Android Application Permissions and Privacy Issues

Jithu Philip [1] *and Merin Raju* [2*]

Abstract

The use of smartphones increased worldwide during the past decade. The usage share of mobile Operating Systems shows the popularity and acceptability of mobile Operating Systems along with its application programs. Android remains the most widely used mobile operating system in the world. Here in this paper we discuss about the workflow of Android applications along with the application permissions and privacy issues related to it.

Keywords : **Android security, app permission security, data breaches, data security, user privacy**

I. INTRODUCTION

The usage share of mobile Operating Systems worldwide [1] shows it popularity and increasing acceptance by users. Android is the most widely used Operating System in the world.

The users of the system utilize the hardware which is mostly of ARM architecture with the help of the wide variety of application programs available. The increasing growth and usage share also made it the meeting place of everything. The user of a smartphone keeps all of their private personal documents, sensitive passwords for banking related stuff etc. within the device itself.

The usage of applications relies on the security factor called application permissions. Application permissions allow applications to access different sensors and hardware components of the device. The application permission is a major security factor that determines the security of the system. The user of the system needs to be knowledgeable about the fact that once an application is granted access to a specific permission, that application has the right to access the related hardware and can modify the contents of the hardware based on that permission [2]. For example, if an application is provided storage access, the application can read from and write to that storage.

This also increases risk if the security of the device is compromised in any form, the user's personal documents may be made available to the threat or utilized in some form to make profit. There exist different types of data security issues that are shared or leaked by user applications which fetch user data in its pure form or as metadata. Most of the applications gain this by achieving permissions on the user's device either at install time or at runtime. Most common users who lack the knowledge of the underlying processing behavior of the applications agree and accept the permissions requested by these applications. There also exists another category of security problem in which an attacker from outside can make use of a flaw in the device's source code and gain access to the system in the form of a malware [3]. Such a case is shown in Fig. 1.

II. WORKFLOW OF APPLICATIONS

The normal work behavior of a secure system from a user's operational workflow perspective and how all of the operational layers interconnect is shown in Fig.2. Here, if the signing and verification stages are completed, the boot loader loads the operating system. Once the user completes the authentication procedures, they can

Manuscript Received : December 12, 2022 ; Revised : December 23, 2022 ; Accepted : January 5, 2023. Date of Publication : February 5, 2023.

J. Phillip[1], *Content Writer*, Kerala. Email : jithuphiliph@gmail.com ; ORCID iD : https://orcid.org/0000-0003-4834-5772
M. Raju[2*], *Lecturer (Computer Science)*, Department of Commerce, Bishop Kurialacherry College for Women, Amalagiri, Kottayam - 686 561, Kerala. Email : merin.raju12s@gmail.com ; ORCID iD : https://orcid.org/0000-0002-8882-9651

