Quantitative Evaluation of Android Application Privacy Security Based on Privacy Policy and Behaviour

Alcides Bernardo Tello[1*], Sohaib Alam[2], Archana Ravindra Salve[3], B.M. Kusuma Kumari[4] and Meena Arora[5]

[1*] Professor, Universidad de Huanuco, Huanuco, Peru.
Professor, Universidad Nacional Hermilio Valdizan, Huanuco, Peru.
abernardo@udh.edu.pe, Orcid: https://orcid.org/0000-0002-0946-0236

[2] Assistant Professor, Department of English, College of Sciences and Humanities in Al-Kharj, Prince Sattam bin Abdulaziz University, Kingdom of Saudi Arabia.
s.alam@psau.edu.sa, Orcid: https://orcid.org/0000-0002-9972-9357

[3] Professor, Department of MBA, Indira College of Engineering and Management, Pune, Maharashtra, India. archanasalve13@gmail.com, Orcid: https://orcid.org/0009-0008-7859-6859

[4] Assistant Professor, Department of Studies and Research in Computer Applications, Tumkur University, Tumakuru, Karnataka, India. kusuma.kuku@gmail.com,
Orcid: https://orcid.org/0000-0003-2961-7752

[5] Associate Professor, IT Department, JSS Academy of Technical Education, Noida, India.
meenaarora@jssaten.ac.in, Orcid: https://orcid.org/0000-0001-9999-9763

Received: June 24, 2023; Accepted: August 07, 2023; Published: September 30, 2023

Abstract

The emerging landscape of Android applications in mobile phones encompasses industries involving millions and billions of app developers to improve usability and comfort for smartphone users. Popular apps are categorized into social media, entertainment, games, news, lifestyle, health and fitness. In this vein, privacy security is categorized into two major sections: distribution and development of particularities and running software on the user's mobile. According to European Union, the major issues of legal and regulations arising from the requirement from the GDPR, the Personal information protection law of China and other related regulations combined with the behaviour and privacy policy of application. In this article, Privacy security was quantitatively analyzed through data collection and analysis of scores by comparing the comprehensive use of ML, NLP and other technologies. E-privacy was regulated in the environment of mobile applications. The features were analyzed in privacy and data protection. The scope of this study is to evaluate the privacy security of the application in Android devices based on the privacy policy and behaviour.

Keywords: Android Application, Privacy Policy, Behaviour, Quantitative Analysis, Data Protection.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 14, number: 3 (September), pp. 253-266. DOI: *10.58346/JOWUA.2023.I3.019*

*Corresponding author: Professor, Universidad de Huanuco, Huanuco, Peru.
Professor, Universidad Nacional Hermilio Valdizan, Huanuco, Peru.

1 Introduction

The operating system Android is used in mobile devices that include computers, televisions, tablets and mobile phones that are open source, which work based on Linux. Headed by Google, joint handily with other businesses Open handset alliance developed Android OS. The Android platform is built on the Linux operating system in its most basic form; it resembles a multi-layered desktop operating system in terms of both appearance and functionality. As a result, the user can get a rich, highly engaging experience by integrating a variety of components into the user-interface, such as boxes, lists, windows, widgets, and more. Depending on the kind of application, Android can have as few or as many levels as the user choose. For instance, while developing a smartphone application, the user can instruct the program to utilize the device's built-in Wi-Fi, Bluetooth, NFC, and other connections. This broadens the range of interactions a user can have with the program. Users are increasingly using voice-based services, such as virtual assistants, to engage with their Android applications.

For consumers who are worried about how their "Personally Identifiable Information" (PII) is being used online, the privacy policy has been put together. Information that can be used to identify, reach out to, or find a single person, or to identify a person in context, is referred to as PII in US privacy law and information security. To fully understand how we gather, utilize, safeguard, or otherwise handle the Personally Identifiable Information in compliance with our website, please read our privacy policy carefully.

To fulfil user or corporate objectives, mobile applications regularly access sensitive personal information. Regulators are increasingly requiring developers of mobile app for providing privacy behaviours and policies which outline the data that collects the information because such information is sensitive in general. Additionally, when the privacy policies conflict with actual data for the mobile applications, regulators have penalized corporations. They have suggested the framework of semi-automated type consisting of API (application programming interface) policy terminology method which connects the phrases of policies to the API methods which producing the sensitive kind of information to assist mobile app developers in verifying the consistency of their privacy policies against the code of their apps (Slavin et al., 2016).

