Security and Privacy Awareness: A Survey for Smartphone User

Md. Nawab Yousuf Ali[1], Md. Lizur Rahman[2], Ifrat Jahan[3]
Department of Computer Science & Engineering
East West University, Dhaka 1212
Bangladesh

***Abstract*—Smartphone becomes one of the most popular devices in last few years due to the integration of powerful technologies in it. Now-a-days a smartphone can provide different services as like as a computer provides. Smartphone holds our important personal information such as photos and videos, SMS, email, contact list, social media accounts etc. Therefore, the number of security and privacy related threats are also increasing relatively. Our research aims at evaluating how much the smartphone users are aware about their security and privacy. In this study, firstly we have taken a survey for smartphone users to access the level of smartphone security awareness displayed by the public. We also determine whether a general level of security complacency exists among smartphone users and measure the awareness of android users regarding their privacy. From survey result we have found that, most of the people are not aware about their smartphone security and privacy. Secondly, based on survey results, we have shown a method to measure the level of awareness (LOA) for the smartphone users. By using this method, a user can easily measure his/her smartphone security and privacy related level of awareness.**

Keywords—Smartphone; Smartphone Problems; Level of Awareness (LoA); Security and Privacy

I. INTRODUCTION

The technologies of smartphone have been increasing with a huge rate over last few years. Smartphone provides many services as data sharing, phone calls, internet, different online & offline games etc. Therefore, it increases the chance of security and privacy related threats comparatively. Almost 80% of activities related to the internet, so it is important for us to become aware about security and privacy. Several recent studies shown that, when security comes to smartphone, most of the smartphone users are propitious [1, 2, 3]. In order to authentication of smartphone, people often use different patterns, finger print password, face password, pin passwords etc. All these are not enough to protect us from security related issues [4]. Smartphones are handhold device where different personal information are stored. We have to ensure the security of our personal information. Most of the time, due to lack of our awareness we fail to protect our personal information. If all this information falls into a bad hand, we might be in trouble.

According to a recent study, Google play published more than 3.5 million apps from 2009 to December, 2017 [5]. The number of apps is rapidly increasing over recent few years. Another recent security study showed that, in Google play store, more than 200 malevolent apps were found [6]. These apps collected private information like contact numbers, places etc. from users and sent to the attackers' server. Time to time this information was resending to the attackers' server when users use these apps. In the early 2016, Google banned 13 apps from Google play store because, these apps collected information from users and sell to other server [7].

In this paper, we discuss about results of a security and privacy awareness survey for the smartphone users. The research aims at evaluating how much the smartphone users are aware about their security and privacy. In this survey, we create questionnaire to access the level of smartphone security awareness displayed by the public. We determine whether a general level of security complacency exists amongst smartphone users and based on these result we show a statics model to measure the awareness of android users regarding their privacy.

This paper is organized as follows. We start with a discussion of the various previous related works in Section II. Then we explain about the smartphone problems in Section III and discuss different types of attacks in smartphone. In Section IV, we focus on our research methodology along with pilot study, research instrument and target population, and data analysis. In Section V, we analyze the result of our survey including research questions, evolution of research question and then propose a model that can measure the level of awareness. Finally, we show some concluding remarks and future direction in Section VI.

II. PREVIOUS WORK

Benenson et al. [8] pointed that IT security plays an important role while someone use smartphone, because of its' broadly acknowledged and well documented feature, which mainly focused on the technical area of a smartphone security system. According to their interview of 24 users on IT security of smartphone, they found the role of user. Based on this result they consecrated five hypotheses and proposed a mental technique after evaluation of these hypotheses.

A recent study in South Africa by Ophoff & Robinson [9] shown that the level of awareness on smartphone security based on public users and determined how much a common security level exists in smartpnone users. According to their survey on smartphone security awareness, they examined 619 South African smartphone users based on the trust of smartphone apps and other third party apps. They found that users showing high level of trust on smartphone apps, rather than when they install other third party apps. In this study, they used an updated version of model developed by Mylonas et al. [10].

Alani [11] noted that android smartphone privacy awareness concern grow with spread in users' perspective. A huge number of apps are downloaded daily by the users, but it is really difficult to differentiate between good terms of service security apps and bad terms of service security apps. In this paper, authors shown a result based on a survey of 4027 android smartphone users for android user security awareness. According to their survey, they tried to show the interactions between users and terms and service security while they install apps.