DOI : https://doi.org/10.17010/ijcs/2023/v8/i1/172681

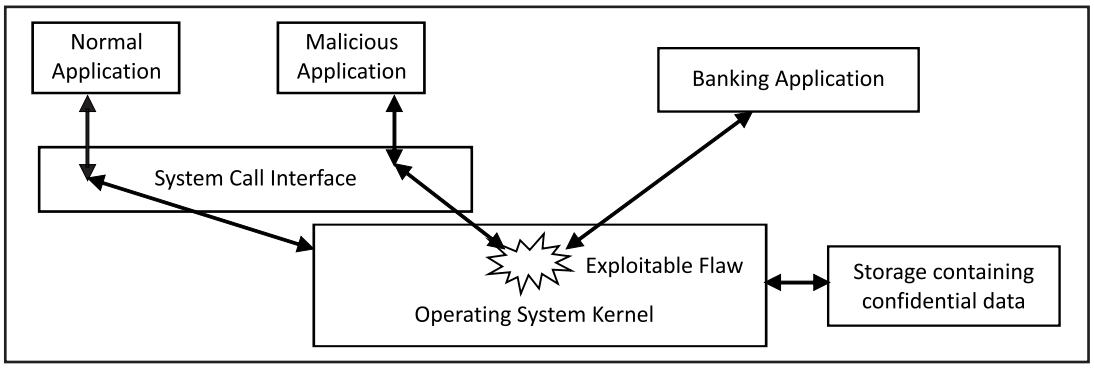

Fig. 1. Attacker taking control of the system through malicious application

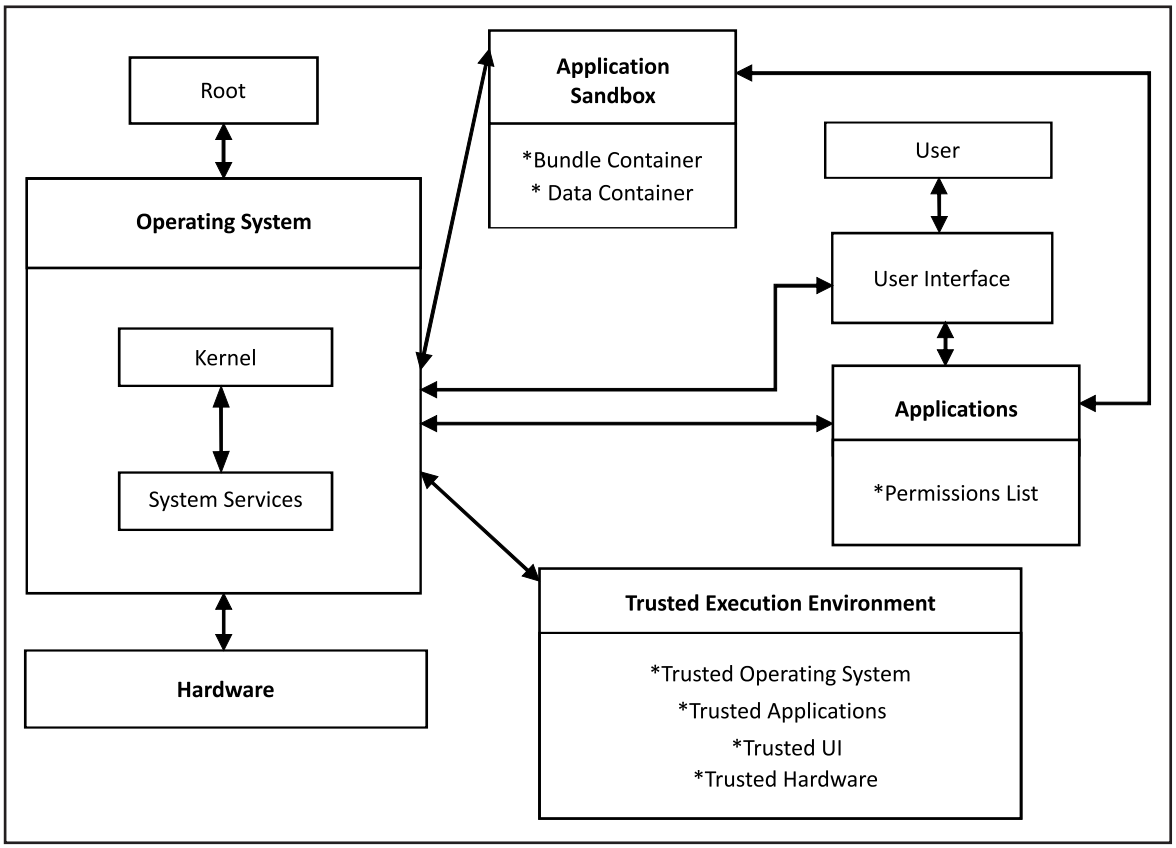

Fig. 2. How user interacts with applications and different operational layers in a system

interact with the system through different applications available. The application holds a list of permissions that it needs to get opted for its successful working. The security of the working applications is further achieved by application sandbox, whose behavior is different for different Operating Systems, for example, the Android uses a UID based sandbox and iOS uses a per-app sandbox [4]. The applications which were secured by application sandbox interact with the system hardware through system services.

