A Study of Security Awareness Among Android Users

Pramod Prakash Ghogare
Computer Application Department, KCES's Institute of Management and Research, Jalgaon
pramod.ghogare@yahoo.com

Manoj P. Patil
School of Computer Sciences, North Maharashtra University, Jalgaon
mpp145@gmail.com

***Abstract*— Android users are rapidly increasing so is use of internet on mobile devices. This paper present settings, configuration, habits of internet usage made by user on android devices. Data collection has been done for understanding usability of android devices. The purpose of data collection was seeking information about security vulnerabilities created due to unawareness of android operating system and its settings. Analysis is done on the basis of responses from users for avoiding vulnerabilities due to unawareness of different settings exists in android devices.**

Keywords- Mobile Computing, Cyber Crime, Privacy and Security in Mobile Multimedia, Cyber Security, Security and Privacy of Mobile/Wireless Systems.

I. INTRODUCTION

Android device is becoming necessary in today's communication world. It is very easy to complete a task by using smart device if it related to internet or digital communication. In India android devices are favorite due to reduced price and additional functionalities compare to others smart devices. Mobile internet users are increasing year after year. The consumers are attracted to the high offers provided by the mobile network operators as a part of marketing strategy to sustain in the market. Android has less limitation for developer as compare to other smart device operating system, thus it increases risk for end user [1]. Figure 1 shows rate of growth in mobile internet users in India from June 2012 to June 2016. As on December 2016, India had estimated 432 million Internet users. Report also confirms 42% of points of access for internet are mobile phone in rural India [2]. Report by StatCounter, mobile and tablet devices accounted for 51.3 percent of internet usage worldwide compared to 48 percent on desktops [3]. This expresses use of mobile device for accessing internet is increasing year after year because of advantages of mobility, price compare to desktop. A report by Kantar IMRB & MMA about "Smartphone Usage and Behavior" indicate smartphone users are spending more time than on any other media, including TV and Print. Social media and messaging apps account for the highest reach among all categories. They also account for almost 50% of all time spent on smartphones. An average user spends approximately 3 hours daily accessing the Internet on a smartphone. Active internet users spend 60% more time on mobile compared to Desktop. Entertainment apps are extremely popular with Native/stored content contributing to hugely to the time spent. With increased internet connectivity, financial transactions and related activities online are on the rise [4]. Because of this scenario threat to vulnerability on android device may increase so users must aware of android operating system functionality, setting, configuration. To avoid cyber theft or misuse of own information by hackers. Android operating system is an open source which makes source code accessible to device manufacturers for development. Because of this availability most of manufacturer provide android OS in their manufactured smartphone. Android devices not only contains contacts or messages but also personal information in form of photos, documents, audio and visuals. It's important to keep android device safe and secure using various application and configuration.

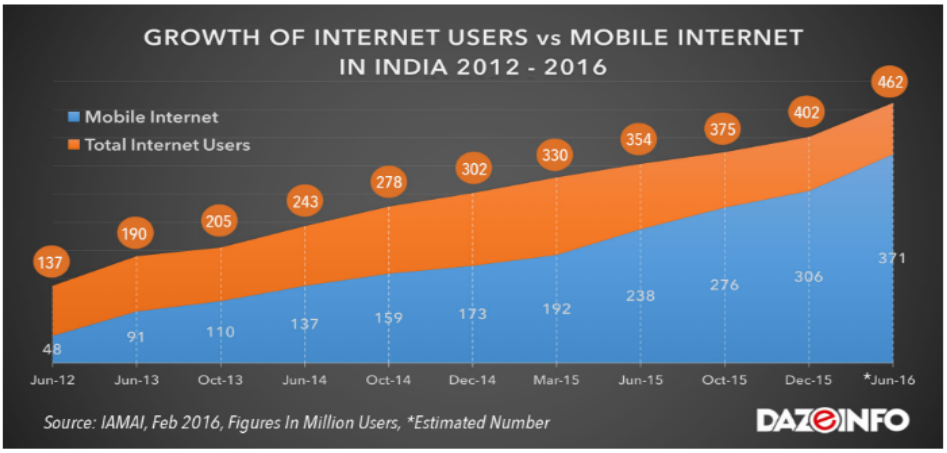

Figure 1 Growth of internet users on mobile devices in India from year 2012 to 2016

"In India more than 70% of Android smartphone users don't get an update to the latest Android OS". As per report Indian users not receiving updates of latest Android system by default before purchasing devices this can lead to unsecure surroundings while retrieving internet on device. Latest OS updates includes security updates due to that security of respective device increases, so even user don't update device manually it has its own security setting included in OS by which there are less chances for intrusion. In India more than 80,000 infection found in mobile devices and these are only unique infections [5].

