Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

Assessing users Awareness and user Adaptation to the Android Privacy and Security

Attaullah
M.Sc. Student Department CS & IT
University of Engineering and Technology
Peshawar, Pakistan

Aamir Saeed
Assistant Professor, Department CS & IT
University of Engineering and Technology
Peshawar, Pakistan

***Abstract*— The Android operating system is used by most smartphones and has a huge number of users. App developers provide services in the form of apps. Due to the large user base and app developers, it must maintain the users' security and privacy. Android Apps are needed to access resource utilization after getting permission from the user. But the user does not read the app permission details for using the device resources and may grant excessive or objectionable permissions, where Android gray-ware app developers collect large amounts of personal information through such apps. The user is also unaware of what type of permission they are granting to the apps. This paper presents an assessment method for examining the security and privacy controls of Android users' adaptation to the Android permission model. The study consists of evaluating Android users' attention while installing or understanding the purpose of the permissions during or after installation. So, the assessment will be carried out through an Android app whose sole purpose is to monitor all the permissions granted to every installed app on the device. During the study, it was discovered that the data set of 102 users paid little attention and were granted unnecessary permissions. Moreover, the android deployed permission model assessed, and we observed the literacy and awareness of users of the Android permission model is an essential factor that can control the misuse of a malicious app.**

Keywords*— *Android, Smartphone, App Permissions, Privacy and Security, App Developer, Malicious apps.

I. INTRODUCTION

Most smartphones come with the Android operating system pre-installed. The operating system has an enormous user base and application developers to provide state of the art services and applications [1]. Due to the huge user base and application developers, the operating system should retain the security and privacy of the users [2, 3]. The app store is the primary location for app distribution. Developers can use the store to publish their apps and manage their updates. Users can find the required apps through the store app. App store providers can filter which apps they allow or ban if they are identified as malicious. However, sometimes store operators might accept apps but not deeply review, i.e., their restricted permissions; instead, after thousands of downloads or installs and flag reports from the user side, the store starts the review. The App is developed for sending SMS. Why does it use cameras, GPS permissions, etc.? Stores sometimes ignore such issues, which is why user profiles are leaked and used for advertising purposes. Another issue The Android operating system does not prevent apps from being installed from an unknown source. It just alerts users to privacy- or security invasive applications. The security and privacy concerns of users are being given importance. But the user may grant excessive or objectionable permissions [2]. Objectionable permissions include location access, SMS, storage, contacts, call logs, cameras, MIC access, etc. In principle, apps' users must be aware of privacy issues and malicious attempts made to access various resources [3]. Investigating user awareness and consciousness of user privacy concerns is worth evaluating. Moreover, the operating system deployed permission models assessed. There we observed that the literacy and awareness of users is the main factor that can control the misuse of malicious apps. The privacy and security breaches are due to the neglect of user focus and the gray hole in the operating system permission model.

The aim of the study is to be literate and aware that users can control the misuse of malicious apps. The objective is to reduce the technicalities of the permission model from users' point of view and allow them to spend less time know the access of permissions for resource utilization in the device. This paper will also help policymakers and permission model designers to thoroughly analyze the existing permission model and define a refined permission model.

II. LITERATURE REVIEW

The primary focus will be on Android mobile privacy and security. The security and privacy concerns are of primary importance for each application. The deployment of third-party applications has posed security and privacy threats [6, 13]. Android has introduced a permissions model to regulate third-party application developers to maintain users' privacy and security [2].

The permission model was too simple when Android 1.0, and their apps are without permission. In Android 3.0 the permission model to prevent apps from external storage access. The permissions model of android 4.4 the apps required permission during installation. Also, internal storage permission is added. However, the issue is that all the permissions are asked at once. In Android 5.0 permission model, many permissions are added, but still, permission based on install time permission once asked, never ask it again. One of the powerful permission models introduced in Android 6.0 [15]. The permission model was asking user permission during the initial installation of apps. However, the App never asked after the installation. As a result of this approach, the privacy of the users was violated, and the user was unable to differentiate between the required permissions and those unnecessarily acquired [7, 8, 9, 10].

Panagiotis et al. [19] developed and published an App to gather data relevant to the resources access permissions. They

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

analyses users' attention and illustrates that our users showed a constant value pertinent to the resources that different apps can access. Al Jutail et al. [15] developed the Sparrow application to assist users in determining whether the app needed to be installed or not and whether it is safe to install. This app scanned the app's manifest file to check dangerous permission. However, it does not scan the internal communication of the app with the operating system.