There exist hardware encryption or locks which ensure the authenticity of working user through different keys [5]. The secure enclave processor chips found on iPhone and the Titan-M chips on Google Pixel devices are specially designed encrypted hardware mechanisms that were made for the purpose of securing user

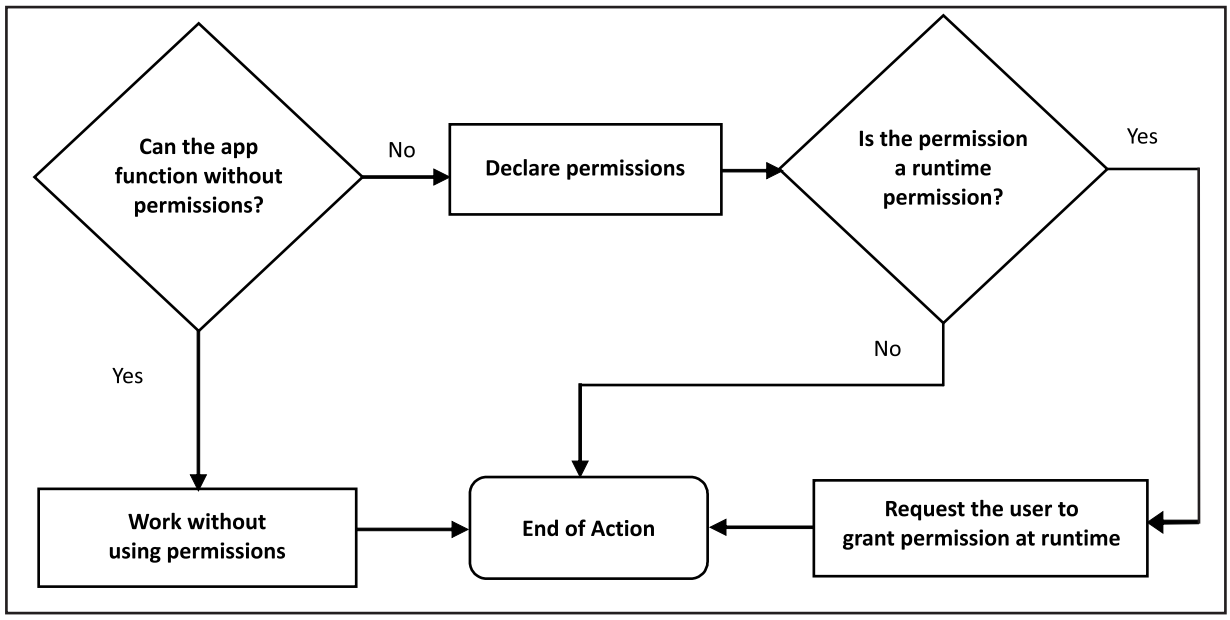

Fig. 3. Workflow of application permissions

authentication. User authentication processes like biometric authentication and the storage and matching process of confidential passwords are also done with the help of these secure hardwares. There also exists a successful approach called Trusted Execution Environment (TEE) where dedicated secure hardware is used in combination with its own Operating System software which works apart from the real execution environment for achieving an isolation from the real world processing of operations. App permissions play a major role in these environments and act as a privacy control mechanism which restrict access to restricted data and restricted actions.

III. APPLICATION PERMISSIONS

Application permissions are used as a way of controlling and regulating access to specific system and device-level functions [6]. They may include access to device hardware features like camera, microphone, and device storage. Permissions are typically declared in an applications manifest. Some permissions require the user to grant access at runtime.

Application permissions are common and work as a security feature in mobile Operating Systems like Android. App permissions help support user privacy by protecting access to:

- **Restricted data** like users contacts
- **Restricted actions** like read from or write to a storage

The general workflow of application permissions is shown in Fig.3. The workflow of apps that provide functions requiring access to restricted data and restricted actions can use different use cases. There might be cases where these functionalities can be provided without declaring any permissions. A user pausing a file's playback, taking a photo can be treated in such cases.