TABLE 1 STATISTICS OF CYBER CRIME IN INDIA FROM YEAR 2013 TO 2015

SL	Crime heads under IT Act	Cases Registered			% Var.	Persons Arrested			% Var.
		2013	2014	2015		2013	2014	2015	
1	Tampering Computer Source Documents (Sec. 65 of IT Act)	137	89	88	-1.1	59	64	62	-3.1
2	Computer Related Offences(Sec. 66 to 66E of IT Act)	2,516	5,548	6,567	18.4	1,011	3,131	4,217	34.7
3	Cyber Terrorism@(Sec. 66F of IT Act)	-	5	13	160.0	-	0	3	-
4	Publication/Transmission of Obscene/Sexually Explicit Content(Sec. 67 to 67C of IT Act)	1203	758	816	7.7	737	491	555	13
5	Intentionally not Complying with the Order of Controller(Sec. 68 of IT Act)	13	3	2	-33.3	3	4	3	-25
6	Failure to Provide or Monitor or Intercept or Decrypt Information(Sec. 69 of IT Act)	6	2	0	-100	7	0	0	-
7	Failure to Block Access any Information Hosted etc.@ (Sec. 69A of IT Act)	-	1	0	-100	-	0	0	-
8	Not Providing Technical Assistance to Govt. to Enable Online Access@(Sec. 69B of IT Act)	-	0	3	-	-	0	0	-
9	Un-authorized Access/Attempt to Access to Protected Computer System(Sec. 70 of IT Act)	27	0	8	-	17	0	4	-
10	Misrepresentation/Suppression of Fact for Obtaining License etc. (Sec. 71 of IT Act)	12	5	4	-20	14	13	2	-84.6
11	Breach of Confidentiality/Privacy(Sec. 72 of IT Act)	93	16	20	25	30	13	6	-53.8
12	Disclosure of Information in Breach of Lawful Contract@(Sec. 72A of IT Act)	-	2	4	100	-	5	2	-60
13	Publishing/Making Available False Elect. Signature Certificate (Sec. 73 of IT Act)	4	0	3	-	8	0	0	-
14	Create/Publish/Make Available Electronic Signature Certificate for Unlawful Purpose(Sec. 74 of IT Act)	71	3	3	0	51	5	3	-40
15	Others	274	769	514	-33.2	161	520	245	-52.9
Total Offences under IT Act		**4,356**	**7,201**	**8,045**	**11.7**	**2,098**	**4,246**	**5,102**	**20.2**

Note: '-' implies sezo value in previous year. % Var. – refers the Percentage Variation during 2015 over 2014
"@ implies data collected in 2014 for the first time

TABLE 2 CYBER CRIMES/CASES REGISTERED AND PERSONS ARRESTED UNDER IPC DURING 2013-2015

Sl. No	Crime Heads under IPC Crimes	Cases Registered			% Var.	Persons Arrested			% Var.
		2013	2014	2015		2013	2014	2015	
1	Offences by Public Servant	1	0	0	-	2	0	0	-
2	Fabrication/Destruction of Electronic Records for Evidence	12	1	4	300.0	11	1	2	50.0
3	Cheating@	-	1,115	2,255	102.2	-	335	754	55.6
4	Forgery	747	63	45	-28.6	626	58	72	19.4
5	Data Theft@	-	55	84	52.7	-	11	135	91.9
6	Criminal Breach of Trust	518	54	42	-22.2	471	39	1,292	97
7	Counterfeiting *	59	10	12	20.0	93	8	14	42.9
8	Others	-	974	980	0.6	-	772	598	-29.1
Total Offences under IPC		**1,337**	**2,272**	**3,422**	**50.6**	**1,203**	**1,224**	**2,867**	**57.3**

Note * includes property marks, tampering and currency/stamps till 2014 and currency & stamps during 2015
Note: " -" in the column of percentage variation implies zero value in previous year
"@" implies newly entered crime heads. '% Var.' – refers to Percentage Variation in 2015 over 2014

Table 1 shows variations in cases of IT Crime or Cybercrime cases registered from year of 2013 to 2015. Whereas person arrested in cybercrimes in year 0f 2014 varies 20.2 percent compared to year 2014. This are indications for increase in cybercrime cases and arrest against complaints. In India prices of smartphones are becoming cheaper day by day as market of smartphone is increasing due to this users of smartphone are increasing, also cheap internet packs are another reason for same. Table 2 indicates 57.3 % variations in person arrested in 2015 [6]. Table 3 indicates tremendous increase in internet users across India. India shares 13.5 % of world internet users. It leads to unsecure environment because only internet users are increasing but awareness of internet security is not increasing in that ratio. Unsecure mobile devices are easy to use for cybercrime because of low security. Mobile devices not only have data in form of images or contacts but essential information in form of mobile banking apps, social networking apps and many more. So it essential to know all about mobile devices and security.

