation 1. However, this question will show the actions of the user in securing their smartphone. A list of modified questions is presented in Table 1. This table also shows the modifications to the unsafe options section. We change and added some of the possible options, then gave a weight to each option. The weight given will be the Q value for each question. For questions that have more than 1 selectable answers, the Q value is the accumulation of each weight. This differs from the existing method, where the weight of all unsafe options is 1.

| Question                                                                 | Safe option                          | Unsafe option                                                                 |
|-------------------------------------------------------------------------|--------------------------------------|------------------------------------------------------------------------------|
| Q1 Do you save the following information on your smartphone (perhaps as a reminder or for personal consumption) | Nothing (0)                          | Personal identity (0,25) Financial App username & pass (0,25) Non-Financial App username & pass (0,25) |
| Q2 Do you log out your personal accounts (e.g. Email, Facebook, Etc.) after assessing it via Smartphone? | Always (0)                           | Never (1); Rarely (0,75); Sometimes (0,5); Often(0,25)                      |
| Q3 Do you ever installed an unknown sources or third party applications in your smartphone? | No (0)                               | Yes (1)                                                                      |
| Q4 Did you read the application provider’s privacy and policy before installing application? | Always (0)                           | Never (1); Rarely (0,75); Sometimes (0,5); Often (0,25)                     |
| Q5 Did you ever read the Application’s Phone Access Permissions before installing application? | Always (0)                           | Never (1); Rarely (0,75); Sometimes (0,5); Often (0,25)                     |
| Q6 What type of screen locks do you use for Security?                   | Pin Code/Password/Pattern/Fingerprint (0) | Nothing (1)                                                                  |
| Q7 What type of locks do you use for applications?                      | Pin Code/Password/Pattern/Fingerprint (0) | Nothing (1)                                                                  |

The calculation of the level of awareness in our study uses the same equation as the existing methods, as follow as:

\[
LoA = 1 - \left( \frac{2}{1 + e^{-\varphi}} - 1 \right)
\]  

(1)

where Q is the sum of all Q values for each question. By using this equation, the LoA will be 0 - 1. By using this equation, the LoA will be 0 - 1. If the user chooses all safe answers for all questions, then the LoA is 100%, and if the user chooses all unsafe answers with the highest weight, then the LoA will be close to 0%.

3. Result and Discussion

We have distributed the questionnaire links via SMS and the internet such as Facebook, WhatsApp and Telegram. There are 540 smartphone users in Indonesia filled out the questionnaire. The total number of respondents is almost equal between men and women. The majority of respondents are adults (57%), then teenager (33%) and the rest were elderly people. About 52% of responses are diploma and bachelor graduates. 28.5% are masters and doctorates, and the rest are high school graduates. Our responses come from all over Indonesia. Most came from Sulawesi (46%), then Java (32%), Bali and Nusa Tenggara (8%), and a small proportion came from Kalimantan, Sumatra, Papua and Maluku. We have processed the user's answers to the questions previously discussed. The answers to the questions of this research will be discussed one by one. It is important to know the user's awareness in detail.
3.1. Answer to research question

3.1.1. The purpose of using smartphone. Currently, smartphones can perform various activities on computers such as email, location tracking, photo and video storage, photo and video processing, internet access such as browsing, social media, e-commerce, etc. The question (according to Q1 on existing method) is about the intended use of the smartphone. This is to find out how many people are using each of these services on their smartphone. Figure 1 shows the response to this question, only 1.1% of users use smartphones only for calling and texting. This user is quite safe compared to 99% of people who use smartphones for other activities, especially the internet.

3.1.2. Saving some information on smartphone. Like a computer, a smartphone can also store various information such as contact lists, notes, documents, photos and videos. Even if you are not connected to the internet, all this information can be stored on your smartphone. Q1 is about what information is stored by respondents on their smartphones. Figure 2 shows that around 57% of respondents save their financial application accounts and passwords on their smartphones. 56% of respondents admitted to storing their personal identities, 39% storing accounts and passwords for non-financial applications, and 30% storing personal photos and videos on their smartphones. This shows that they are less secure than the other 24% of respondents who do not store any information on their smartphone.

![Figure 1. The purpose of using smartphone.](image1)

![Figure 2. Number of respondents who save information on their smartphone.](image2)
3.1.3. Log out from personal accounts. As previously discussed, smartphone provides various internet facilities such as email, cloud, social media, etc. All of these services can be accessed via smartphone. Not only through the browser, all of these services already have applications that can be installed on smartphones. There are a lot of personal information in this application that is very important to us and we must keep it safe. But most of us, access personal accounts (eg. Email, Facebook, Google drive, etc.) and leave them connected. For example, a person loses his smartphone and if a personal account is logged into the smartphone, he may lose his personal information. Q2 is about whether they always sign out from their personal accounts when using a smartphone. This question is to reveal how many people are aware of their security and privacy. Figure 3 shows that 65.5% of people are not aware of this problem.