There is another case in which it is required to declare permissions for the app to continue its processing to access restricted data and restricted actions. In such cases, permissions need to be declared before continuing. There exists a case in which checks need to be done to verify whether the required permission is a runtime permission. In such scenarios, permission can only be granted by the user at runtime of the process.

IV. DIFFERENT TYPES OF PERMISSIONS

There exist different types of permissions in Android that can be applied to an application based on its working nature. The permission types specify the scope of restricted data the app can access and the scope of

restricted actions the app can perform when a specific permission is applied to that app.

A. Install-time Permissions

The install time permission setting employs an all-or-nothing approach in which users are required to accept a permissions list while installing an application. The install time permission dialog of an application while installing from Google Playstore is shown in Fig. 4. In scenarios like this, users are mostly unaware of all the needs related to the permissions requested by the application [7]. This also introduced a way for outside attacks on the system because of the default permission granting nature.

B. Normal Permissions

Normal permissions allow access to restricted data and restricted actions that extend beyond the application's sandbox but present very little risk to the user's privacy and to the working of other apps.

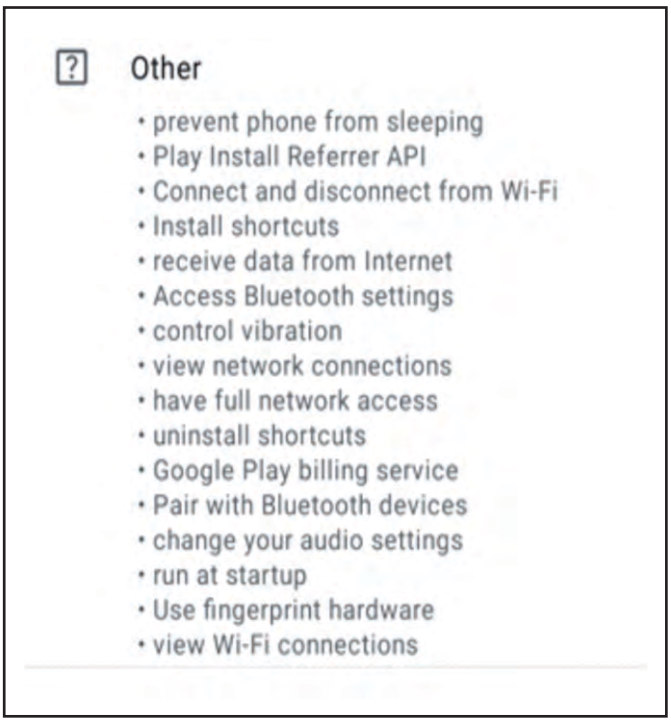

Fig. 4. The install-time permission dialog of an application while installing from Android Playstore again

C. Signature Permissions

Signature permissions are granted to an app by the system only when the app is signed by the same certificate as the app or the OS that defines the permission. Privileged services like auto fill services or VPN services can make use of this type.

D. Runtime Permissions

The all-or-nothing approach of install-time permissions has been criticized in several works [8, 9, 10]. Runtime permissions provide users with the choice of decision making, where permission-wise requests are shown each time whenever required. Runtime permissions appear to be more effective because permission requests are prompted only during the usage time of an application. This helps users to notice and identify whether the requested permission is relevant or not. The general application permission settings of the gallery application is shown in Fig. 5(a).

The runtime permission dialog of file manager application is shown in Fig. 5(b). The runtime permission dialog of file manager application with don't ask option again is shown in Fig. 5(c).

E. Special Permissions

Special permissions are defined by the platform and OEMs which correspond to particular app operations. The platform and OEMs define special permissions to protect access to powerful actions like drawing over other apps.

F. Permission Groups

Permission groups consist of a set of logically related permissions. For example, the permissions to send and receive SMS may belong to the same group.

