IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

The Study of Smartphones Security and Privacy

Nahida Jameel Siddiqui
Student, Department of MCA
Late Bhausaheb Hiray S. S. Trust's Institute of Computer Application, Mumbai, India

Abstract: *Smartphone becomes one in all the foremost popular devices in last few years thanks to the combo of powerful technologies in it. Smartphone holds our important personal information like photos and videos, SMS, email, contact list, social media accounts etc. Therefore, the quantity of security and privacy related threats are increasing relatively. We also determine whether a general level of security complacency exists among smartphone users and measure the eye of android users regarding their privacy. From survey result we've found that, most of the people don't seem in touch in mind about their smartphone security and privacy. Secondly, supported survey results, we have got shown a way to measure the amount of awareness (LOA) for the smartphone users.*

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

I. INTRODUCTION

Technologies of smartphone are increasing with a large rate over previous few years. Smartphone provides many services as data sharing, phone calls, internet, different online & offline games etc. Therefore, it increases the prospect of security and privacy related threats comparatively. Almost 80% of activities associated with the net, so it's important for us to become privy to security and privacy. Several studies have also shown that, security related to smartphone, most of the smartphone users are favorable [1, 2, 3].

For Authentication of smartphone, people use different Types of security like keeping patterns, finger print password, face Recognition, pin as a passwords etc. of those aren't enough to protect us from security related issues [4]. Smartphones are device which is used to store different personal information. We have to verify the security of our personal information. Most of the time, due to lack of our awareness we fail to shield our personal information. If all this information falls into a nasty hand, we'd be in trouble. According to a recent study, Google play published quite 3.5 million apps from 2009 to December, 2017 [5]. Number of applications is also increasing over years as need increases. Another recent security study showed that, in Google play store, over 200 malevolent apps were found [6]. Application also collect's private information such as contact numbers, Gallery and camera data, Location etc. Attacker's then save that in server. On regular Intervals this information is recorded on the server when users use these apps. Within the first 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 are showing results associated with awareness survey for security and privacy associated with Smartphones The research aims at evaluating what quantity the smartphone users are conscious of their security and privacy. During this survey, I've got used questionnaire methodology to access the amount of security awareness associated with smartphones we determine whether a general level of security complacency exists amongst smartphone users and supported these result we show a statics model to live the attention of android users regarding their privacy.

This paper is organized as follows.

In the upcoming section we start with a discussion of previous related work in section II. Explanation of Smartphone problems in section III and Different types of smartphones attacks .In Section IV, we have Literature review, proceed with Research methodology. In Section V, we have 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.

II. PREVIOUS WORK

Benenson et al. [8] pointed that IT security plays a crucial role while someone use smartphone, due to its‟ broadly acknowledged and well documented feature, which mainly focused on the technical area of a smartphone security system.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

In step with their interview of 24 users on that security of smartphone, they found the role of user. Supported this result they consecrated five hypotheses and proposed a mental technique after evaluation of those hypotheses. A recent study in South Africa by Ophoff & Robinson [9] shown that the extent of awareness on smartphone security supported public users and determined what proportion a standard security level exists in smartphone users.

Survey for Smartphone security awareness, They Found 619 African users support third party apps. They found that users showing high level of trust on smartphone apps, rather than after they install other third party apps. During this study, they used an updated version of model developed by Mylonas et al. [10].

A huge number of apps are downloaded daily by the users, but it's really difficult to differentiate between good terms of service security apps and bad terms of service security apps. During this paper, authors shown a result supported a survey of 4027 android smartphone users for android user security awareness. Consistent with their survey, they tried to indicate the interactions between users and terms and repair security while they install apps. in a very recent study by Mylonas et al. [10] discovered 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 chance of smartphone security may increase because sometimes the protected information may well be accessed by third party apps.

According to their survey, they tried to search out out whether users privy to their security of smartphone while they downloaded and installed apps form apps store house. Supported their survey, they developed a model which will identify these users who trust apps storehouse. Zaidi et al. [11] pointed that because of the advanced technologies, smartphone has become a daily necessary component, and also the prospect of security based attacks has increased. New attack and old attack are the 2 kinds of security-based attacks. In keeping with this study, authors provide a straightforward view of varied smartphone security related attacks, and also provide the possible solutions for these attacks to boost the protection of smartphone.