Users of smartphones with platforms like Android and iPhone have access to the range of capabilities through a large variety of apps (Rahmawan, S., 2023). The numerous phone sensors, including the camera, accelerometer, and GPS, can be used by app developers to offer users amusing or practical services. Due to the fact that mobile devices are frequently always in use and always on, app developers have unprecedented access to consumer data. These powers do, however, come with significant privacy and security dangers. There has been little research on the perspectives of app developers, despite the fact that studies have looked at smartphone users' perceptions and demands for privacy and security. Organizations all over the world face new challenges as a result of General Data Protection Regulation (GDPR) of the European Union, which also offers possible opportunities. The majority of businesses are still not sufficiently set up to comply with the GDPR. Organizations all over the world must alter to comply with the GDPR in order to reduce liability under it. This editorial prelude analyses the influence of GDPR on the advancement of technology worldwide, including opportunities and problems. We also talk about how the two biggest economies in the world, China and the United States, can better address GDPR's difficulties and potential (Li et al., 2019).

Every day, billions of users install Android apps, granting the access for sizable amount of personal information. Over the time fewer methodologies was created for comprehend the applications either preserve that tries to compromise the privacy of the users. However, these findings came from several

academic fields and approached privacy from various angles, creating a substantial but dispersed body of knowledge. Different stakeholders value knowing what methods and tools are available for evaluating Android app privacy. The more sophisticated methodologies can help developers and testers find and address privacy problems, enhancing the quality of the apps that are being evaluated. They can be used by auditors and data protection authorities to identify privacy-related irregularities in third-party applications. To find and develop new research avenues, researchers must be aware of the state of the art. It can be difficult to get a good overview of the contributions that are currently accessible in this area. Researchers initially tackle the issue from various angles, for as by tackling various privacy issues or adhering to various privacy paradigms. Additionally, because contributions are divided throughout numerous fields, including software engineering, cybersecurity, and computer networks, there is an expanding yet fragmented body of knowledge. Although they were completed more than five years ago, some earlier studies have shed light on the subject or considered security rather than privacy (Del Alamo et al., 1999).

Research Problem

- Required to evaluate the privacy policy and behaviour of android application running in the mobile phones
- Existing studies does not deal with the quantitative and comparative analysis of Machine Learning (ML), Natural Language Processing (NLP) and other technologies

Research Objectives

- The main objectives of the proposed study are
- Comprehensive use of ML, NLP and other technologies for privacy policy of application
- Understanding the privacy regulations, privacy policy and behaviour for the applications

Significance of Research

- Analyzing all the parameters of technologies like ML, NLP and other technology for finding the better privacy security
- Quantitative score for GDPR, Personal Information protection law of China and other regulations for the privacy security of the android application.

2 Literature Review

Lin et al., (2022) studied the privacy policy framework and protection system of websites in China. The security and privacy concerns of the personal information in the apps are crucially relevant in light of the increasing expansion of China's digital economy. China's current legal requirement for the protection of privacy information, websites must adopt the fundamental procedures for the protection of personal information that include protection policies disclosing the personal information. Even though the websites use a self-regulation approach, there is still a chance that personal information will leak. To give countermeasures to the improvement of the individual data security lawful structure in China, here initially recommend the estimation examination of notable sites in China utilizing methodology investigation and web confirmation. The exploration is achieved through the investigation of a bunch of 199,060 organization ways of behaving from 663 sites throughout the span of a half-year, the assessment of the consistency between site conduct and strategy, and the precise assessment of the security approaches posted on every site. The outcomes are fluctuated: 67.6% of notable sites in China have

made their protection approaches openly accessible, and all consistence prerequisites had met in excess of 60%; however, less than 5% of websites have made their third-party sharing and cookie retention policies explicit and strictly adhered to them (Lin et al., 2022).