Permission groups reduce the number of system dialogs presented to the user while requesting a permission. When a user is presented with prompt to grant permission for a particular app, permissions belonging to the same group are presented in the same interface.

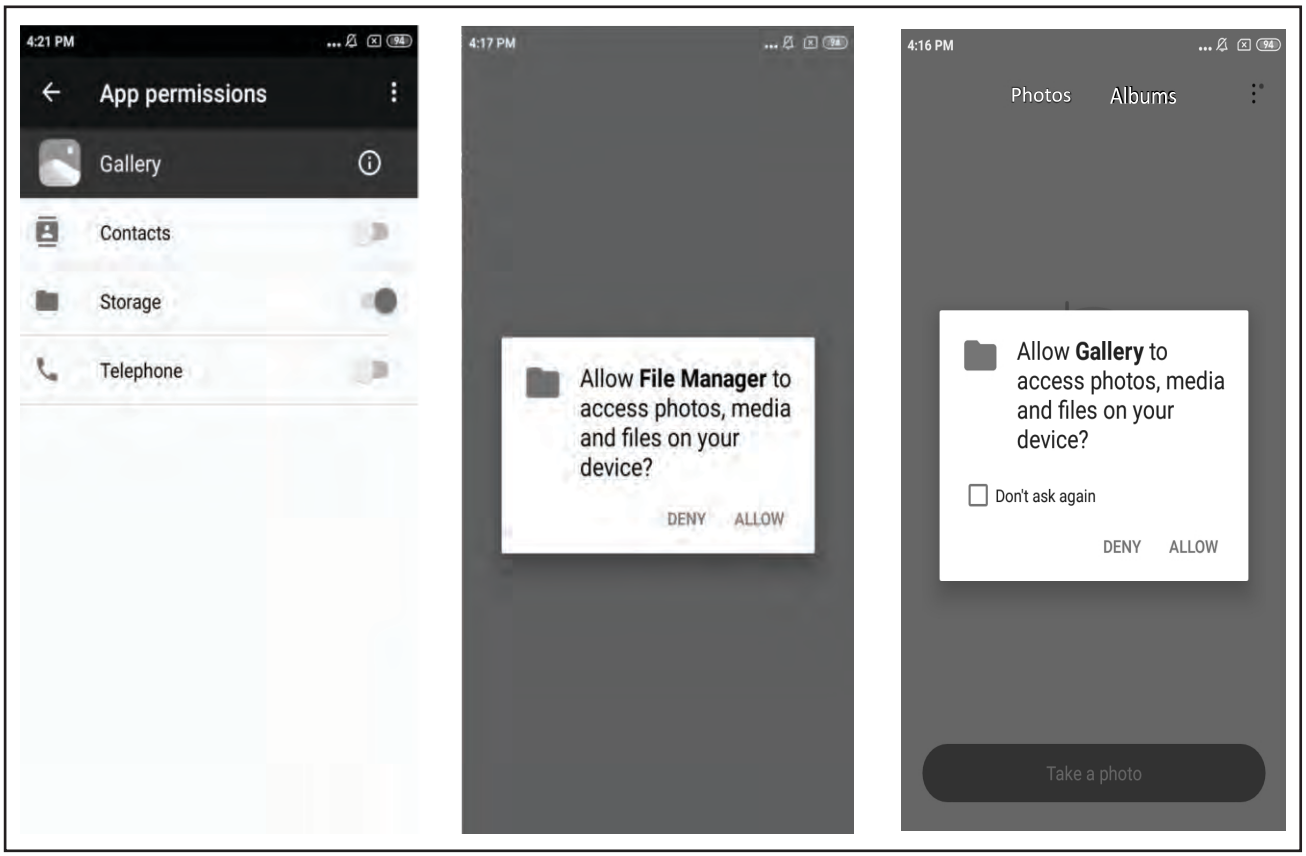

Fig. 5. (a) Fig. 5. (b) Fig. 5. (c)

Fig. 5. (a) General application permission settings (b) Runtime permission dialog of file manager application (c) Runtime permission dialog of file manager application with don't ask option again

V. APP PERMISSIONS AND USER PRACTICES

As described in the previous sections, application permissions act as a security layer that controls or regulates the access of restricted data and restricted actions. The complex nature of hardware with controlling software makes smartphones targets of many attackers. The hardware with sensors which play a major role while operating the device and through which most of the malicious operators fetch user data are described next.