TABLE 3 STATISTICS OF INCREASE IN INTERNET USER IN INDIA FROM YEAR 2000 TO 2016

Year	Internet Users**	Penetration (% of Pop)	Total Population	Non-Users (Internetless)	1Y User Change	1Y User Change	Population Change
2016*	**462,124,989**	34.8 %	1,326,801,576	864,676,587	30.5 %	108,010,242	1.2 %
2015*	**354,114,747**	27 %	1,311,050,527	956,935,780	51.9 %	120,962,270	1.22 %
2014	**233,152,478**	18 %	1,295,291,543	1,062,139,065	20.7 %	39,948,148	1.23 %
2013	**193,204,330**	15.1 %	1,279,498,874	1,086,294,544	21.5 %	34,243,984	1.26 %
2012	**158,960,346**	12.6 %	1,263,589,639	1,104,629,293	26.5 %	33,342,533	1.29 %
2011	**125,617,813**	10.1 %	1,247,446,011	1,121,828,198	36.1 %	33,293,976	1.34 %
2010	**92,323,838**	7.5 %	1,230,984,504	1,138,660,666	48.5 %	30,157,710	1.38 %
2009	**62,166,128**	5.1 %	1,214,182,182	1,152,016,054	18.6 %	9,734,457	1.43 %
2008	**52,431,671**	4.4 %	1,197,070,109	1,144,638,438	12.5 %	5,834,088	1.47 %
2007	**46,597,582**	4 %	1,179,685,631	1,133,088,049	42.9 %	13,995,197	1.51 %
2006	**32,602,386**	2.8 %	1,162,088,305	1,129,485,919	19.3 %	5,275,016	1.55 %
2005	**27,327,370**	2.4 %	1,144,326,293	1,116,998,923	22.8 %	5,067,787	1.59 %
2004	**22,259,583**	2 %	1,126,419,321	1,104,159,738	19.1 %	3,567,041	1.63 %
2003	**18,692,542**	1.7 %	1,108,369,577	1,089,677,035	11.5 %	1,926,786	1.67 %
2002	**16,765,756**	1.5 %	1,090,189,358	1,073,423,602	136.9 %	9,689,725	1.71 %
2001	**7,076,031**	0.7 %	1,071,888,190	1,064,812,159	27.3 %	1,518,576	1.75 %
2000	**5,557,455**	0.5 %	1,053,481,072	1,047,923,617	96.5 %	2,729,647	1.79 %

* estimate for July 1, 2016

** **Internet User** = individual who can access the Internet at home, via any device type and

II. LITERATURE REVIEW

Chauhan and Singh in their research 'Security Risk Associated with Android Applications' concluded Android developer has few restrictions in development of application for android, which leads security risk for android users. Also Android OS fragmentation by manufacturer of smartphones and lack in releasing security updates increases low security [7].

Enck, et. al. on their research 'A study of Android application security', concluded risk of android application is higher due to low restriction were given to developers of android application. Their findings of exposure of phone identifiers and location are consistent with previous studies, analysis framework allows them to observe not only the existence of dangerous functionality, but also how it occurs within the context of the application [8].

Kirandeep and Garg tried to suggest security for android application in their research on 'Implementing Security on Android Application' but it was limited to contacts, call logs and location or phone identity. While using their system, as per system use sometime it will send wrong response to the user corresponds to their request. These fake replies could create problems for some applications of android. To provide more security this system can be improved so that user can easily access this app in a friendly manner. This system does not provide instructions for using privacy settings [9].

Powar and Meshram discussed on three approaches for the security of Android. At installation on android devices Kirin and Lightweight approaches are used for securing application with permission grant and other security restrictions. This approach cannot work at runtime; this is drawback of Kirin approach. Kirin does not support check on dynamic broadcasts. In Android Permission Extension Framework (Apex) approach, it continuously checks the application behavior while running, and on base of decided policy don't allow particular application to do something for which permission is not granted. If user grants such permissions by mistake to an application which can be produce harmful. This can be solved by conjunction of Kirin with Apex, in which analysis of constraints and permissions should be done for verifying violation of security rules [10].