The most soughed information that has been retrieved from mobile devices is primarily focused on location tracking and sharing [7, 8, 9, 10, 11]. Location information sharing is a piece of critical information that can endanger user privacy. The App that collecting location-based information might not be crucial for the process, but it may great privacy risk.

Several studies highlighted user behavior in granting permission to the apps [12]. Most users pay no attention to operating system alerts that are related to permission requests [2, 5, 12, 14], and the device user gives full access to the App to access the resource and share sensitive data.

Studies demonstrated that users were regularly staggered by an app's ability to gather personal or sensitive data in the background process and send such data remotely to third parties [4]. The Advertisement libraries or API revealed a tendency in advertisements networks to become more offensive in gathering achievable user data [1].

Some research aim is the detection of malware. Since a higher percent of malicious and vulnerable apps target the Android Operating system [17]. Furthermore, the conventional methods for malicious app detection, such as signature-based or behavior-based identification [18]. Permissions itself to be used as a tool to detect mobile malware. Apps with less functionality and more permissions require consideration of low-quality Apps, or permissions pattern can quickly notice that it might be malicious. Some of the methods were found that represent apps and their permissions for anomaly detection, which only work because they only examine a relatively small number of apps.

Based on a review of the current research and development, we conclude that our study would provide an analytical model supported by experimental and feedback-based information about security and privacy breaches. To reduce technicality from the permission model from users' point of view and allow them to spend less time understanding and responding to a warning message.

III. RESEARCH METHODOLOGY

The research methodology to conduct the study is to develop a systematic style for understanding the android permission models and developing a strategy to investigate user behavior to grant permission to accomplish said tasks. An android app would be designed with the core functionality of Permissions Monitor (PermTool). It would act as a survey gadget. Data we collect includes name, age, email, location, gender, education level, and app permissions information installed on the device. (Email address will get from the current Google account while using ip-api.com for location information). We collect some of the other data from a user about Device API, user apps, system apps, or pre-installed apps. We also prepared a list of 44 different types of apps for our survey, including social networking apps, Health fitness, Online Banking, Educational, Designing, Digital Marketing, Entertainment, News apps, and some popular games. So, the app will collect information about such apps if some or all the above apps are installed on a device.

We also conduct a survey in-app to get information from a user to identify whether users know about permissions and their usage or not. The PermTool app would be installed on the devices of the volunteer participants. The users will be needed to download and install the application from the Google official store (Play store) on their devices. We will provide the usage terms and conditions agreement to a user. If a user agreed, the application would continue executing and performing the data collection tasks and accomplishing the survey. After the user completes the survey, the app will send data in the background, including app details, permissions, and survey questionnaire responses.

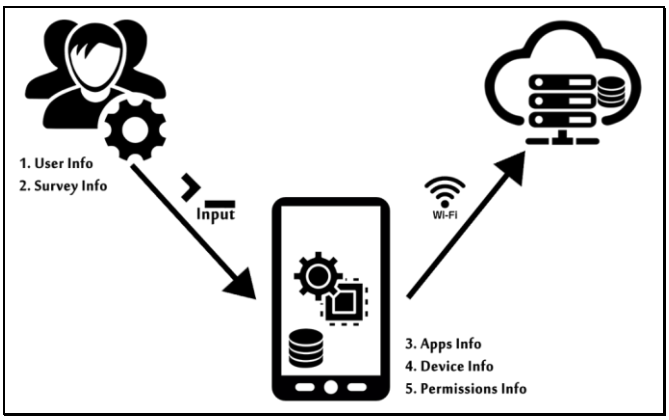

Fig -1: Data Collection system

Figure. 1. Two tasks need to be completed. From the user side, are User Info and Survey Info, On the other side, three tasks: Apps, Device, and Permissions Information This data will be collected automatically through the device (PermTool) itself. Send it VPS.

A. Android Phone app

We will develop an app for collecting information. The information will be collected in the local storage of the android device. In case of Internet availability, the collected information will be retrieved from local storage and submitted to a virtual private server (VPS). Our design application will consist of three activities: Register, Survey activity, and Permission Group activity. Suppose the user information has been submitted successfully from Register activity to VPS. In that case, the app will hide two activities, Register and Survey activity, while Permission Group activity will display for user interaction with application permissions. In case of failure in submitting the user information, none of the activities/buttons will be hidden. If only the survey were submitted, the "Survey" button would disappear. Similarly, if only the user information is submitted to VPS, the "Register" button will disappear from a user. It can be shown in figure 2, where all the activities are illustrated.