3.1.4. Install third party applications. Third-party applications are defined as applications that are developed by other parties, not genuine from certain device manufacturers. Apps made by other developers may be able to run on smartphones made by different developers. Usually, these applications can be downloaded through the Play Store or App Store. Sometimes, third-party applications are also unknown. We may get it via e-mail, instant message or advertisements listed on an internet page.

Figure 3. Number of respondents who usually sign out from personal account when using it with smartphone.

Figure 4. Number of respondents who ever install third party application from unknown source.
Third party applications may contain more malware than system applications. That is why, third party applications are less secure than system applications. In our survey results for the Q3 question in Fig. 4, we know that 47% users installed third-party applications from unknown sources. They are less secure than 52% others.

3.1.5. Read application provider’s privacy and policy. Before installing an application, providers provide their privacy and policies. This privacy and policy contains policies regarding access to user information. For example, an application has policies for accessing contact information and an address book. By reading the privacy policy, users can find out what information that can be accessed by application and what it is used for. Users can also find out what information can and cannot be hidden.

Figure 5 show the number of respondents who usually read application provider’s privacy and policy. About 17% respondents said that they always read application provider’s privacy and policy before installing the application. This means that only a small proportion of Indonesians are aware of the importance of reading providers’ privacy and policies regarding their personal information.

![Figure 5](image1.png)

**Figure 5.** Number of respondents who usually read application provider’s privacy and policy.

![Figure 6](image2.png)

**Figure 6.** Number of respondents who usually read through application’s access permission.
3.1.6. Read the application’s phone access permissions. Smartphone technology is growing from year to year. As discussed earlier, Smartphones can store a variety of our personal information such as photos and videos, documents, message conversations and other important information. Before the user installs the application, the application provider shows the permission request to access the phone application. Phone app access permission means what information on the smartphone is accessed by the app. A user should always read the app's phone access permissions carefully.

Figure 6 show the number of respondents who usually read through application’s access permission before installing the application. 30.56% respondents said that they always read through application’s access permission before installing the application and only 4.8% respondent never read that access permission. The rest, rarely, sometimes, and often read them before installing.

![Figure 7. Number of users using authentication system](image)

![Figure 8. Number of users using lock for application](image)

3.1.7. Using screen locks. Authentication is a very important thing on a smartphone. Without authentication, smartphones can pose a big problem. For example, someone gets your cellphone in a short time, if he doesn't know your smartphone's authentication system, he won't be able to unlock your smartphone. So, He can't access any information from your smartphone.
There are many authentication systems for smartphones such as: pin code, password, pattern, fingerprint, etc. Figure 7 shows the percentage of people who do not use the authentication system as well as the percentage of the authentication system used by smartphone users. Only 8.52% of people do not use the authentication system on their smartphone. By the number of people who use the authentication system, fingerprint is the most widely used authentication system (27%).

3.1.8. Locks for applications. Some of the applications installed on the smartphone may be very important and contain various confidential information. To secure this application from being accessed by other people who might get our smartphone, we need to lock the application. The lock is the same as an authentication system. Figure 8 shows the types of locks used by smartphone users in Indonesia. About 11.5% of people do not use any locks for private and confidential application. Based on respondents' answers, fingerprints, pin codes, and passwords are mostly used to lock applications.

3.2. Level of awarenesses
We have compiled the answers of smartphone users in Indonesia to questions related to security and privacy. The results we have described in the previous section. As we have said that we continue to ask the existing questions on the existing methods that we have eliminated and replaced with another question (Q1). thus, we can still calculate the Level of Awareness (LoA) based on the existing methods.

We calculate the answers from smartphone users using Equation (1). The calculation result is shown in the graph in Figure 9. The average LoA of smartphone users in Indonesia is shown in Figure 10. The red line and bar represents the calculation result using the existing method, while the blue line and bar shows the calculation using the modified method.

We can see in figure 9 that the calculation using the modified method produces more variety LoA compared to the existing methods. The existing method only produces 6 LoA while the modified method produces 22 different LoAs. With the modification method, the average LoA is higher than the existing methods. With the existing method, the average LoA is 17%, while with the modified method, the average LoA is 23%.