Tiwari et. al. in research on "Android Malware Detection Using SVM and GA" wrote on weakness in android security, Android has no management over the apps being uploaded on its market. Some apps exploit the services of another app while not creating a permission request. Android's permission primarily based security model offers power is given to the user to create a decision whether or not an app ought to be trustworthy or not. This human part introduces lots of risk. The idea of an Open supply OS isn't solely open to legitimate developers however conjointly to hackers. So complete framework of android can't be trustworthy once it involves building vital systems. The android OS developers clearly state that they're not answerable for the protection of secondary storage. Any app on the android platform will access device information just like the GSM and SIM trafficker Ids while not the permission of the user age [11].

Users unknowingly does not use security settings and configuration which may lead to make personal information on device unsecure. Attacks can be occurring by two ways, first is due to unawareness and other is system defects. Most of attacks make use of vulnerabilities in smartphone operating system. The threats appear on mobile devices are Rootkits, Trojans, Botnets which came from daily used applications and this is very hard to replace. For this user should aware of this for keeping track of usability and threats of such application of android operating system. Mamun and Alam in their paper brief about vulnerabilities due to user unawareness on Malware, Peripheral Interfaces Attacks, Data hijacking [12]. Kaur wrote about technique used to attack on android device are as Spam, Phishing, Spoofing, Sniffing, Vishing, Pharming, Denial of Service attack [13]. Privilege escalation, Version Update Issues, Native Code Execution, Security Enhancements in the Recent Versions, Third-Party Security Enhancements these are also threats for android security [14].

III. SURVEY ON USER AWARENESS

For research purpose data collection was done on group of 100 android users. These questions were asked for recognizing habits of users for using android devices. Questions were asked related to security settings, locking device, sharing information on social media. List of question to users for data collection are given below.

1. How many hours you use internet?
2. Do you use public Wi-Fi?
3. Do you use shared HOTSPOT from other android phone?
4. Do you share your internet?
5. Do you set password to LOCK / UNLOCK phone?
6. Do you use banking apps?
7. Do you save bank account number, PIN, PAN, PASSWORD Other sensitive information on android phone?
8. Do you read instruction while installing any APP?

9. Do you know permission for APPs?
10. Do you ALLOW permission while installing apps?
11. Do you enable USB debugging?
12. Do you enable Install from unknown sources?
13. Do you ROOT android device?
14. Do you use any unauthorized APPs?
15. Do you use any Wi-Fi password cracker Apps?
16. Do you hide your personal information?
17. Do your backup data from android to other location?
18. Do you update Android OS?
19. Do you update APPS regularly?
20. Frequency of backing up data
21. From where you install APPs
22. Do you share your phone with other person?
23. Do you enable GPS while using internet?
24. Do you save your documents on third party location?
25. Do you install antivirus app?
26. Do you change passwords regularly on Mobile phone?
27. Do you use social networking APPs?
28. Do you share sensitive data through social networking apps?
29. Do you ALLOW remember password?

IV. DATA ANALYSIS AND INTERPRETATION

Collected data from survey indicates facts about usage of android device. The analysis of data collection about unawareness is shown and described by using following figures.

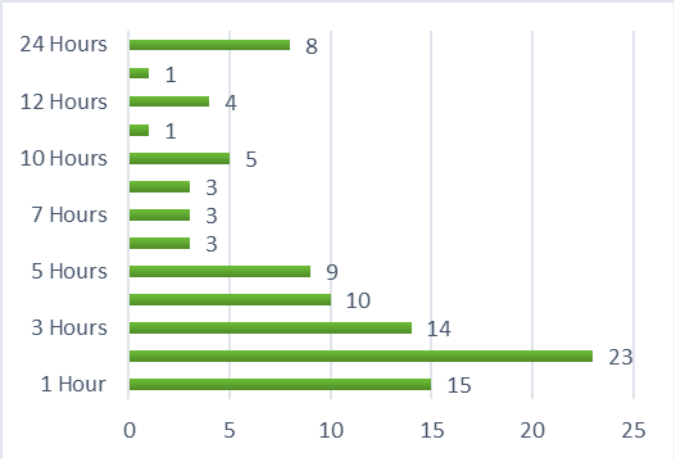

Figure 1 Use of Internet On Android Device

Android device users averagely access internet 1.11 hours per day. Actual percentage of accessing internet hour wise is shown in Figure 2. It varies from user to user, but most of them access internet at least 2 hours daily.