Figure. 2. The first activity is an agreement on usage terms and conditions. The second activity is about user information, the third activity is a research survey activity, and the last is Permissions Groups, where the user interacts with app permissions.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

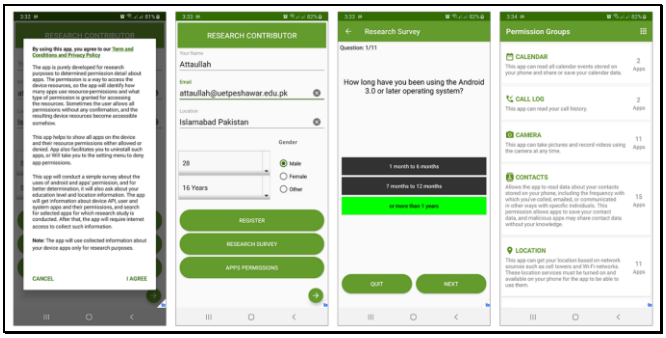

Fig -2: PermTool app Activities

IV. DATA ANALYSIS AND DISCUSSION

We developed the app PermTool through this app, more than a hundred participants data are collected and analyzed. The collected data includes user demographical data and survey responses from the participants. PermTool helps us a lot while collecting device information. After that, we extract valuable features from that. We noticed that some of the participants did not send their demographical data instead sent survey questionnaire responses and device information, sent automatically by the PermTool app. We represented and analyzed data in graphical forms.

A. Analyzing User Information

We also notice most of the participants are most educated, and their age is between 21 to 35 years, which is about 80% of the participants. Most of them are unaware of the device resource permissions, and most users favor improvement in the protection of their device privacy. The participants also trusted that our privacy and data were secured, but they were unaware of the permission models and blindly allowed access to resources.

B. Analyzing Research Survey Questionary Data

According to our survey questionnaire, we have 11 questions with predefined answers. The total response on the questionnaire is 102. In response to the 1st question, which is about the Android operating system's usage, 36% of the respondents had been using Android for an interval of 1 month to 6 months. 6% had been using 7-12 months, and 58 percent of users were using android for more than a year.

In response to the 2nd question, which is about knowing the permissions model, 10 percent of users responded, "I Don't know", 22 percent of users responded, "Little bit". In comparison, 69 percent of participants knew about the android permission model.

In response to the 3rd question about Android runtime permissions, 16 percent of participants responded, "I Don't know". 26% of participants' responses were "Little bit" and 58% of responses knew about runtime permission.

In response to the 4th question, which is about permission for resource access, 5% of the responses were "Disagree". 11% of responses were "I Don't know". And maximum i.e., 84% know that granting permission means accessing device resources.

In response to the 5th question, which is about the number of permissions granted to the app. 15% of the participants' responses were "I Don't Know", 22% of responses were "6-10 permissions", and 64% of participant responses were "1-5 permissions" allowed for each app.

In response to the 6th question, it is about observing the variation in the permission model of different android versions. The 34% of participants' response was "I Don't Know". 11% disagreed with the permission model's variation, and 55% of participants agreed with the variation of the permission model.

In response to the 7th question, which is about participant command over personal data. 17% were unaware of personal data, and their response was "I Don't Know". Similarly, 23% of responses were "Disagreed", which means that sure participants know that their data remains unsecured. In comparison, 61% of participants' responses agreed and knew that their data was secured.

In response to the 8th question, is revoking any App permissions anytime from the 'App Settings'. 18% were unaware of such an App Setting, and their response was "I Don't know". 21% of participants' responses were "Disagree" while the rest of the participants knew about revoking permission from the app setting.

The 9th question, which is about the runtime permissions model, is aggravating because runtime permission asks many questions while using the app. 26% of the participants were unaware of the annoying from the runtime permissions. Their response was "I Don't Know". 14% of respondents were "Disagreed" with the irrelativeness of the runtime permission model. In contrast, the rest of the participants agreed.

In response to the 10th question, which is about favor of runtime permissions. 30% of the participants' responses were "I Don't Know". 8% of respondents disliked the runtime permission, and their responses were "Disagree". while the rest of 62% were in favor of the runtime permission.

In response to the 11th question, which is about a suggestion to make the permission model more user-friendly, 17% of participants were not interested, and their response was "I Don't know". 7% of participants were "Disagree" with making permission more user-friendly. While the rest of the participants agreed to make the permission model more user-friendly.