4. Conclusion
This research aims to described the security and privacy awareness of smartphone users in Indonesia and to measured their level of security and privacy using the modified of existing method. Based on the results previously described, we can conclude that most of Indonesians citizen are not aware about security and privacy on using smartphone, level of security and privacy awareness among Indonesians is still low. Secondly, our modification provides a more variable Level of Awareness than
the existing methods. With the existing method, the average LoA is 17%, while with the modified method, the average LoA is 23%.

References
[1] Alfarizi MK 2020 Belajar dari rumah, penjualan smartphone entry-level diperkirakan meningkat teknolo.tempo.co/read/1379758
[2] Suud YA 2020 Digital 2020: pengguna internet indonesia dalam angka cyberthreat.id/read/5387
[3] Roesner F, Kohno T, and Molnar D 2014 Security and privacy for augmented reality systems Commun ACM 57 88–96
[4] Chin E, Felt AP, Sekar V, and Wagner D 2012 Measuring user confidence in smartphone security and privacy Proc Eighth Symp Usable Priv Secur SOUPS
[5] Jones B, and Heinrichs L R 2012 Do business students practice smartphone security? J Comput Inf Syst 12(2) 22-30
[6] Yildirim N, Das R, and Varol A 2014 A research on software security vulnerabilities of new generation smart mobile phones 2nd International Symposium on Digital Forensics and Security (ISDFS’14) 12-13 May, Houston, TX
[7] Maulana A 2020 Hikmah corona, pendapatan app store dan play store meningkat teknologue.id/hikmah-corona-pendapatan-app-store-dan-play-store-meningkat/amp
[8] Upstream 2020 Upstream’s secure-d detects malware spike in Q1 2020 with 29,000 malicious android apps at play, double 2019 figures upstreamsystems.com/upstreams-secure-d-detects-malware-spike-q1-2020-29000-malicious-android-apps-play-double-2019-figures
[9] Sari P K, and Candiwan C 2014 Measuring information security awareness of Indonesian smartphone users Telecommunication Comput Electron Control 12(2) 493–500
[10] Sari P K, and Sihotang F S 2016 Measurement of information security awareness among Facebook users in Indonesia Asia Pacific J Contemp Educ Commun Technol 2
[11] Abd Rahim N H, Hamid S, and Mat Kiah M L 2019 Enhancement of Cybersecurity Awareness Program on Personal Data Protection among Youngsters in Malaysia: An Assessment Malaysian J Comput Sci 32
[12] Noor T H, Zeadally S, Alfazi A, and Sheng Q Z 2018 Mobile cloud computing: Challenges and future research directions J Netw Comput Appl 115 70–85
[13] Androulidakis I, and Kandus G 2011 Mobile phone security awareness and practices of students in Budapest Int Conf Digit Telecommun 2011 18-24
[14] Amin M 2014 Information security awareness level measurement using multiple criteria decision analysis J Penelit dan Pengemb Komun dan Inform 5 15–24
[15] Kruger H A, Kearney W D 2006 A prototype for assessing information security awareness Comput Secur 25(4) 289–296
[16] Zaidi S F A, Shah M A, Kamran M, Javaid Q, and Zhang S 2016 A survey on security for smartphone device J Ind Adv Comput Sci Appl 7(4) 206-219
[17] Muslukhov I, Boschma Y, Kuo C, Lester J, and Beznosov K 2012 understanding users’ requirements for data protection in smartphones IEEE 28th Int Conf Data Eng Work 228–35
[18] Muslukhov I 2012 Survey: Data Protection in Smartphones Against Physical Threats (The University of British Columbia: Department of Electrical and Computer Engineering)
[19] Khouzani M H R, Sarkar S, and Altman E 2012 maximum damage malware attack in mobile wireless networks Proceedings: IEEE INFOCOM 20(5) 1347 1-9
[20] Peng S C 2012 A survey on malware containment models in smartphones Appl Mech Mater. 263–266 3005–3011
[21] Goodin D 2016 Malicious apps in Google Play made unauthorized downloads, sought root Ars Technica
[22] Kataria A, Anjali T, and Venkat R 2014 Quantifying smartphone vulnerabilities Int Conf SPIN 645–649
[23] Umar S, Phrommathed P 2005 Research Methodology (New York: Springer US)
[24] Couper M P 2005 Technology trends in survey data collection Soc Sci Comput Rev 23 486–501
[25] Granello D H, and Wheaton J E 2004 Online data collection: strategies for research J Couns Dev 82 387–393

[26] Zheng F, Tao R, Maier H R, See L, Savic D, and Zhang T 2018 Crowdsourcing methods for data collection in geophysics: state of the art, issues, and future directions Rev Geophys 56 698–740

Acknowledgement
We would like to thank all those who helped us distribute and complete this research questionnaire. We also thank Center for Human Resources Development and Communication and Information Technology Research Makassar, for facilitating this research.