Recent privacy laws like the GDPR and CCPA (California Consumer Privacy Act) have stressed the importance of clear, open privacy policies. In this literature, the study examines how technical language affects policy transparency (Tang et al., 2021). They conducted a study using Amazon Mechanical Turk to determine whether users can correctly define the technical terms, to spot common misunderstandings, and to look about the use of technical terms that affect the comfort of the users in terms of privacy policies. The technical words were identified through a previous pilot study by the researchers. The author discovered that the popular misconceptions about some technical words are pervasive. Additionally, the comfort levels with different privacy rules and their reported propensity to accept those policies are impacted by the usage of technical words. They concluded that the existing usage of technical words in privacy policies challenges the openness of the policies and user privacy, and that businesses should take action to lessen this impact.

Kununka et al. (2018) observed that the target samples' privacy rules and privacy behaviour were inconsistent after conducting a thorough investigation on a limited number of apps. However, due to the small number of analysis samples, there may be data discrimination problems. Momen et al. (2019) used a thorough examination of app permissions to examine whether the issue of app privacy had improved before and after the GDPR was implemented. According to their research, app privacy behaviour is affected by the GDPR in a normative way.

Regola and Chawla (2013) provide an outline of the issues facing researchers today as they use health care data to investigate personalised medicine and other developments in information technology. Health domain was probably the first to have privacy regulation. In 1996, the Health Insurance Portability and Accountability Act (HIPAA) required the United States Department of Health and Human Services to safeguard protected health information according to national standards. The Researcher attempts to address an appropriate network and systems architecture to support compliance with Health Insurance Portability and Accountability Act (HIPAA) regulations in the United States in a research environment. They present a prototype infrastructure in Amazon’s Virtual Private Cloud to allow researchers and practitioners to utilize the data in a HIPAA compliant environment.

Weber et al., (2020) compared the personal data protection regulations of EU and China. The quantity of personal information exchanged and submitted online has substantially expanded for the development of the platforms of e-commerce and certain other platforms. Proper usage and securing the gathered information and process of the data is the significant concern. The EU's implementation of a new data protection regulation in 2018 has proved to be crucial in the advancement of personal information protection. Coding of texts were used for comparison of protection of personal data regulatory environments currently in the place of China and EU for ascertaining distinctions between the regulations of personal data protection as well as General data Protection Regulation in the developing countries with rapid growth of E-Commerce Sector (Weber et al., 2020).

Researchers are examining how artificial intelligence (AI) can be implemented and used for ensuring that the technology progresses ethically and be advantageous for the society because it is anticipated that AI governance will have a revolutionary impact on mankind. Although several nations have started to create governance plans to control AI, there are still surprisingly few developing AI regimes that have a set framework. In the meantime, technology is developing quickly and has already harmed disadvantaged people unfairly. To reduce the problems and hazards associated with the use of AI, solid governance must be established immediately. While many suggested structures, principles and ethics

the study seeks for bridging the gaps in policies through offering straightforward and persuasive framework for the policymakers the governance of AI, principles of AI guide the standard in creating as well as assessing regulations. The recent writing time of the technologies and governing the comprehensive documents from the European Union, the United States and China are systematically studied and examined for the comparative analysis for addressing the principles of AI for the three regimes. This was done instead of coming up with new policy recommendations (Dixon, 2022).

A draft of China's Personal Information Protection Law (PRC) was made available for public discussion in October 2020. The proposed bill is meant to be China's first integrated and all-encompassing personal information protection law. If the law were to be passed in its current form, it would impose a number of requirements on businesses in both the public and private sectors as well as on individuals who handle the personal data of Chinese citizens. The draft law's scope, organization, and content both closely match and differ from the European Union and General Data Protection Regulation in a number of significant areas. Although the US not passed a comprehensive federal privacy law that is applicable nationwide, the draft Chinese bill shares some parallels with a number of US privacy regulations. Despite the differences in the regulatory structures of China, the EU, and the US, companies that operate there can use the privacy compliance programs they may have set up for the US and EU to get ready for the adoption of the proposed Chinese Personal Information Protection Law. This article presents high-level observations regarding the draft Chinese law's parallels and differences from the GDPR and significant US privacy laws, as well as a summary of its essential requirements (Determann, et al., 2021).