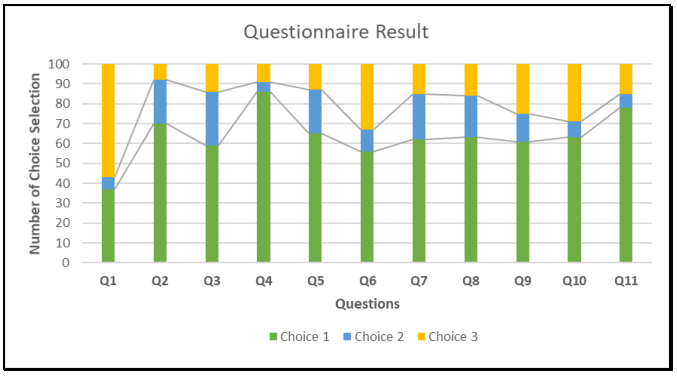

Fig -3: Shows that number of choices selection.

C. Analysis of Device API

Based on collected data, we analyzed that many users using Android 10 have API-29, and according to our survey, 30

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

percent of users use API 29. usage of API-28 is 26 percent. API 23, 26 are 16%, and 12 percent used, respectively. The API 24, 27 uses 4 percent, while the rest of the APIs are 7 percent used. We know that runtime permissions introduced by Google for Android 6 have API-23 and later versions of the android; the current stable version is Android 11 and has API-30. Only 2 percent of the participants have android 11, and the minimum API-18 is used in the survey, which is Android 4.3. The usage of APIs is shown in the figure below.

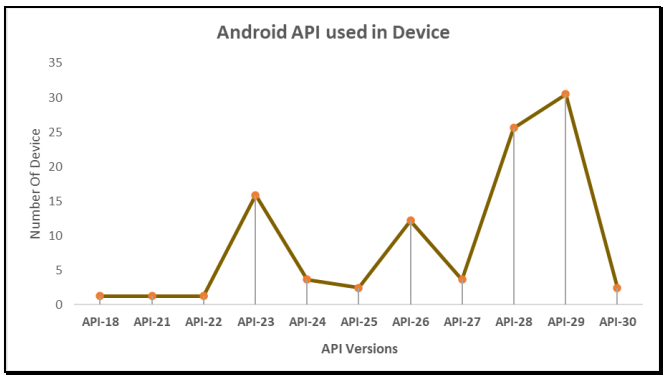

Fig -4: Android APIs usage in survey

We noticed from the data set the Device API is directly proportional to permission because API levels tend to increase. The number of defaults and dangerous permissions is also increasing. We examine that older device apps have a smaller number of permissions. While the latest device with the same apps has the maximum number of permissions, it can be shown in the figure below.

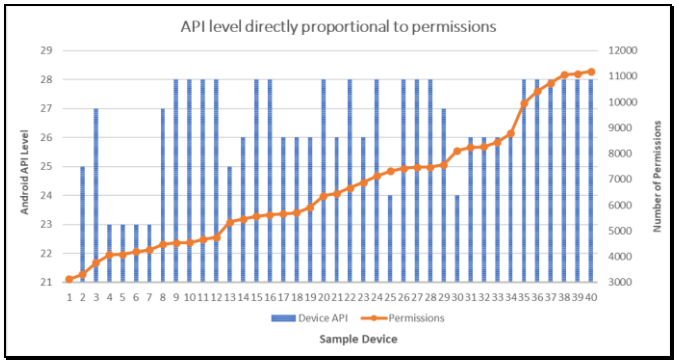

Fig -5: APIs level directly proportional to Permissions.

D. Analysis of User and System App

According to our survey, on average, user app 50, and 256 system apps are installed on mobile devices. We noticed that the minimum number of system apps on a single mobile device is 12 user and 63 system. Similarly, we found the maximum number of user and system apps installed was 179 and 417 on a single mobile device. We also found that, based on sample selected devices, the maximum number of apps on a device are system apps, i.e., 20% of apps are user apps and 80% are system apps. These results concluded from 40 sample devices of the survey. It is shown in the figure 6 below.

Fig. 6. On Android devices, system and user apps are available. It means that by default, every smartphone device has more system apps than user apps.