In a recent study by Mylonas et al. [10] pointed out that when a user installs different third party apps from official apps store-house (e.g., Play store, Google play, Apple's app stores etc.), the risk of smartphone security may increase because sometimes the protected information might be accessed by third party apps. According to their survey, they tried to find out whether users aware about their security of smartphone while they downloaded and installed apps form apps store house. Based on their survey, they developed a model that can identify these users who trust apps storehouse.

Zaidi et al. [12] pointed that due to the advanced technologies, smartphone has become a daily necessary component, and also the chance of security based attacks has increased. In this study, authors' discussed about the different threats in smartphone, security based attacks in smartphone and also the solutions to solve these problems. New attack and old attack are the two types of security-based attacks. According to this study, authors provide a simple view of various smartphone security related attacks, and also provide the possible solutions for these attacks to improve the security of smartphone.

III. Smartphone Problems

The technologies of smartphone have been increasing with a huge rate over last few years. Now-a-days a smartphone can provide different services as like as a computer can provide. Our smartphone holds much information such as mailing information, messaging information, calling information etc., which are very important for us. Therefore, we have to ensure the security and privacy of our smartphone.

The addition of powerful OSs, applications, hardware etc., makes smartphone strong and secure, but all these are not enough to protect our privacy. As the number of privacy and security related threats are raising comparatively. The security and privacy related challenges in smartphone are slightly same as the computer threats environment. Smartphone problems are categorized into four parts [12] including: Data protection and privacy, Attacks, Authorization, and Vulnerabilities (Fig. 1).

A. Data Protection and Privacy

Muslukhov *et al.* [13] found out the problem of data protection and privacy and discussed the types of data a user wants to protect in smartphone. Authors' also showed for the different types of data how the required security protection is change. In another recent study, Muslukhov [14] discussed about data protection and privacy problem and showed that the regular update of smartphone lock screen for users' authentication and accessibility creates the security and protection level more strong.

B. Attacks

Attacks are similar in all smart devices such as smartphone, laptop, tablet etc. Attacks in smartphone categorized into two parts including: old attack and new attacks. Old attacks include physical attacks, different type of smartphone virus, backdoor, threats, Trojan, different types of malware, worms, radio and wireless network attacks, and spam attacks. New attacks include relay attack, counter attack, DOS attack, brute force attack, camera based attacks, SMS based attack, XSS attack, control-flow attack, etc.

C. Authorization

Zaidi *et al.* [12] noted that authentication could be getting by three methods. First one is to get the password or code or PIN which is used by actual user for authentication on smartphone. For example, if someone gets your smartphone cleverly and if he/she knows the password or code or PIN which you use, easily can get your personal information from smartphone. Second one is to find which users have used certain code to authentication of his/her smartphone. The third one is to get the fingerprint which is used by users also known as biometric.

D. Vulnerabilities

Vulnerabilities are the weak points of a smartphone, and it causes several different problems such as insecurity of personal information, privacy broken by malicious attackers etc. Users are not much aware about their personal information because, most of the time users' e-mail account, social media account etc. are logged in their smartphone. The vulnerabilities of smartphone contain many parts such as lack of awareness on personal information in smartphone, system fault, insecure apps in smartphone, insecure wireless network etc.

Among all these categories of smartphone problems 'Attacks' is the most common one. Two types of attacks are old attack and new attack. Both attacks have some individual impact to the smartphone. Table I and Table II show the impact of smartphone due to old attack and new attack.

Fig. 1. Categorization of Smartphone Problems.

TABLE. I. OLD ATTACKS AND THEIR IMPACT TO THE SMARTPHONES

Attack Name	Impact to the Smartphone
Physical Attack [15]	• Makes the security of smartphone weak • Causes abnormal behavior in smartphone • Unauthorized code can be effect to the users privacy
Smartphone Virus [16,17]	• Causes abnormal behavior in application and smartphone • Private information can be leaked via applications
Backdoor [18]	• Makes the security of smartphone weak • Create a backdoor for smartphone viruses
Threat [19]	• Makes the security of smartphone weak • Data may be hacked • Creates backdoor into private information
Malware [20,21]	• Interfere in smartphone operations • Collects private information
Wireless Attack [22]	• Data may be hacked • Makes the security of smartphone weak • Private information may be leaked.
Spam [23]	• Fill the e-mail inbox with unnecessary information • Decrease the smartphone internet speed • Collect different important information like contact list, message etc.