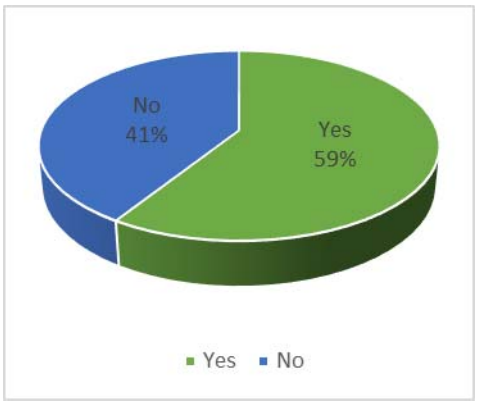

Figure 2 Use of Public Wi-Fi

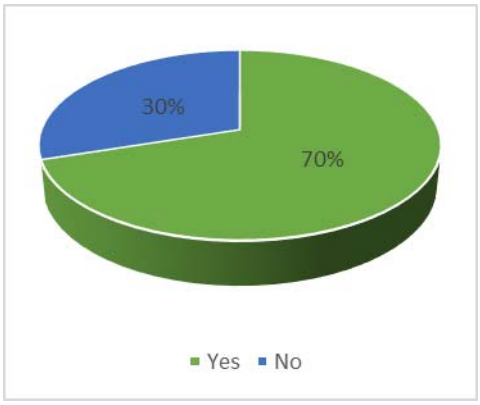

Figure 3 Use of shared Hotspot from android devices

Figure 3 shows 59 % users access public Wi-Fi and this is very bad practice due to this anyone can exploit android device for misuse. In general, public Wi-Fi are unsecured that's why it's always good to avoid use of public Wi-Fi.

Figure 4 shows 70% android users fetch internet from shared HOTSPOT from other android devices which may leads to insecure environment, as receiver device in connected to sender device. So sender may be having rights for accessing receiver side device because of this a wrong opportunity created due to this receiver side device can be misused. This can give control of receiver device for malicious use.

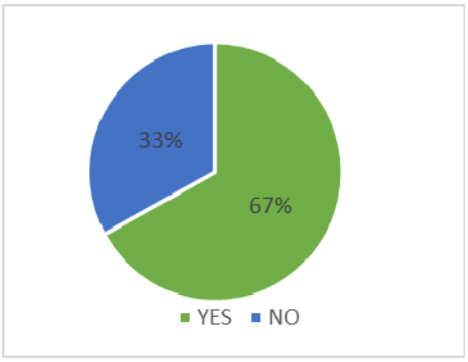

Figure 4 Sharing internet for other devices

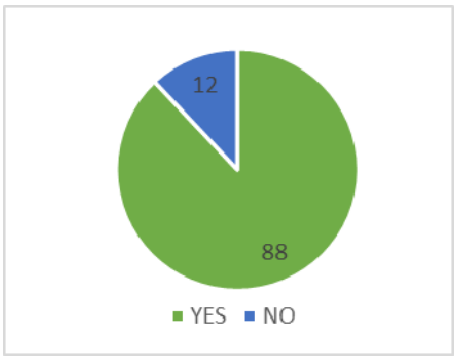

Figure 5 Use of Password for Unlocking device

Sharing internet from own android device also leads to vulnerability, above Figure 4 shows 67 % android users share internet from them. 88 % android device users set password to lock or unlock device which shown in above Figure 6. Remaining 12% users avoid setting password which can lead to misuse of personal data in case of theft or loss of device. In case of lost or theft of device reset or format is required to use device which means personal data erased while resetting or formatting device. In other words, setting password for locking or unlocking device secures personal data.

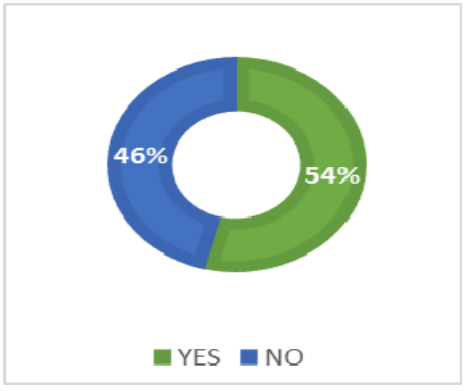

Figure 6 Using banking apps

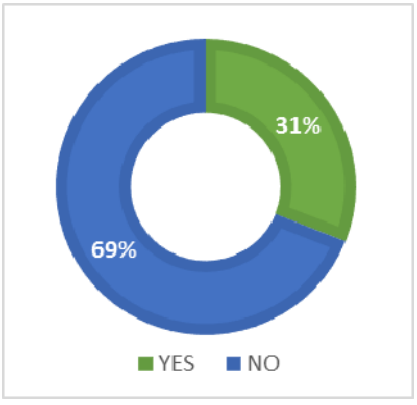

Figure 7 Storing sensitive information on device like bank account number, pin, pan, password

Figure 7 shows 54% of android device users install and use banking applications on their android device. Using banking apps on device is good but setting a proper security for them is also mandatory for avoiding misuse of device.

Figure 8 a good habit of android users has been detected that 69% users don't save sensitive information on device. Whereas 31% of users save these type of information in device.