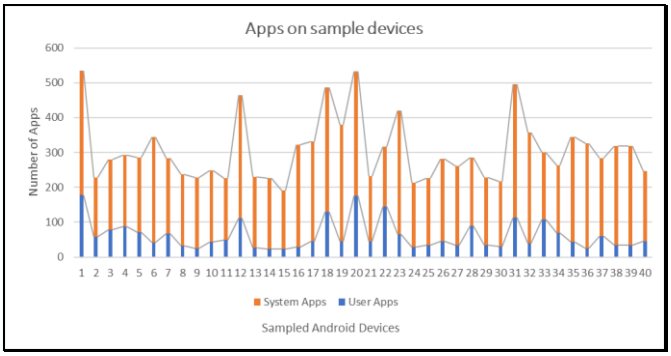

Fig -6: Apps on Sample devices

E. Analysis of Permission Grant or Denied

Permission grant or denied means that a user allows or denies the app to utilize the device resource, e.g., camera, contacts, GPS, etc. We collected data about granted and denied permission. We noticed that the average number of permissions that were allowed and denied from the apps was 5123 and 1294. The maximum number of permissions granted and denied in a device is 9089 and 2228, and 4 and 10 minimum permissions were granted and denied in a single device. Base on selected sample devices.

From the figure 7 of comparison of granted and denied permissions we can quickly Comparison of granted and denied permissions determine the number of granted permissions is more than denied permissions. It shows that fewer users are denied the app from accessing the device resource and denied their app permission. It may be possible that the user does not use an app, that app permissions are considered denied permission.

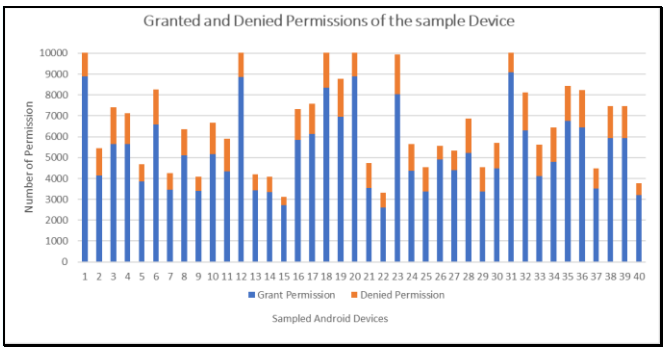

Fig -7: Granted and Denied Permission

Figure. 7. Comparison of granted and denied permissions. The orange colors represent permissions that were denied, while the blue colors represent permissions that were granted.

TABLE I. PRE-DEFINED APPS IN SURVEY

Statistics	Total Apps	Grant Permission	Denied Permission
Avg	8	194	126
Min	1	36	26
Max	17	428	254

Statistic of dangerous permission to pre-defined apps in survey devices.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

F. Analysis of Internet Permissions

The internet permission for mobile devices is considered in a group non dangerous permission, but most of the data or information is uploading through the internet. We collected the following data about internet permissions. In each device, the average number of internet permissions is 161. We identified the minimum number of internet permissions was 20 in a single device, and the maximum number of internet permissions was 349 in a device. Based on the selected sample device, we found the following result. It is shown in the figure below.

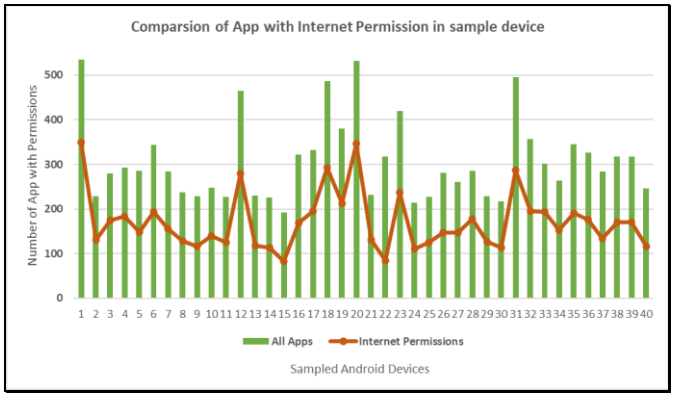

Fig -8: Apps with Internet Permissions

Figure. 8. Apps and their internet permissions. sample of 40 devices on x-axis and number of internet permission on y-axis, similarly the red line indicates number of permissions.

G. Analyzing pre-defined apps

We separate this portion from the analysis of device data because, as we know, we selected specific apps for research, including social media apps, health-related apps, educational apps, banking, and some other essential categories of apps to identify participants. The selection of the above apps identifies different types of users. Based on gender, for example, females use beautifying cameras and photo editors like apps. The Age base specifies their selection of apps like under 13 to 18 play gaming apps, and education level shows participants' professions. Moreover, we checked out how many participants know about permissions or not. Secondly, all information about permissions in the survey is collected in the background without user interaction. For every app, we assigned a unique key that identifies the name and description of the app in the app detail table. The main purpose of such a technique is to examine the users' awareness of mobile device privacy and security. Here we noticed that some users are not aware of device permissions. Certain users know about permission, but they do not know which permission, how many permissions are granted to a specified app and the purpose of permissions. Even in a survey, participants are highly educated. In survey question No. 5, we asked participants how many permissions they assigned to the app. The majority of users selected 1 to 5 permissions, however, when collecting data from the specified apps. We found out the number granted permission was more than ten.