TABLE. II. NEW ATTACKS AND THEIR IMPACT TO THE SMARTPHONES

Attack Name	Impact to the Smartphone
Counter Attack [24]	• Target information can be accessed
Relay Attack [25]	• Private information may be hacked.
DOS attack [26]	• Slow the network • Busy the smartphone services
Camera based attack [27]	• Makes the security of smartphone weak • Collects users private information
SMS based attack [28]	• Slow the smartphone operations • Collects sensitive information
Control flow attack [29]	• Collect different important information like contact list, message etc. • Memory information can be accessed
Brute force attack [30]	• Slow the CPU speed • Users password may be hacked

IV. METHODOLOGY

The aims of this research at evaluating how much the smartphone users are aware about their security and privacy. Data collection based on industrial survey is the most common process for research project, but this process requires large time to complete, and data analysis is costly [31]. However, a recent study by Couper [32] discussed about the different technologies of data collection, which can be used to analyze the data automatically (e.g. Google form). Another study by Granello *et al.*, [33] pointed that online data collection has become very popular strategy in many research methodologies.

A. Pilot Study

In our study, we have used survey strategy to find the quantitative results. The survey was planned to find out the level of security and privacy awareness among the smartphone users. To understand the topic better on "security and privacy awareness survey for smartphone users" we consulted with many smartphone users and discussed about their smartphone security related problems. We found three types of users. Some users treated their phones as normal phone, although their phones contain smartphone functionalities, they just use their phone for call or SMS related work only. Some user installed different third party apps without knowing the terms and service related conditions. Some users utilize the full smartphone functionalities.

B. Research Instruments and Target Population

An online tool was used here based on the questions to analyze the collected data. This research contains 20 questions and the answers might be one or multiple. All these questions are based on security and awareness of smartphones. Among these questions we have used just 7 in our study, which can fulfill our goal and objectives. Our aim is to evaluating whether smartphone users aware about their security and privacy related issue, and to evaluate how much aware they are. The target population of this study was smartphone users, especially university students of different countries on the age group between 20 to 26 ages. The purpose of this study is to understand the security and privacy awareness from the smartphone users.

C. Data Analysis and Discussion

At first, we set our questionnaires in a Google form. By using this Google form, we have taken survey from university students' age group in between 20 to 26 year. Then we have stored these results in Microsoft Excel format for further use. After completion the survey, we have found how many responses are there, whether everything is okay or not. We also check every necessary question is answered clearly or not, whether the result fulfills our objectives. Then we combined our survey result together and found out our objectives. Since, our problem statement is related to the security and privacy awareness of smartphone and we combine the survey results and try to find the level of smartphone security awareness displayed by public, whether the general level of security exists amongst smartphone users etc. To present our survey results, we use bar chart. In this study, we have used Google form, computer, Microsoft Excel to find out the security and privacy awareness of smartphone.

V. SURVEY RESULTS

In total 3,424 responses recorded in this survey, among them 175 (5.11%) responses were rejected during initial exploration of data analysis because, all required questions were not answered. Of the remaining 3,249 responses are used in this study. We have analyzed the survey results based on seven research questions which have discussed in this section. All these questions are important to find out the awareness of smartphone security and privacy because all these questions are addressed to smartphone problems.

A. Research Questions

The aim of this research is to measure the level of smartphone security awareness displayed by the public. Also to determine whether, a general level of security complacency exists amongst the smartphone users and to measure the awareness of android users regarding their privacy. The research questions are planned in very simple language, which is easy to understand. All these objectives lead to the following questions:

- Q1: For what purpose do you use Smartphone?
- Q2: From where you mostly install applications?
- Q3: Do you ever install third party applications or applications from Unknown sources in your Smartphone?
- Q4: Before installing application do you read application provider's privacy and policy for using application's?
- Q5: Before installing application do you ever read through application's phone access permissions?
- Q6: What authentication system do you use to lock screen for security?

B. Evaluation of Research Questions

Q1: Now-a-days smartphone can perform different services as like computer such as email, SMS, location tracking, contact list, stores photos and videos, social media account etc. Q1 is about the purpose of using smartphone to find how many people use all these services in their smartphone. Fig. 2 shows the result of this question, we can see that only 7.3% of the people use smartphone just for communication and they are less insecure than 88.20% of the people who use smartphone for all these activities.