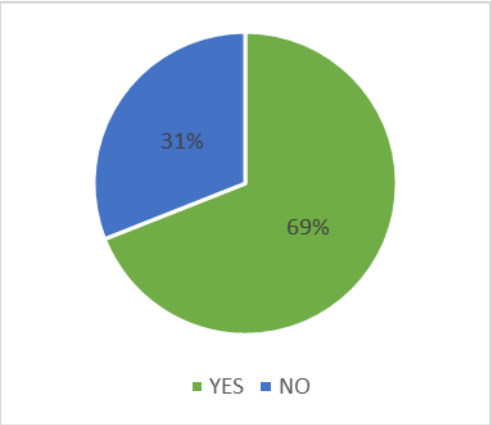

Figure 8 Reading instructions while installing application

Figure 9 shows facts about reading instructions while installation of application on device. 69% of users read instruction for application while installation whereas 31% users ignore reading instructions.

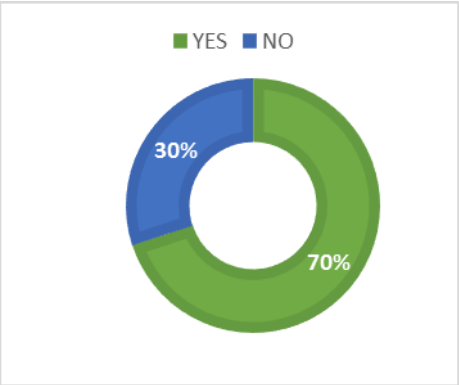

Figure 9 Awareness about permission for apps

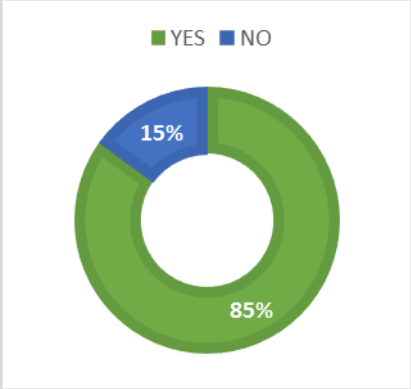

Figure 10 Setting permission while installation of apps

Figure 10 shows 70 % of user has awareness about permissions for application on other hand 30 % users don't know what are permission for application. Figure 11 shows 85 % of android users allow permission while installing apps.

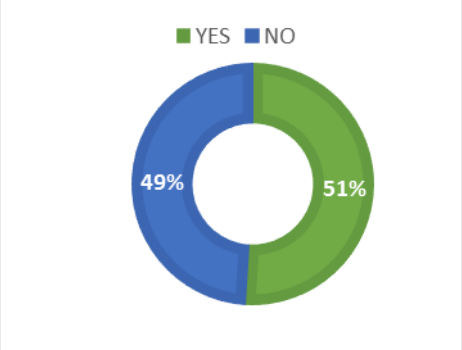

Figure 11 Settings for installation from unknown source

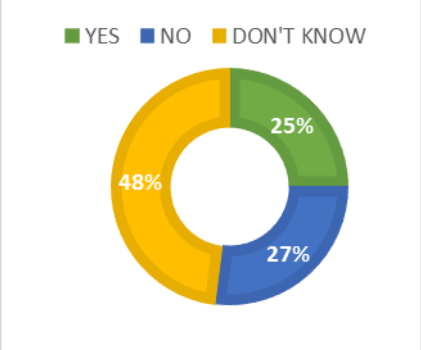

Figure 12 Rooting Android Device

Figure 12 shows 51 % of android users enable setting of install from unknown source. It is shown in Figure 13 that 27 % of users don't root their android device which avoids hacking or misuse of device due to unauthorized use through operating system, 25 % users in survey use rooted android device which can create trouble to device through hacking or misuse of device as rooted device is easy to crack and 48 % users are not aware of root device.

TABLE 4

Question No.	Question	Frequency (in %)	
		YES	NO
1	Do you use any unauthorized APPs?	24	76
2	Do you use any Wi-Fi password cracker Apps ?	22	78
3	Do you hide your personal information?	78	22
4	Do you backup data from android to other location ?	73	27
5	Do you update Android OS ?	83	17
6	Do you update APPS regularly ?	84	16

Table 4 has six questions and frequency of answers in form of YES and NO is shown. Frequency of answers for Question 1 and 2 from Table 1 shows that 76 % users avoids to use unauthorized app and 78 % of users also avoid Wi-Fi cracker apps. 78 % user hide their personal information in android device using different method provided by android operating system. 27 % users don't take backup of data from android device to other location which may leads to loss of important data in case of theft or loss of device.