II. SMART PHONE PROBLEMS

The technologies of smartphone are increasing with an enormous rate over previous couple of years. Smartphones provide various services that can be provided by computers. Our smartphone holds much information like mailing information, messaging information, calling information etc., which are vital for us. Therefore, we've got to make sure the protection and privacy of our smartphone. The addition of powerful OSs, applications, hardware etc., makes smartphone strong and secure, but of these don't seem to be enough to guard our privacy. Because the number of privacy and security related threats are raising comparatively. The protection and privacy related challenges in smartphone are slightly same because the computer threats environment.

While there are many benefits of smartphones, some believe that they're a distraction and permit the user to depend on the device an excessive amount of for daily tasks. But other than the possible benefits and drawbacks, some say that smartphones create a unique problem—privacy risks. People share all the updates related to their life on smartphones by posting on social media networks. Apps allow you to tag yourself. They also say that smartphones are often used as tracking devices by private hackers, the government, or cloud service provider. Cloud computing further enables data to be obtained. It doesn't matter if the smartphone is an iPhone or an Android; the breach of privacy of still possible by the transmission of information through apps. Data that's collected through apps is really used for targeted advertising after it's assembled into user profiles. In fact, the businesses that set the standards for app data gathering are big contenders within the ad business.

Here are some tips to shield your data and identity when using your smartphone:

- Manage location settings. If you wish to regulate location settings in apps like Facebook, Twitter, etc., make sure to show off all possible types of location assessment. If you are doing this, apps won't know your location.
- Lock your phone. Set your phone up in order that you would like a password to use it. This can be an easy thanks to keep your data in check.
- Encrypt data. This makes it possible for your phone to stay protected because the contents are going to be encrypted.
- Avoid downloading apps from untrusted sources. Apps are likely to be invasive in nature if they don't seem to be approved by an app store.

2.1 Attacks

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

Attacks are similar altogether smart devices like smartphone, laptop, tablet etc. Categories of attacks in smartphones are Old and New attacks. Types of Old attacks are physical attacks, different style of smartphone virus, backdoor, threats, Trojan, differing kinds of malware, worms, radio and wireless network attacks, and spam attacks. Types of new attacks are relay attack, counter attack, DOS attack, brute force attack, camera based attacks, SMS based attack, etc.

2.2 Authorization

Zaidi et al. [11] noted that authentication may well be getting by three methods. First one is to urge the password or code or PIN which is employed by actual user for authentication on smartphone. as an example, if someone gets your smartphone cleverly and if he/she knows the password or code or PIN which you utilize, easily can get your personal information from smartphone. Second is to search out which users have used certain code to authentication of his/her smartphone. The third one is to induce the fingerprint which is employed by users also called.

2.3 Vulnerabilities

Vulnerabilities are the weak points of a smartphone, and it causes several different problems like insecurity of non-public information, privacy broken by malicious attackers etc. Users don't seem to be much privy to 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 like lack of awareness on personal information in smartphone, system fault, insecure apps in smartphone, insecure wireless network etc. Among of these categories of smartphone problems Attacks is that the most typical one. Two forms of attacks are old attack and new attack. Both attacks can impact to the smartphone.

III. LITERATURE REVIEW

There aren't any clear solutions presented to the Android Security issues. All security protection of information is based on two factors-something you recognize and something you own. An access card and a password are perfect depictions of this scenario. Many times, only 1 of these items is required, and sometimes within the foremost secure of places, both are needed. But with mobile we can store all personal as well as private information of Bank account and etc., the need for an easy but effective biometric solution has risen exponentially [12]. In addition malware detection services currently use a stronger battery footprint than most applications, causing users to disable any security that had been previously implemented [13].

3.1 Use a Passcode

This may sound obvious, but consistent with a Consumer Reports survey, 64% folks don’t use our passcodes. (For the record, using the factory set passcode totally doesn’t count.) Quite frankly, not employing a passcode could be a horrible idea. You’re essentially delivering all of your personal information to anyone who swipes your phone.