Q2: Since a smartphone provides different facilities such as email, Google drive, SMS, and different social media, etc. It contains a lot of personal information that is very important for us and we should keep these secure. But most of the time we keep our personal accounts (e.g. Email, Facebook, Google drive etc.) logged in to our smartphone. Suppose, someone lost his/her smartphone and if personal accounts logged in to the smartphone, he/she might be lost his/her personal information. Since, our study is about security and privacy awareness we have used this question to find out how much people aware about their security and privacy. Fig. 3 shows the result of this question, and we can see 65.5% people are not aware in this concern.

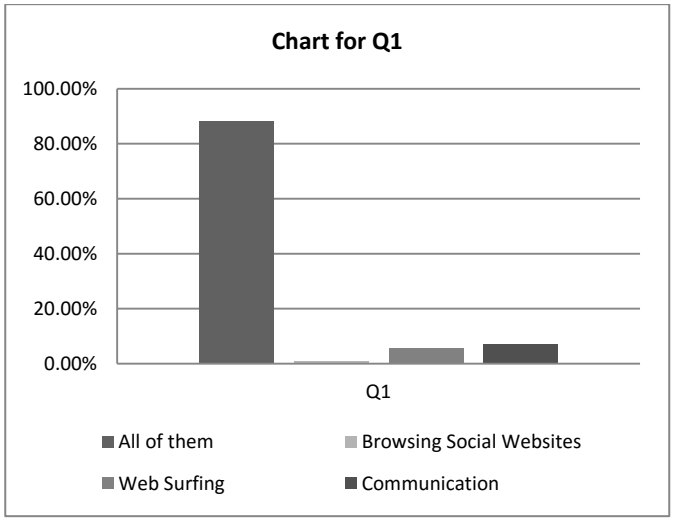

Fig. 2. For What Purpose do you use Smartphone?

Q3: Third party applications are not same as the operating system or manufacture of smartphone, as they are created by vendor. Third party apps contain most of the malware rather than system apps, that's why third party apps are more insecure than system apps. In another scenario, third party apps from unknown sources are more insecure than third party apps from built-in source for system (e.g. play store). In our survey result for question Q3 in Fig. 4, we can see 60% people installed third party apps from unknown sources.

Q4: Before installing apps, the application provider provides the privacy and policy of their apps. This privacy and policy contains about the policy of information about users' access. For example, your application extracts the contact list information from user, so you must have to notify the user about it. From the privacy and policy user can know where, for what and how long his/her information will be used. This is very important and users should read these privacy and policy before installing application. In Fig. 5, we have shown the survey result for Q4, we can easily observe that 25.50% people never read privacy and policy and 52.70% of the people read privacy and policy sometimes.

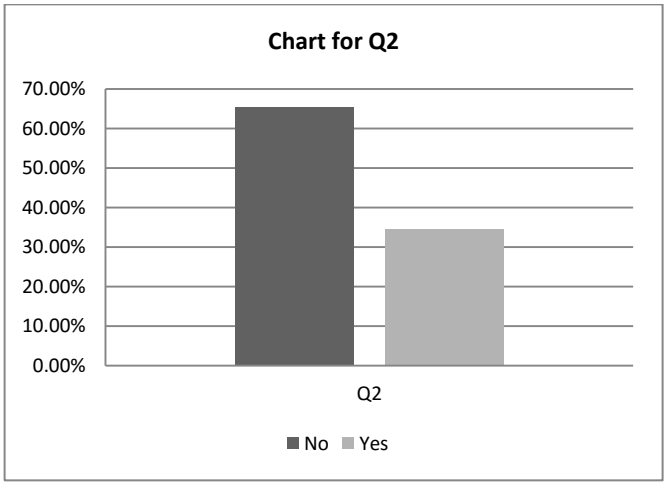

Fig. 3. Do you Sign out from your Personal Accounts (e.g. Email, Facebook, Google Drive Etc.) after using it with Smartphone?