Updating android operating system makes device secure because of new updates, 83 % of users update android operating system which makes their respective device secure where and 84 % users updates android application regularly which also leads to better secure environment. Updating application not only makes secure but also removes bugs from old version of applications.

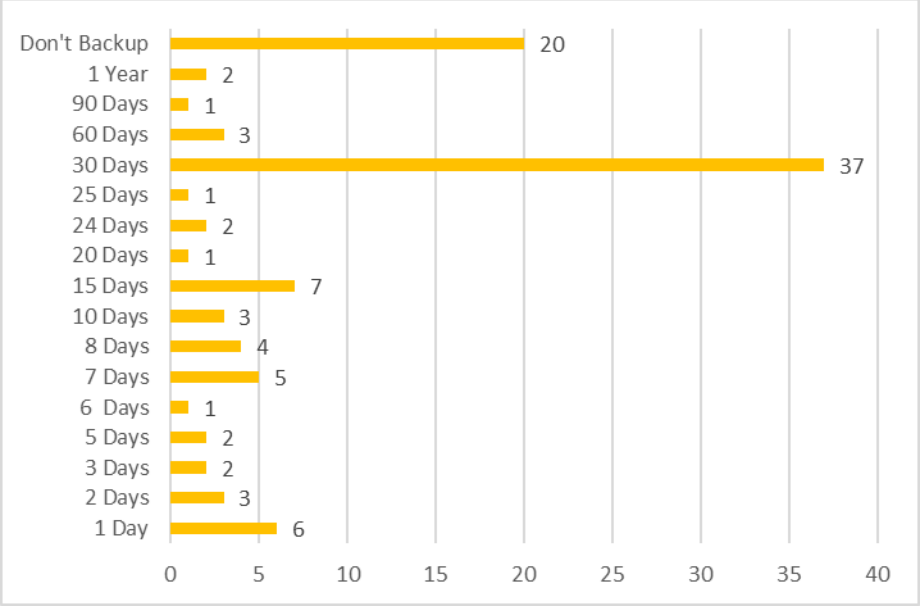

Figure 13 Frequency of Backup

Figure 14 indicates frequency for backing up data on other location than same device. In which 20% people skips for backup od data which is a bad habit due to this huge data loss can happen in case of device loss or crash of operating system. 37% people takes backup monthly which is a good habit, it makes data secure in case of loss or theft of device. Other frequencies of backup of data are shown in Figure 14.

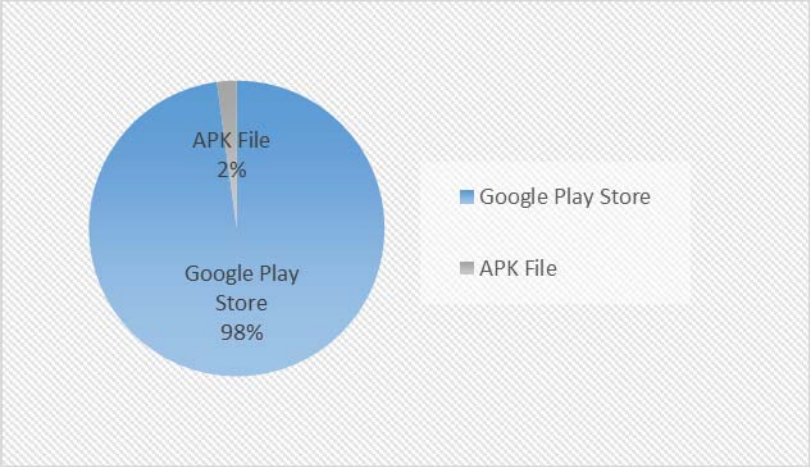

Figure 14 Installation Source For Applications

Figure 15 shows 98 % of android users in survey choose safe and secure procedure for installing applications on android device. Only 2 % of users choose shared or third party locality to acquire apk files for installation. Choosing third party location or shared location is an unsure way. Avoiding such type of ways for installation is better for securing against attack by hacker.

TABLE 5

Sr. No.	Question	Answer (In %)	
		YES	NO
1	Do you share your device with other person ?	50	50
2	Do you enable GPS while using internet?	54	46
3	Do you save your documents on third party location ?	37	63
4	Do you install antivirus app ?	68	32
5	Do you change passwords regularly on devices ?	66	34
6	Do you use social networking APPs ?	94	06
7	Do you share sensitive data through social networking apps ?	32	68
8	Do you ALLOW remember password ?	41	59

Table 5 specifies frequencies in percentage for questions asked to people in survey. Question 1 from Table 5 shows frequencies in 50-50 % for sharing own device with other person. For Question 2 54 % people choose YES for enabling GPS while using internet which is somewhat useful in case loss or theft of device. In this case finding device is become easy due to tracking trough GPS. But in case where hacker is using your device for getting location is unsafe to user.