H. Analysis of Permission to pre-defined apps

Similarly, we also collected data about permissions of the specified apps. Based on 10 sample selected device we concluded that 41% of apps permissions are denied while 59% are granted by user to the apps. UC browser, Facebook, and IMO are on top and have the maximum number of permissions. While WhatsApp, Facebook, and IMO are on top of granted permission apps. The data can be shown in the figure below.

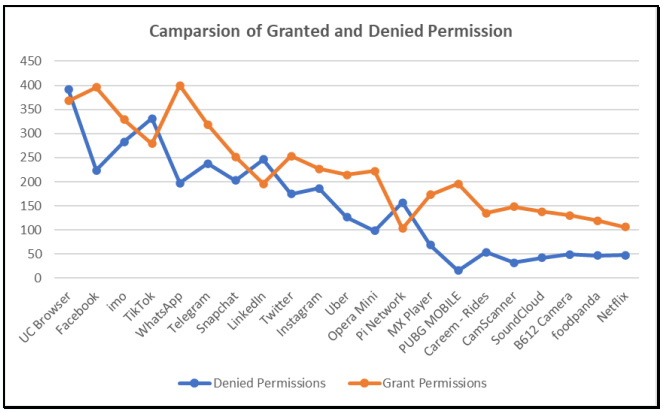

Fig -9: Granted and denied permissions for apps.

I. Analysis of Installed app and their Permission

We found many participants using social media apps, which is on top of the list, while cryptocurrency apps are on second, multimedia apps on third, designing apps on fourth, browser apps on fifth and sixth are educational apps. The rest of the apps were used, not mentioned.

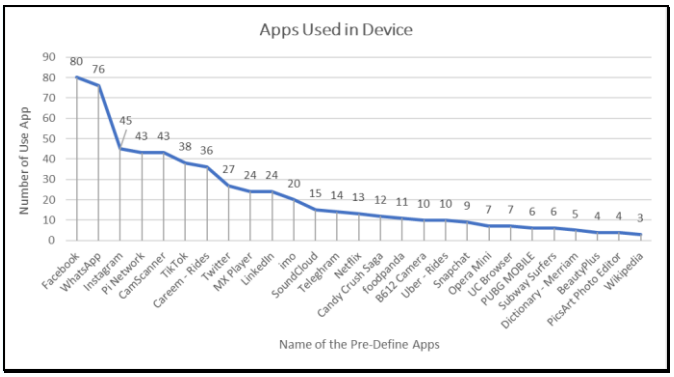

Fig -10: Usage of selected apps on survey device

At the end we examine that user could easily grant access to an app to access a device resource even if they are unaware of it. The excess of grant access permissions, and as a result, social media apps take advantage of the permissions to use device resources. It may or may not notify the user of its use before sharing its location details or contact information, etc. From the data set, granted permissions are more than denied permission. For this reason, there are more possibilities of serious breaches of personal data and privacy.

J. Analysis of Permission to pre-defined apps

We noticed from the data set there is no app without permission. We found the app has single permission but not without permission. Moreover, some of the apps with miscellaneous permissions were found. The miscellaneous permission, also called internal app permission, works internally in-app. Miscellaneous permissions are developed by the developer itself or developed by the device manufacturer, or developed by the API provider to access app resources or

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

services. We found that the devices' apps without permissions are 0.3%, and 27% of apps have miscellaneous permissions compared to all apps in the survey sample devices. It is shown in the figure below.

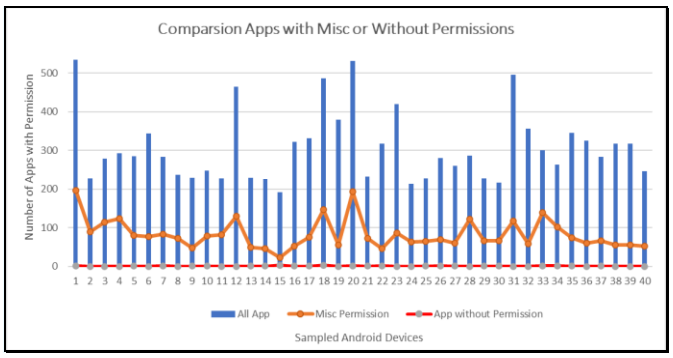

Fig -11: Miscellaneous permission with apps on device.