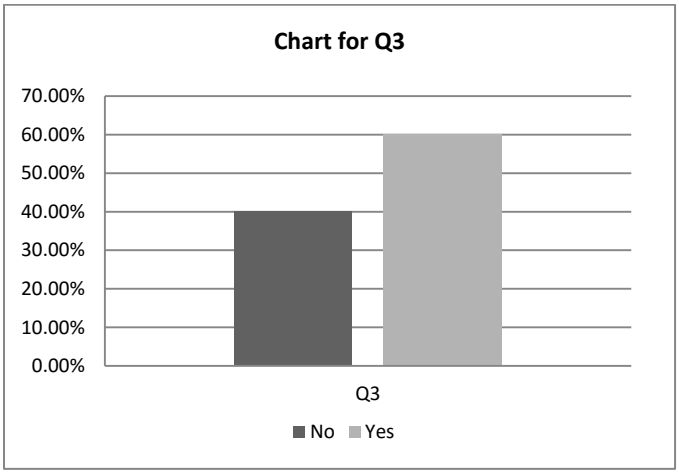

Fig. 4. Do you ever Install Third Party Applications or Applications from unknown Sources in your Smartphone?

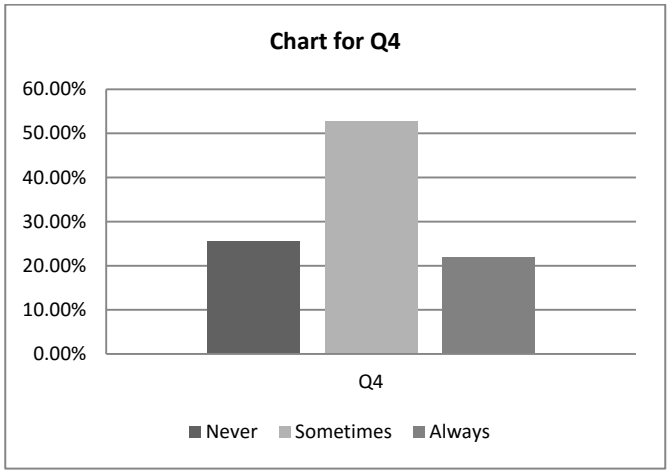

Fig. 5. Before Installing Application, do you Read Application Provider's Privacy and Policy for using Application's?

Q5: The technologies of smartphone have been increasing day by day. A smartphone can hold our different personal information such as photos and videos, mail, SMS etc. and other important information. Before installing application, the application provider shows the applications' phone access permission. Applications' phone access permission means what information of your smartphone access by the application. A user should always read through the applications' phone access permission carefully. Fig. 6 shows the bar chart of the Q5 questions' result. The chart shows that 11.6% people never read the applications' phone access permission and 46.5% people sometimes read the applications' phone access permission before install application.

Q6: Authentication is one of the major problems of smartphone. Suppose, someone gets your phone cleverly for a short time, if he/she does not know your smartphone authentication system, he/she cannot access any information from your smartphone. There are many authentication systems for smartphone including: pin code, password, pattern, fingerprint etc. Among them fingerprint is more secure than others. Fig. 7 shows our survey result for question Q6. We can see almost 98% of the people use authentication system to unlock the smartphone lock screen.

C. Proposed Model

Smartphone security is not limited to those six questions but, when we think about smartphone security and privacy awareness survey those questions gets the top priority. In recent days, those reasons are more responsible for losing the privacy of smartphone. Based on survey result we have developed (1) which can measure the level of awareness (LoA) for a smartphone user.

$$LoA = 1 - \left(\frac{2}{1+e^{-Q}} - 1\right) \quad (1)$$

Where, Q = Q1+Q2+Q3+Q4+Q5+Q6

We have considered some safe option and unsafe options for each question which denote to secure and insecure zone respectively. Safe options for every question carry the value of 0 (zero) and unsafe options carry value of 1 (one). Table III shows the safe and unsafe options for each question.

This proposed equation shows the level of awareness (LoA) in between the range of 0 to 1. Table IV shows the percentage level of awareness (*LoA*) for every possible value of '*Q*'. In Table IV, we can see if a user answered safe option of all the questions his/her LoA is 100%, if user contain 1 unsafe option his/her LoA is 53.78% and so on. Since we have mentioned earlier that only those questions do not responsible for losing the privacy of smartphone, many others reasons also harmful for privacy of smartphone. If we add more questions to this system, it will produce more accuracy.

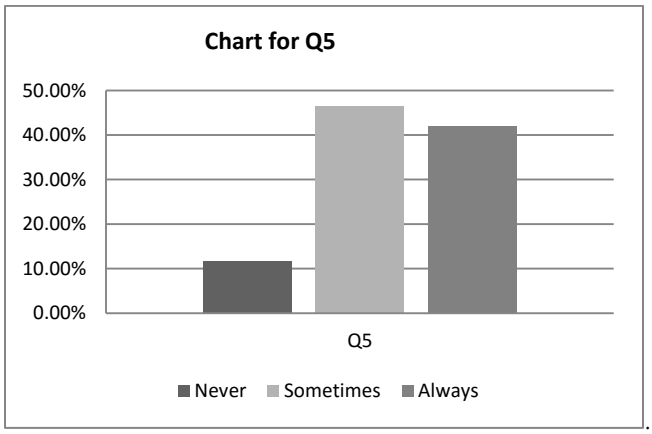

Fig. 6. Before Installing Application, do you ever read through Application's Phone Access Permissions?