A. Device Modem, IMEI, IMSI

Mobile broadband modem is the hardware which sends and receives signals for telecommunication. There exist cases where security agencies under government collect unnecessary details about telecommunication without users' consent [11]. The International Mobile Equipment Identity (IMEI) is an identifier which is unique to a device, and International Mobile Subscriber Identity (IMSI) are numbers that uniquely identifie the user of a network. Most applications request permission to access track these identifiers [12, 13].

(1) *Sensors, Camera, Microphones :* Different types of sensors are activated inside a smartphone like accelerometer, proximity sensor, gyroscope etc. that most of the applications request and gain access to. The camera and microphone that the user works with can also be used as mediums for spying.

(2) *Location Services, GPS*

Location services are used by the operating system for functions like finding the lost device location. Location tracking user applications also use these services to guide through different locations with the help of a GPS tracker.

(3) *Bluetooth, Wifi*

Bluetooth and Wifi are hardware components that are used for data sharing within short distances. These can also be compromised to attacks if the connected network or device is untrusted or malicious [14].

Despite the presence of all of the security mechanisms like application permissions, most users still lack knowledge about the internal behavior and working of the system and its applications. There is a need for huge user awareness in this area as malware attacks and data breaches [15] [16] [17] [18] [19] are growing day by day.

There exist surveys [4] that show the increasing number of malware attacks on mobile operating systems like Android and iOS. As the user base increased, attacks happening against the system also increased. If the system is not secured while exploring the details, there is a possibility that an intruder taking control of an application can make use of flaws in the source code to take advantage of it, thereby compromising the security of the entire system.

There also exists a scenario in which the user application itself collects user data directly or as metadata. Applications makes use of these information to gain profit by sharing these personal details with third parties. Third parties involved may be advertisers, e-Commerce platforms etc.

Due to all of these security issues, application permissions in Android are built focussed on the goals:

(1) *Control :* The user has control over the data they share with apps.

(2) *Transparency :* The user can understand what data an app uses and why the app uses that data.

(3) *Data Minimization :* An app uses only the data that is required by the app to do the specific task or action that the user invokes.

As the user share of Operating System like Android is huge and the applications running on it are of a wide variety, we don't know how the users of different age groups deal with this scenario. So, we conducted an experiment on real world users to study their work behaviour on different Android applications and on their permissions settings. During the analyzing stage we collected details about the permissions that the most widely used applications requests during install time and runtime. The data that these applications can access from a user's device is huge and can affect the security of the concerned devices. The experimental results and their behaviour are discussed in the next section.

VI. EXPERIMENTAL RESULTS

We conducted experiments on people of different age groups from 20–70 to study their usage behaviour patterns. During the stages of experiments different applications ranging in categories like social media apps, banking apps, and multimedia apps were installed in default settings and are used. Users were divided into 5 separate groups based on their age groups ranging from 20–30, 30–40, 40–50, 50–60, and 60–70. Experiments were conducted on a batch of 10 people who belonged to these different age groups.

The percentage of users falling into two different categories of usage were studied, i.e. the type of users who have knowingly given permission to an application with exact knowledge about the application's permission behaviour, and the type of users who have given permission to an application without exact knowledge about the application's permission behaviour. The observed results are shown in Table I, Table II, and Table III. The experimental results of users with social media apps are shown in Table I. The experimental results of users with banking apps is shown in Table II. The experimental results of users with multimedia apps is shown in Table III.