Machine learning (ML) has recently played a significant role for producing privacy and security in wide range of android applications. A comprehensive review is given by Sagar et al., (2020) on the application of ML to fulfil current real-world requirements in security. Significant issues that include vulnerable assessments, attack detection in real-time application and data leaking are addressed using Machine Learning. In wider areas error-free processing, cost efficiency, short times of learning cycle, large amount of data processing, decision making in real time are complemented by the Machine Leaning comprehensively for satisfying the needs of the present world. In order to solve contemporary security-related real-world concerns, they studied cutting-edge methodologies in this work that make better use of machine learning. They examine numerous security applications via the lens of ML models and assess the accuracy results from a variety of conceivable angles. The investigation of ML methods in security applications provides a blueprint for an interdisciplinary research subject. Even with the use of cutting-edge, complex technology and tactics, attackers can defeat the ML models by launching adversarial attacks. The vulnerability of the ML models to adversarial assaults must therefore be assessed at the time of development. The author also looks at the many adversarial attacks that can be launched against ML models to support this idea. To accurately depict security aspects, they have developed the threat model and defence strategies against adversarial attack methodologies. They also discussed the model point where prospective assaults might occur and presented adversarial assaults based on the assailants' model knowledge. Finally, they investigate a number of adversarial assault traits (Sagar et al., 2020).

The widespread use of Android mobile applications and the services they support allow for the worldwide collection and sharing of people's personal data. Regardless of location, data protection laws typically require all parties involved in the flow of personal data guarantee the exact level of protection of data. For example, the European General Data Protection Regulation restricts and specifies certain conditions for cross-border transfers of personal data to non-EU nations. Guaman et al., (2021) presented an approach to systematically determine if apps in android devices adhere to the standards for transfers

set forth by the European data protection regulation. One hundred Android apps were used to validate the strategy, and they discovered that 66% of cross-border transfer declarations were unclear, inconsistent, or missing (Guamán et al., 2020).

3 Methodology

Determine whether the user can obtain the information or carry out the operations without needing to declare permission for delivering the functionality of the app required to access the data restricted or actions restricted. The user doesn't need to declare any permissions in order to fulfil numerous use cases in the app, such as capturing images, halting media playback, and showing pertinent advertisements. Declaring the required permissions if the user decide that the app has to access limited data or carry out restricted actions in order to satisfy a use case. When the program is installed, certain permissions that are automatically granted are referred as install-time permissions. Some permissions, referred to as runtime permissions, demand that the program go one further step for asking permissions during the runtime. The secondary data used in the present study were the examination of existing literature and other similar sources. Sources are obtained from Google Play Store, 2014; www.pewresearch.org, 2015; and https://github.com/gauthamp10/android-permissions-dataset. The secondary data collected was analyzed using percentile analysis, one sample t-test, Chi-square statistics, regression analysis and correlation test.