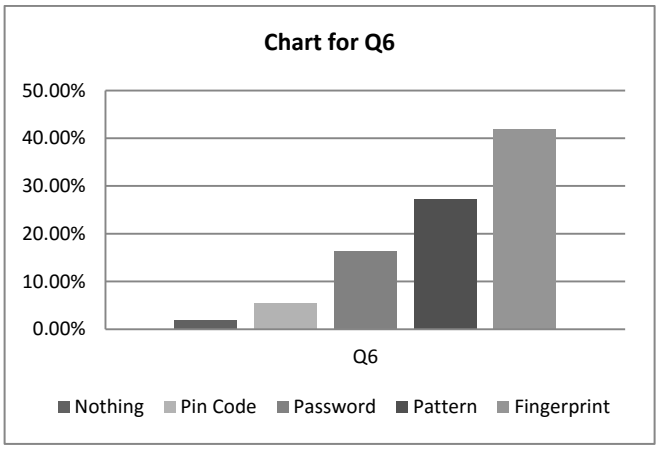

Fig. 7. What Authentication System do you use to Lock Screen for Security?

TABLE. III. CONSIDERED OPTIONS FOR QUESTIONS

Question	Safe option	Unsafe option
Q1	• Communication	• All • Browsing social websites • Web surfing
Q2	• Yes	• No
Q3	• No	• Yes
Q4	• Always	• Never • Sometimes
Q5	• Always	• Never • Sometimes
Q6	• Pin Code • Password • Pattern • Fingerprint	• Nothing

TABLE. IV. PERCENTAGE LOA FOR THE VALUE OF 'Q'

Value of *'Q'*	Percentage *LoA*
0	100%
1	53.78%
2	23.84%
3	9.49%
4	3.60%
5	1.34%
6	0.49%

VI. CONCLUSION

This research aims at evaluating how much the smartphone users are aware about their security and privacy. In this study, firstly we have taken a survey from smartphone users to access the level of smartphone security awareness. We have found that on average 60% people do not aware about their smartphone security and privacy. Secondly, we have proposed a model to measure the level of awareness for smartphone users. We have found that almost 50% of the smartphone user contains 9.49% level of awareness. Although, the addition of new technologies makes a smartphone smarter, the security and privacy related threats also increases relatively. In future work, we will extend this study by adding others security and privacy related behavior and make our model more efficient and accurate.

REFERENCES

[1] Roesner, F., Kohno, T., & Molnar, D. (2014). Security and privacy for augmented reality systems. Communications of the ACM, 57(4), 88-96.

[2] Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012, July). Measuring user confidence in smartphone security and privacy. In Proceedings of the Eighth Symposium on Usable Privacy and Security (p. 1). ACM.

[3] Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security?. Journal of Computer Information Systems, 53(2), 22-30.

[4] Yildirim, N., Daş, R., & Varol, A. (2014, May). A Research on Software Security Vulnerabilities of New Generation Smart Mobile Phones. In 2nd International Symposium on Digital Forensics and Security (pp. 6-16).

[5] PhoneArena, "Android's Google Play beats App Store with over 1 million apps, now officially largest," [Online]. Available: http://www.phonearena.com/news/ [Accessed: 07 July,2019].

[6] Dr.Web, "Android.Spy.277.origin," [Online]. Available: http://vms.drweb. [Accessed: 07 July, 2019].

[7] Dan, G., "Malicious apps in Google Play made unauthorized downloads, sought root,"[Online]. Available: http://arstechnica.com/information-technology/2016/01/malicious-apps-in-google-play-made-unauthorized-downloads-sought-root/. [Accessed: 07 July,2019].

[8] Benenson, Z., Kroll-Peters, O., & Krupp, M. (2012, September). Attitudes to IT security when using a smartphone. In Computer Science and Information Systems (FedCSIS), 2012 Federated Conference on (pp. 1179-1183). IEEE.