During the experimental stages a survey was conducted with the participant users who belonged to the age groups 20–70. The survey was done based on studying the usage. behavior of users interacting with different applications belonging to test categories. The

TABLE I.

EXPERIMENTAL RESULTS OF USERS WITH SOCIAL MEDIA APPS

Age Group	Users giving permissions knowingly	Users giving permissions unknowingly
20–30	8	2
30–40	7	3
40–50	5	5
50–60	3	7
60–70	1	9

TABLE II.

EXPERIMENTAL RESULTS OF USERS WITH BANKING APPS

Age Group	Users giving permissions knowingly	Users giving permissions unknowingly
20–30	10	0
30–40	8	2
40–50	7	3
50–60	5	5
60–70	4	6

TABLE III.

EXPERIMENTAL RESULTS OF USERS WITH MULTIMEDIA APPS

Age Group	Users giving permissions knowingly	Users giving permissions unknowingly
20–30	9	1
30–40	8	2
40–50	7	3
50–60	6	4
60–70	2	8

subjects were also examined with questionnaires which helped us categorize them and study their in depth knowledge about the working applications and their permissions.

Some of the test questions used for the survey are as follows:

- Do you install applications from outside of playstore?
- How long time will you use the app continuously?
- Do you know what app permissions are?
- Do you give all the permissions that an application requests?
- Do you turn on Mobile Data, Wi-Fi, and Bluetooth all the time or only turn them on when needed?
- Do you turn off application permissions that are unnecessary for an application and only turn them on when needed (Yes/No)?
- Do you give camera and microphone permission to all the requested apps or only provide these permissions when needed?
- Do you give storage access permission to all the requested apps or only provide these permissions when needed?
- Are you familiar with runtime permissions?

The permissions opting criteria test was conducted and is shown in Table I, Table II, and Table III. These include results of both install time permissions and runtime permissions. The end result shows that the category of users who give app permissions without any knowledge about the permission's behavior mostly falls in the list of aged people.

VII. CONCLUSION

During the survey we studied the usage behavior of users on different applications. A survey questionnaire result was also collected from participant users. Based on the tests we came to the conclusion that most of the users who work with application programs were unaware of the actual working of the app permissions nature. The users who fall into this category consist mostly of aged people. Even though middle aged people were having knowledge about the app permission scenario and their uses, the popularity of most applications and their public nature forced them to use the apps without any restrictions. Nowadays, more and more applications are making profit by targeting private personal information either in the form of pure data or as metadata. So, end users need to be aware of the fact that they must select app permissions and their security levels carefully to avoid potential risk of incoming threats.

AUTHORS' CONTRIBUTION

Jithu Philip and Merin Raju actively participated throughout the processing of this paper. Jithu Philip designed the workflow of the experiment. Merin Raju conducted the survey on users and finalized the results.

CONFLICT OF INTEREST

The authors certify that they have no affiliation with or involvement in any organization or entity with financial implications in the subject matter presented in the paper.

FUNDING ACKNOWLEDGEMENT

The authors have not received any funding support for conducting the work presented in the paper.

REFERENCES

[1] "Mobile Operating System market share worldwide - April 2021." gs.statcounter.com. https://gs.statcounter.com/os-market-share/mobile/worldwide

[2] J. Philip and M. Raju, "Analyzing the growing needs of users to employ hardware and software restrictions in smartphones for increased privacy and data security," *Indian J. Comput. Sci.*, vol. 6, no. 5, pp. 17–27, 2021, doi: 10.17010/ijcs/2021/v6/i5/166514.

[3] J. Philip and M. Raju, "Security impact of trusted execution environment in rich execution environment based systems," *Indian J. Comput. Sci.*, vol. 5, no. 4–5, pp. 26–37, 2020. doi: 10.17010/ijcs/2020/v5/i4-5/154785.