V. CONCLUSION AND FUTURE WORK

Our survey and collection of information do not improve the current privacy and security of the android device. However, it may be helpful to policymakers and permission modelers. Because if we see the result, we noticed that the users are educated but unaware of android permission. Users must be made conscious of issues and risks related to app permissions that access smartphone resources. The latest Android operating systems version need to increase the number of permissions. However, they do not irritate the user by asking and showing many dialogs or messages but make it more friendly and interactive. Due to the boring android permission dialog, users blindly allow access to an app to access resources. Permission dialog needs to be improved and provide a clear message to users. Similarly, there should be a need for a user-friendly mechanism to revoke access permission from the app. This factor also improves the security permission model. Android OS also needs to reduce the number of permissions to system apps. In other words, most of the device manufacturer apps have a series of permissions already assigned to the system application it also capturing unnecessary data and logs.

We also notice that the Play store contains some application developed only for advertisement purposes. While the ad company gathers data about the location and network details from users even though Google specifies in developer policy, "Mobile Unwanted Software" is restricted. However, they still allow such applications. So, the play store needs to select the quality of apps instead of an unwanted nonfunctional app. As we know from a survey, the user is concerned with their privacy. So, the Operating system should have a module or master app that notifies and monitors all the data visible to the user sent from the user or received from the server.

One significant finding was that 75% of apps use internet permission. Currently, this permission is considered by Android OS as Normal permission. Nevertheless, Internet permission needs to be considered as dangerous permission. Because any type of data uploading necessitates the use of the internet, if it is normal, then it causes serious breaches of privacy or personal information.

The installing of apps from unknown sources is also dangerous for devices to secure the device. Operating system need to make apps only downloadable from authentic sources or stores and restrict them from unknown sources. We observed that installing an app to an unknown source is always risky for a device from one literature review. Some devices manufactured have detection mechanisms for malware detection. However, it is not enough only for a specific device, but it is needed for the whole Android OS. To ensure that an app is secured and less risky. The operating system should have a technique or online security experts that quickly examine the app for installation or uninstalling. Currently, Google play protects only works on the Play Store. So, in the end, this work would offer policymakers and permission model designers to thoroughly analyze the existing permission model and define a refined permission model that provides the user with better permission granting models.

A. *Optimal Practices*

Before launching or installing an app, we must read and recognize the required permission details in the app. It will help us advance.

a. We need to download an application from an authentic source like the play-store. Because when a developer uploads an application to the Play Store, Google scans entire source code for malicious activities and permission and then approves the app. When we download apps from an unknown source, there is a greater chance that the apps contain malicious code that captures personal information or important data for misuse.

b. Some apps are helpful, but they have multiple dangerous permissions, so use alternative apps if they exist. Now, nowadays in the play store, there are multiple alternative apps for each app.

c. Avoid keeping unnecessary apps on the device. Apps that are only needed once a month or once a year must be removed from a device. Such as a hotel free Wi-Fi access app or information or resources about hotels. Most researchers found malicious activity on such apps. [16]

d. Do not try to root for a mobile device. It will give extra features to the device but installing multiple apps might contain malicious code that may steal our sensitive data, such as payment details and login passwords or other important store data. It might be dangerous in some ways to gain control of our phones.

e. Do not keep confidential data or information on a mobile phone if data is needed to keep it on a mobile phone. Data must need to be encrypted first. Because if a hacker wants to access such information, it will be unreadable.

B. *Limitation*

Every research study has some issues that affect the result. In our research survey, the main issue is the unavailability of internet access. Because many users download our PermTool app, but no data is sent to VPS due to the unavailability of internet access. The data is locally saved and submitted after a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

week, and some participants send incomplete information. We noticed that most researchers collect data via an online form; however, to collect our research data, we used a proper procedure. We must first download and install the app from the Google Play store. After installation, the user sees the terms and conditions dialog; some users ignore the dialog, and some agree with it. As a result, some users uninstalled the app if they disagreed with its terms and conditions. Another issue in our research study was the limited number of participants who participated in the survey. i.e., old age participants did not participate. As a result, we are unable to conclude that the result is entirely accurate. Similarly, gender-wise participants, most users are male. To determine the accuracy, we need gender equality. The other limitation is a location-based participant. Most users came from Pakistan, but we need data from all over the world to quickly determine and decide on the outcome.