When you founded your passcode, use the identical security measures you'd on the other device, like not using your birthday or social insurance number for your passcode, and definitely not “1234.” Never share your passcode with anyone, whether or not they ask nicely or offer you sad, puppy eyes. Don’t use or reuse passwords from sites or devices. While this is often a theme of debate, most experts think it’s best to travel with a pin instead of the swipe patterns, because the chances of guessing a pin are much below guessing a pattern. But hey, if it gets you locking your phone, either choice is okay.

3.2 Be Selective With Your Apps

That new app might look great, but with such a big amount of unknown third party providers out there, it is difficult to understand how private and secure it should be. For that reason, it’s best to travel through a trusted app store like iTunes, Android Market or Amazon, and to thoroughly check reviews before downloading any app and entering your personal information.

3.3 Don’t Click on Suspicious Links

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

Maybe it's those tiny, almost indecipherable screens, maybe it's a false sense of security, except for some reason, people are thrice more likely to click on suspicious links on their mobile phone than on a PC. One should hover over Link and have a look at the URL, if you find Link appropriate then only Click on the Link.
Most banks have a page explaining what they'll and cannot kindle. Do your research before divulging your personal details.

3.4 Enable Remote Wiping

Should your phone ever be lost or stolen, it might be great to erase your important data from afar. You'll be able to do that through remote wiping, and it's relatively easy to try to on most devices. An iPhone, for instance, simply requires you to try and do enable "Find My Phone" on the device and to sign on for an iCloud account, which can be your command central when it's time to wipe.

3.5 Regular Software Update

Software updates often patch security and privacy holes users have found as they've tested the software go in the 000 world. Keeping your software up to now will mean you'll have the very latest solutions. That said, sometimes it is sensible to attend every week, or two, before installing the newest versions to work out if there are any problems with rollouts.

3.7 Use Security Applications

Both Spyware and Malware are getting an increasingly formidable problem for itinerant users. They track your whereabouts, channelize your personal information, and curtail your phone. It is difficult to avoid downloading these, and users often don't know they're running. To combat this, install security software, rather like you may wear your computer, to safeguard your privacy against any unbeknownst mischief. Ensure that you just keep this software up to this point.

3.8 Keep off of Open Wi-Fi Networks

Since smartphones are now acting like mini-PCs, avoid unknown open Wi-Fi networks, rather like you'd on your PC. As you type, malicious hotspots can transmit your MasterCard information and passwords without you even knowing it.

3.9 Write Down Your IMEI

Every phone contains a fifteen digits serial number called an IMEI (International Mobile Equipment Identity), which might are available in handy if your phone is ever lost or stolen. You'll find it behind your phone's battery or within the settings. It's well worth writing down, because it can speed the method of getting the phone back to you.

3.10 Copy Your Phone Regularly

Backing up your phone means you'll always have access to all or any of your photos, music, apps and whatever else. this is often in fact important just in case your phone gets lost or stolen, but it can even are available in handy when you're doing an OS update and skill a loss of information (it happens). Confirm to back up a minimum of once on a daily basis for the simplest results, or think about employing automatic syncing with a cloud program.

3.11 Guard the information on Your Sim Card

If you choose to sell your cellular phone, there are variety of belongings you should do before shipping it off to a stranger. One amongst the foremost important is to get rid of both your SIM and your SD card, both of which contain a wealth of information. Do that when sending your phone sure repairs, as well, particularly if you don't know your store well.

IV. METHODOLOGY

The aims of this research at evaluating what proportion the smartphone users are aware of their security and privacy.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

Data collection supported industrial survey is that the commonest process for scientific research, but this process requires large time to complete, and data analysis is expensive [14]. However, a recent study by Couper [15] discussed about the various technologies of knowledge collection, which might be wont to analyze the info automatically (e.g. Google form). Another study by Granello et al., [16] pointed that online data collection has become very hip strategy in many research methodologies.