[9] Ophoff, J., & Robinson, M. (2014, August). Exploring end-user smartphone security awareness within a South African context. In Information Security for South Africa (ISSA), 2014 (pp. 1-7). IEEE.

[10] Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. Computers & Security, 34, 47-66.

[11] Alani, M. M. (2017). Android Users Privacy Awareness Survey. International Journal of Interactive Mobile Technologies (iJIM), 11(3), 130-144.

[12] Zaidi, S. F. A., Shah, M. A., Kamran, M., Javaid, Q., & Zhang, S. (2016). A Survey on security for smartphone device. IJACSA) International Journal of Advanced Computer Science and Applications, 7, 206-219.

[13] Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., & Beznosov, K. (2012, April). Understanding users' requirements for data protection in smartphones. In Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on (pp. 228-235). IEEE.

[14] Muslukhov, I. (2012). Survey: Data protection in smartphones against physical threats. Term Project Papers on Mobile Security. University of British Columbia.

[15] Kataria, A., Anjali, T., & Venkat, R. (2014, February). Quantifying smartphone vulnerabilities. In Signal Processing and Integrated Networks (SPIN), 2014 International Conference on (pp. 645-649). IEEE.

[16] La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. IEEE communications surveys & tutorials, 15(1), 446-471.

[17] Cheng, J., Wong, S. H., Yang, H., & Lu, S. (2007, June). Smartsiren: virus detection and alert for smartphones. In Proceedings of the 5th international conference on Mobile systems, applications and services (pp. 258-271). ACM.

[18] Durairaj, M., & Manimaran, A. (2015). A study on security issues in cloud based e-learning. Indian Journal of Science and Technology, 8(8), 757-765.

[19] Pfleeger, C. P., & Pfleeger, S. L. (2002). Security in computing. Prentice Hall Professional Technical Reference.

[20] Khouzani, M. H. R., Sarkar, S., & Altman, E. (2012). Maximum damage malware attack in mobile wireless networks. IEEE/ACM Transactions on Networking, 20(5), 1347-1360.

[21] Peng, S. C. (2013). A survey on malware containment models in smartphones. In Applied Mechanics and Materials (Vol. 263, pp. 3005-3011). Trans Tech Publications.

[22] Mandke, K., Nam, H., Yerramneni, L., Zuniga, C., & Rappaport, T. (2003). The evolution of ultra wide band radio for wireless personal area networks. Spectrum, 3, 10-6.

[23] Xu, Z., & Zhu, S. (2012, August). Abusing Notification Services on Smartphones for Phishing and Spamming. In WOOT (pp. 1-11).

[24] Lee, H. T., Kim, D., Park, M., & Cho, S. J. (2016). Protecting data on android platform against privilege escalation attack. International Journal of Computer Mathematics, 93(2), 401-414.

[25] Yalcin, S. B. O. (2010). Radio Frequency Identification. Security and Privacy Issues. In 6th international workshop, RFIDSec (pp. 8-9).

[26] Dondyk, E., & Zou, C. C. (2013, January). Denial of convenience attack to smartphones using a fake Wi-Fi access point. In Consumer Communications and Networking Conference (CCNC), 2013 IEEE (pp. 164-170). IEEE.

[27] Amravati, M. E. S. (2015). A Review on Camera Based Attacks on Andriod Smart Phones. International Journal of Computer Science & Technology, 6(1), 88-92.

[28] Stites, D., & Tadimla, A. A Survey Of Mobile Device Security: Threats, Vulnerabilities and Defenses./urlhttp.afewguyscoding.com/2011/12/survey-mobile-devicesecurity-threatsvulnerabilities-defenses.

[29] Davi, L., Dmitrienko, A., Egele, M., Fischer, T., Holz, T., Hund, R., & Sadeghi, A. R. (2012, February). MoCFI: A Framework to Mitigate Control-Flow Attacks on Smartphones. In NDSS (Vol. 26, pp. 27-40).

[30] Kim, I. (2012). Keypad against brute force attacks on smartphones. IET Information Security, 6(2), 71-76.

[31] Kumar, S., & Phrommathed, P. (2005). Research methodology (pp. 43-50). Springer US.

[32] Couper, M. P. (2005). Technology trends in survey data collection. Social Science Computer Review, 23(4), 486-501.

[33] Granello, D. H., & Wheaton, J. E. (2004). Online data collection: Strategies for research. Journal of Counseling & Development, 82(4), 387-393.