C. Future Work

Users' current responses are insufficient to decide, so the app developed for the survey is still available in the Google Play store to collect vast amounts of data from participants of various ages, countries, and educational levels. We will quickly analyze the results based on the collected data. Considering such work, we will propose and develop permission models that are more user-friendly and understandable; they will be app-based at first but may later be usable as the default. Another option we will try to develop is a module for android users that shows all the information that communicates between an app with OS and OS with the network is visible to users in a simple way. To know what is going on inside your device.

REFERENCES

[1] Demetriou, Soteris & Merrill, Whitney & Yang, Wei & Zhang, Aston & Gunter, Carl, "Free for All! Assessing User Data Exposure to Advertising Libraries on Android," *in Conf. ISOC Network and Distributed System Security Symposium (NDSS 16')*, 2016.

[2] D. G. N. Benítez-Mejía, G. Sánchez-Pérez and L. K. Toscano-Medina, "Android applications and security breach," *in Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC)*, Moscow, pp. 164-169, 2016

[3] S. Karthick and S. Binu, "Android security issues and solutions," *in International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, Bangalore, pp. 686-689, 2017.

[4] J. Jung, S. Han, and D. Wetherall, "Short paper: Enhancing mobile application permissions with runtime feedback and constraints," *in Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, New York, NY, USA: ACM, pp. 45–50, 2012.

[5] M. Benisch, P.G. Kelley, N. Sadeh, and L.F. Cranor, "Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs," *Personal and Ubiquitous Computing*, vol. 15, pp. 679–694, 2011.

[6] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," *in European Data Protection*: Coming of Age, pp. 3-32, 2013.

[7] L. Barkhuus and A. Dey, "Location-based services for mobile telephony: a study of users' privacy concerns," *in 9th International Conference on Human-Computer Interaction (INCTERACT03)*, Zürich, Switzerland, pp 709-712, 2003.

[8] S. Consolvo, I.E. Smith, T.Matthews, A. LaMarca, J. Tabert, and P. Powledge, "Location disclosure to social relations: why, when, & what people want to share," *in ACM CHI Conference on Human Factors*, Portland Oregon USA, pp 81–90, 2005.

[9] P. Kelley, M. Benisch, L. Cranor, and N. Sadeh., 2011. "When are users comfortable sharing locations with advertisers," *in Proceedings of the ACM CHI Conference on Human Factors in Computing Systems*, Vancouver BC Canada.

[10] J. Lindqvist, J. Cranshaw, J. Wiese, J. Hong, and J. Zimmerman, "I'm the mayor of my house: examining why people use Foursquare - a social driven location sharing application," *in Proceedings of the ACM CHI Conference on Human Factors in Computing Systems*, NY, USA, 2011.

[11] N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao, "Understanding and capturing people's privacy policies in a mobile social networking application," *in Personal and Ubiquitous Computing*. 2009.

[12] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," *in proceedings of the Eighth Symposium on Usable Privacy and Security*, New York, NY, USA, SOUPS 12, ACM, pp. 3:13:14, 2012

[13] K. Shruthi and P. S. Chinmayi, "Android Device or a Privacy Compromise," *in International Carnahan Conference on Security Technology (ICCST)*, CHENNAI, India, pp. 1-6. 2019.

[14] P. G. KELLEY, S. CONSOLVO, L. F. CRANOR, J. JUNG, N. SADEH, AND D. WETHERALL, "A conundrum of permissions: Installing applications on an android smartphone," *in proceedings of the 16th International Conference on Financial Cryptography and Data Sec*, Berlin, Heidelberg, FC12, Springer-Verlag, pp. 6879. 2012.

[15] Al Jutail, M., Al-Akhras, M. and Albesher, A, "Associated Risks in Mobile Applications Permissions," *Journal of Information Security*, 10, 69-90, 2019.

[16] Chell, D., Erasmus, T., Colley, S. and Whitehouse, O, The Mobile Application Hacker's Handbook, John Wiley & Sons, Indianapolis, 2015.

[17] Vulnerabilities and threats in mobile applications, "The Positive Technologies," complete detail available on-line on website at https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/#id10, 2019.

[18] Rani, S. & S R, Reeja, "A Survey on Different Approaches for Malware Detection Using Machine Learning Techniques," 10.1007/978-3-030-34515-0_42, 2020.

[19] Panagiotis & Sasse, Andriotis, Angela & Stringhini, Gianluca, "Permissions Snapshots: Assessing Users' Adaptation to the Android Runtime Permission Model," *In Proc. 8th IEEE International Workshop on Information Forensics and Security (WIFS)*, 2016.