4.1 Pilot Survey

In our study, we have used survey strategy to go looking out the quantitative results. The survey was planned to hunt out out the extent 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 kinds of users. One who uses phones as normal phone, although their phones contain smartphone functionalities, they solely use their phone for call or SMS related work only. Some user installed different third party apps without knowing the terms and repair related conditions. Some users utilize the entire smartphone functionalities.

4.2 Research Instruments and Target Population

An online tool was used here supported the inquiries to analyze the collected data. This research contains 20 questions and therefore the answers can be one or multiple. Of these questions are supported security and awareness of smartphones. Among these questions we've got used just 7 in our study, which may fulfill our goal and objectives. Our aim is to evaluating whether smartphone users aware of their security and privacy related issue, and to gauge what quantity aware they're. The target population of this study was smartphone users, especially university students of various countries on the people between 20 to 26 ages. The aim of this study is to grasp the protection and privacy awareness from the smartphone users

4.3 Data Analysis and Discussion

At first, we set our questionnaires in an exceedingly very Google form. By using this Google form, we have taken survey from university students‟ cohort in between 20 to 26 year. Then we have got stored these results in Microsoft Excel format for further use. After completion the survey, we've found what percentage responses are there, whether everything is okay or not. We also checked the number of questions answered to check our objectives.

Then we combined our survey result together and located out our objectives. Since, our problem statement is claimed to the protection and privacy awareness of smartphone which we combine the survey results and try to go looking out the extent of smartphone security awareness displayed by public, whether the level of security exists amongst smartphone users etc. To present our survey results, we use chart. During this study, we have got used Google form, computer, Microsoft Excel to go looking out the protection and privacy awareness of smartphone.

V. SURVEY RESULTS

In total 180 Google form responses recorded during this survey, among them 21 responses were rejected during initial exploration of information analysis because, all required questions weren't answered. Of the remaining 159 responses are used during this study. I Have got analysed the survey results supported seven research questions which have discussed during this section. Of these questions are important to search out out the notice of smartphone security and privacy because of these questions are addressed to smartphone problems.

5.1 Research Questions

The aim of this research is to live the amount of smartphone security awareness displayed by the general public. Also to work out whether, a general level of security complacency exists amongst the smartphone users and to live the attention of android users regarding their privacy. The research questions are planned in very simple language, which is simple to know. Of these objectives result in the subsequent questions:

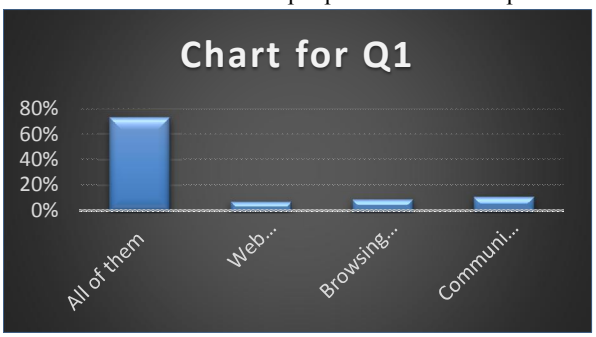
- Q1: For what purpose do you use Smartphone?
- Q2: From where you mostly install applications?

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

- 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 phone screen for security?

5.2 Evaluation of Research Questions

Q1: Now-a-days smartphone can perform different servicesas like computer such as email, SMS, location tracking, contactlist, stores photos and videos, social media account etc. Q1 is to fing the number of folks using all the services of their smartphone.Fig.1 shows the result of this question, we can see that only 11% of the people use smartphone just for communication and they are less insecure than 83% of the people who use smartphone for all these activities



Q2: Since a smartphone provides different facilities such asemail, Google drive, SMS, and different social media, etc. It contains a lot of personal information that is very important forus and we should keep these secure. But most of the time we keep our personal accounts (e.g. Email, Facebook, Googledrive etc.) logged in to our smartphone. Suppose, someone losthis/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. 2 shows the result of thisquestion, and we can see 65.5% people are not aware in this concern.