Saving documents on third party location as google drive or available application in Google Play Store make easy access to documents but also it can also aid for hacker for exploitation. From survey results it is found that 63 % users avoid to store documents on third party locality. Using Antivirus applications makes device safe and secure, 68 % users install antivirus app on device which is a decent exercise. 66 % users in survey change password frequently that help them in avoiding misuse of device.

When users were asked about use of social networking applications, in reply it was found that 94 % of user usage social networking applications for sharing. 68 % users avoids sharing sensitive data on social networking application. 59 % users don't allow to remember password because of this a good rehearsal by which security has been made by user to keep away exploitation of password for any illegal activity.

Analysis of collected data from various responses identifies some facts which can use for securing device. Precaution can be taken as don't open emails until essential. Don't give personal information such as your address, phone number, date of birth to avoid misuse of sensitive information for alteration of password, resetting PIN. Do not follow links in email or text messages until required. Estimate security settings on device on which accessing accounts or personal data. Always use strong and lengthy password. Use Email Filters for avoiding to get mail from unknown person. Avoid to use of open Wi-Fi hotspot for accessing your social accounts. Don't let others peep into your accounts. Turn on Blue Tooth or enable Internet only when required. Do turn off the wireless connections when not needed. Never share personal information with stranger. Never

store personal banking details in cell phones. Be suspicious while entertaining strangers on social networking website. Consider disabling the geo-tagging feature on your phone. If you are connected to a public Wi-Fi, don't access sites where you need to enter your password, credit card information etc. While banking and shopping online, ensure the sites are https or shttp. Android security is improving but still lot more to improve in future. Mobile security should be taken more seriously as increasing use of internet and mobile devices. Understanding security and protecting should be one of everyone's priorities.

V. CONCLUSION

Though it is very difficult to provide complete security in android devices, safe and secured way to use smart devices definitely avoid exploitation by hackers. Nowadays personal and sensitive information is kept on smart devices for fast access so it is our own duty to consider it is one of our priority to keep it safe and secure. Mobile security should be taken more seriously as increasing use of internet and mobile devices. Understanding security and protecting should be one of everyone's priorities. This can be avoided by taking precaution while handling devices and this is easy way to make android device safe and secure.

REFERENCES

[1] I. U. F. Sajid Nabi Khan, "Review on Android App Security," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 7, no. 4, pp. 225-228, 04 2017.
[2] "Internet IAMAI in India-IMRB Report – 2016," 2016.
[3] "Mobile and tablet internet usage exceeds desktop for first time worldwide," 01 11 2016. [Online]. Available: http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide. [Accessed 10 05 2017].
[4] K. I. &. MMA, "Smartphone Usage and Behaviour Report," Kantar IMRB & MMA, 2016.
[5] C. India, "State of Mobile Operating System Adoption in India," CMR, 2016.
[6] "Cyber Crimes," National Crime Record Bureau, 2016.
[7] M. S. Chauhan and K. S. , "Security Risk Associated with Android Applications," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, no. 5, pp. 711-714, 2016.
[8] William Enck, Damien Octeau, Patrick McDaniel and Swarat Chaudhuri, "A Study of Android Application Security," [Online]. Available: http://www.cs.rice.edu/~sc40/pubs/enck-sec11.pdf. [Accessed 25 12 2016].
[9] Kirandeep and A. Garg, "Implementing Security on Android Application," The International Journal Of Engineering And Science, vol. 2, no. 3, pp. 59-59, 2013.
[10] s. powar and B. B. Meshram, "Survey on Android Security Framework," International Journal of Engineering Research and, vol. 3, no. 2, pp. 907-911, 2013.
[11] M. Tiwari, A. K. Srivastava and N. Gupta, "Android Malware Detection Using SVM and GA," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 5, pp. 347-352, 2014.
[12] Tauseef Ibne Mamun and Lamia Alam, "Android Security Vulnerabilities Due to User Unawareness and Frameworks for Overcoming Those Vulnerabilities," International Journal of Computer Applications, vol. 137, no. 1, pp. 14-21, 2016.
[13] N. Kaur, "Techniques Used for Detection of Mobile Spyware," International Journal of Computer Trends and Technology (IJCTT), vol. 11, no. 5, pp. 217-219, 05 2014.
[14] P. S. Dhumal, "A Review on Android Security," International Journal of Modern Electronics and Communication Engineering (IJMECE), vol. 3, no. 3, pp. 53-58, September 2015.