[4] J. Philip and M. Raju "A formal overview of application sandbox in Android and iOS with the need to secure sandbox against increasing number of malware attacks," *Indian J. Comput. Sci.*, vol. 4, no. 3, pp. 32–40, 2019. doi: 10.17010/ijcs/2019/v4/i3/146164.

[5] J. Philip and M. Raju, "An overview about the security architecture of the mobile operating system iOS," *Indian J. Comput. Sci.*, vol. 4, no. 1, pp. 13–18, 2019. doi: 10.17010/ijcs/2019/v4/i1/142412.

[6] "Permissions on Android." Developer.android.com. https://developer.android.com/guide/topics/permissions/overview

[7] A. P. Felt, E. Ha, S. Egelman, A. Haney, E Chin, and D. Wagner. "Android permissions: User attention, comprehension, and behavior," in *Proc. 8th Symp. Usable Privacy Secur*. ACM., 2012. [Online]. Available: https://cups.cs.cmu.edu/soups/2012/proceedings/a3_Felt.pdf

[8] S. Garfinkel and H. R. Lipford. "Usable security: History, themes, and challenges," in *Synthesis Lectures on Inform. Secur., Privacy, Trust*, 2014. doi: 10.1007/978-3-031-02343-9.

[9] J. Lin, B. Liu, N. Sadeh, and J. I Hong, "Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings," in *Proc. 10th Symp*. Usable Privacy Secur., 2014, pp. 199–212.

[10] P. Wijesekera, A. Baokar, A. Hosseini, S. Egelman, D. Wagner, and K. Beznosov, "Android permissions remystified: A field study on contextual integrity," in *24th USENIX Secur. Symp.*, 2015, pp. 499–514. [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-wijesekera.pdf

[11] "Edward Snowden: Leaks that exposed US spy programme." BBC.com. https://www.bbc.com/news/world-us-canada-23123964

[12] A. Alshehri, A. Hewins, M. McCulley, H. Alshahrani,. H. Fu.,and Y. Zhu., "Risks behind device information permissions in Android OS," *Commun. Netw.*, vol. 9, no. 4, pp. 219–234, 2017. doi: 10.4236/cn.2017.94016.

[13] S. Achleitner and C. Xu, "Android apps leaking sensitive data found on Google Play with 6 million U.S. downloads." Unit42. https://unit42.paloaltonetworks.com/android-apps-data-leakage/

[14] Federal Communications Commission, "Wireless connections and bluetooth security tips." FCC.Gov. https://www.fcc.gov/consumers/guides/how-protect-yourself-online

[15] R. Sobers, "89 must-know data breach statistics for 2022." Varonis.com. https://www.varonis.com/blog/data-breach-statistics/

[16] L. Constantin, "One in three organizations suffered data breaches due to mobile devices." CSOOnline.com. https://www.csoonline.com/article/3353560/one-in-three-organizations-suffered-data-breaches-due-to-mobile-devices.html

[17] "Smartphones face high hacking risk in 2020: Report." TheHindu.com. https://www.thehindu.com/sci-tech/technology/gadgets/smartphones-face-high-hacking-risk-in-2020-report/article30450912.ece

[18] "Remote working linked to data breach in 66% Indian firms: Survey." Ciso.economictimes.indiatimes.com.

https://ciso.economictimes.indiatimes.com/news/remote-working-linked-to-data-breach-in-66-indian-firms-survey/77653551

[19] "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach." The Guardian.com. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

About the Authors

Jithu Philip received M.Sc. degree in Computer Science from School of Computer Sciences, Mahatma Gandhi University, Kottayam, Kerala, India. He is currently working as Content Writer. His research interests are in the areas of Operating Systems and Computer Security.

Merin Raju received M.Sc. degree in Computer Science from School of Computer Sciences, Mahatma Gandhi University, Kottayam, Kerala, India. She is currently working as Lecturer (Computer Science), Department of Commerce, Bishop Kurialacherry College for Women, Amalagiri, Kottayam, Kerala, India. Her research interests are focused on Computer Security.