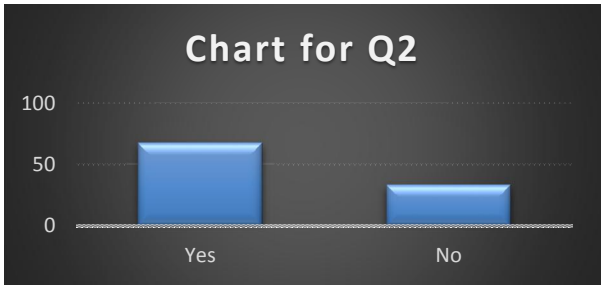
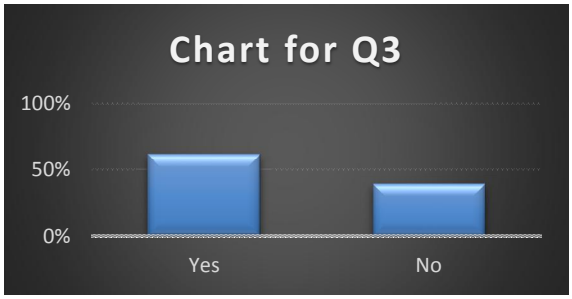


Fig. 2. Do you Sign out from your Personal Accounts (e.g. Email, Facebook,Google Drive Etc.) after using it with Smartphone?

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 insecurethan system apps. In another scenario, third party apps from unknown sources are more insecure than third party apps frombuilt-in source for system (e.g. play store). In our survey resultfor question Q3 in Fig. 3, we can see 61% people installed third party apps from unknown sources.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252



Q4: Before installing apps, the appliance provider provides the privacy and policy of their apps. This privacy and policy contains about the policy of knowledge about users‟ access. For instance, your application extracts the contact list information from user, so you need to must notify the user about it. From the privacy and policy user can know where, for what and the way long his/her information are used. This is often important and users should read these privacy and policy before installing application. In Fig. 4, we've got shown the survey result for Q4, we will easily observe that 15% people never read privacy and policy and 59% of the people read privacy and policy sometimes.

Fig. 4. 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,

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

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 smartphoneauthentication system, he/she cannot access any information from your smartphone. There are many authentication systemsfor smartphone including: pin code, password, pattern, fingerprint etc. Among them fingerprint is more secure than others. Fig. 6 shows our survey result for question Q6. We cansee almost 98% of the people use authentication system to unlock the smartphone lock screen.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

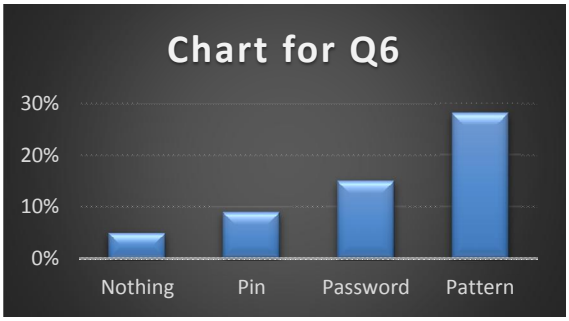


Fig. 6.What authentication system do you use to lock phone screen for security?

Table 1: Considered Option for Question

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

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.

ACKNOWLEDGMENT

I would like to acknowledge the University of Mumbai, India to give me the opportunity to do the research work under the title “The Study of smartphones security and Privacy”. I would like to acknowledge Prof. Divakar Jha for providing Guidance and the college L.B.H.S.S Trust’s Institute of Computer Application, Mumbai India to support during the research process.

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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

[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] 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.
[12] Muslukhov, I. (2012). Survey: Data protection in smartphones against physical threats. Term Project Papers on Mobile Security. University of British Columbia.
[13] 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.
[14] Kumar, S., & Phrommathed, P. (2005). Research methodology (pp. 43- 50). Springer US.
[15] La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. IEEE communications surveys & tutorials, 15(1), 446-471.
[16] Granello, D. H., & Wheaton, J. E. (2004). Online data collection: Strategies for research. Journal of Counseling & Development, 82(4), 387-393.
[17] Granello, D. H., & Wheaton, J. E. (2004). Online data collection: Strategies for research. Journal of Counseling & Development, 82(4),
387-393