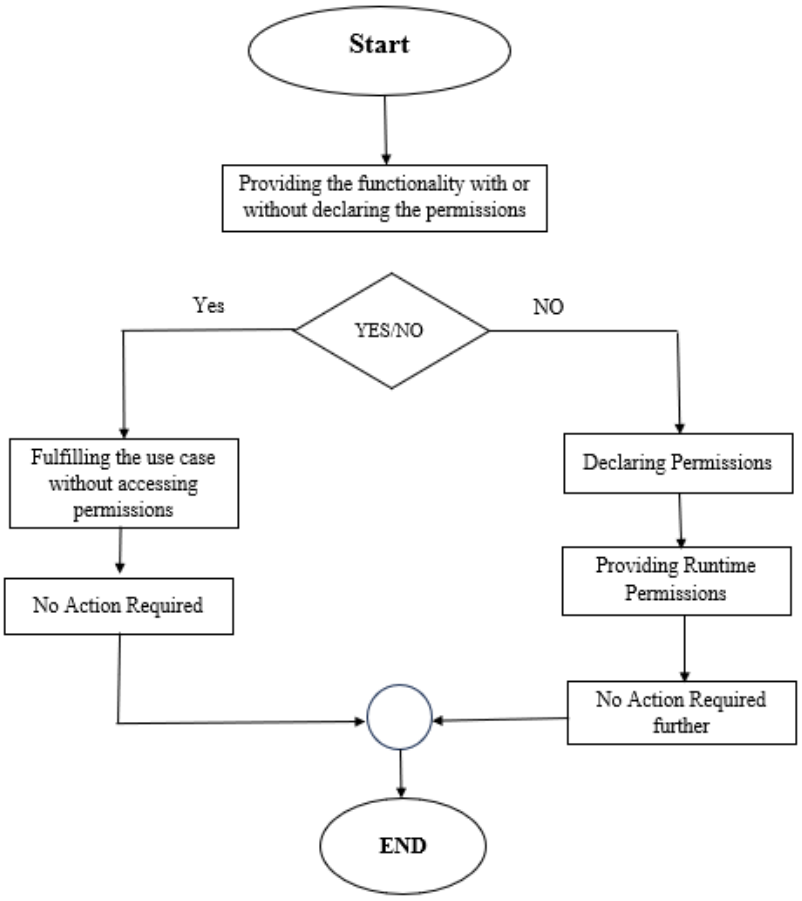

Figure 1: Workflow of Android Permissions

Experimental Scheme

Figure 1 contains the schedule for the experiment. Table 1 contains the analysis done using t-test with assumption of one sample variance. Table 2 explains about the Chi-Square test using the top app permissions in Google for evaluation of test statistics.

Table 3 gives the model summary for the regression analysis and table 4 using ANOVA test. Table 5 contains the correlation test by considering various parameters like concerns of the users about applications and personal information, free or paid apps, type of permissions, top app permission in Google play store, top app permissions for user access information.

Table 6 contains the frequency of the top app permissions for accessing the user information of parameters like cumulative percent, valid percent, percent and frequency.

Privacy Policy

The first step of taking control over the data that are used by the residents and EU citizens and that are used by the corporations and the app developers is the EU General Data Protection Regulation (GDPR). The data accessed by the business from any part of the world for managing the personal information for the citizens of EU should be sticked to follow the regulations of GDPR.

A GDPR privacy notice is a crucial tool for assisting your clients in making knowledgeable choices regarding the data you collect and use. To assist you in understanding the elements of an effective privacy notice, we have included some information from the law itself and from the EU's guidance documents. Additionally, we've provided a privacy notice template at the bottom that you may customize for your own company. The privacy notice is also known as the public statement from the outlining of the company for the management of user information as well as adhering to the laws for information protection. The specific guidelines to the GDPR for the preparation of the privacy policies and behaviours at the time of requirement for emphasizing to make them understandable and simply available that are clearly mentioned in the Article 12, 13 and 14. If the information of a person is directly used the privacy policy should be given for asking permission to access the data from the user. Note that the terms "privacy notice" and "privacy policy," which are virtually interchangeable, do not occur in the text of the GDPR. The rules outlined in this article apply to any public papers in which your business informs clients and the general public about the data processing it performs.

The GDPR mandates that businesses give customers a privacy notice that is:

- in a clear, open, understandable, and readily available manner
- written in a straightforward manner, especially for any information aimed exclusively towards children.
- Presented without charge and delivered on schedule

Type of App Permissions

Group permissions for the android applications are categorized into Normal permission, Special permission, run time permission, install time permission and signature permissions. The app permission is granted by the system for that specific permission which described with the range of data restricted for that particular app to access and the actions that are restricted for the app to be carried out.

Data Description

The secondary data used in the present study are obtained from Google Play Store, 2014; www.pewresearch.org, 2015; and https://github.com/gauthamp10/android-permissions-dataset. The secondary data collected was analyzed using percentile analysis, one sample t-test, Chi-square statistics, regression analysis and correlation test.

4 Results and Discussion

Most common application permissions are according to the EU regulations that are available in the Play store. The 60% of the android app downloaders definitely choose not for installing the app when there found to access for more information required to use the app and for same reason almost 40% of the users uninstall the applications after installation. These findings were important for the user understanding behaviours and privacy policies but the style of collecting the data can't throw more light on another side of the problems, specifically the things is going on within the app and its environment from where it is originated. The users frequently struggle to recollect what exact rights the various applications that download for their requirement and it will not completely comprehend the permissions as the first preference.

In general, consumer survey which does not provide definitive answers to critical research question that include the number of distinct forms of permissions in the mobile app that exist as the first and the prevalence for the request of apps with different types of rights from the potential users. Many researchers also investigated in the wide topic regarding the app permissions in Android environment with variety of behaviours. Using the secondary data about the users (Google Play Store, 2014; www.pewresearch.org, 2015), researchers discovered that some of the users pay more attention to the app permissions as well as few can understand the permissions for the particular android applications. Many studies discovered that the art of asking permission access for user information depends on the context and the users will not deem the suitable for sharing the data with one particular app may flinch the prospect in providing the same information with the other app. Others have investigated circumstances in which apps can go too far while requesting permissions (www.pewresearch.org, 2015).

Table 1: One-Sample t-Test

One-Sample Test						
	Test Value = 0					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Users Concerned About Apps and Personal Information	28.434	99	.000	1.40000	1.3023	1.4977
Paid vs. Free Apps	30.560	99	.000	1.18000	1.1034	1.2566
Type of Permissions	20.216	213	.000	3.44393	3.1081	3.7797
App permissions in Play Store	30.358	410	.000	4.10462	3.8388	4.3704
App permissions for user information access	20.769	202	.000	3.60099	3.2591	3.9429

Source: Google Play Store, 2014; www.pewresearch.org, 2015;

https://github.com/gauthamp10/android-permissions-dataset

The table 1 above show the One-Sample t-test for app permissions of android applications. Where the results infer that the level of concern about apps and personal information showed a two-tailed p-

value of 0.000, indicating that the level of concern about apps and personal information have a significant influence amongst the android users. Moreover, the results infer that type of apps and its permissions also showed a two-tailed p-value of 0.000, indicating that the app permissions in the Google Play Store have a significant influence over the user information amongst the android users.

Table 2: Chi-Square Test

Test Statistics					
	Users Concerned About Apps and Personal Information	Paid vs. Free Apps	Type of Permissions	Top App Permissions in the Google Play Store	Top App Permissions That Could Access User Information
Chi-Square	4.000[a]	40.960[a]	153.383[b]	110.241[c]	102.567[d]
Df	1	1	9	9	9
Asymp. Sig.	.046	.000	.000	.000	.000
a. 0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 50.0.					
b. 0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 21.4.					
c. 0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 41.1.					
d. 0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 20.3.					

Source: Google Play Store, 2014; www.pewresearch.org, 2015;

https://github.com/gauthamp10/android-permissions-dataset

The table 2 indicates the results of Chi-square for app permissions of android applications, and the results showed a p-value of 0.000. The results thus infer that there is a statistically significant association between user concerns, type of apps and permissions amongst the android users.

Table 3: Model Summary of Regression Analysis

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.892[a]	.796	.787	.22719
a. Predictors: (Constant), Top App Permissions That Could Access User Information, Top App Permissions in the Google Play Store, Type of Permissions, Paid vs. Free Apps				

Source: Google Play Store, 2014; www.pewresearch.org, 2015;

https://github.com/gauthamp10/android-permissions-dataset

The table 3 shows the r-square value of .796 which is the relevance of the model (79.6%). Hence, the results suggest that users concern about apps and personal information has a strong influence on the app permissions that could access user information.

Table 4: ANOVA Statistics of Regression Analysis

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	19.096	4	4.774	92.490	.000[b]
	Residual	4.904	95	.052		
	Total	24.000	99			
a. Dependent Variable: Users Concerned About Apps and Personal Information						
b. Predictors: (Constant), App permission for user access for information, App permission in the Play store, Type of Permissions, Paid vs. Free Apps						

Source: Google Play Store, 2014; www.pewresearch.org, 2015;

https://github.com/gauthamp10/android-permissions-dataset

The table 4 describes the ANOVA of users concern about apps and personal information, where the results showed a p-value of 0.000, users concern have a significant influence over the type of app permissions.

Table 5: Correlation Test

Correlations						
		Users Concerned About Apps and Personal Information	Paid vs. Free Apps	Type of Permissions	Top App Permissions in the Google Play Store	Top App Permissions That Could Access User Information
Users Concerned About Apps and Personal Information	Pearson Correlation	1	.574**	.802**	.554**	.844**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	100	100	100	100	100
Paid vs. Free Apps	Pearson Correlation	.574**	1	.716**	.966**	.715**
	Sig. (2-tailed)	.000		.000	.000	.000
	N	100	100	100	100	100
Type of Permissions	Pearson Correlation	.802**	.716**	1	.939**	.980**
	Sig. (2-tailed)	.000	.000		.000	.000
	N	100	100	214	214	203
Top App Permissions in the Google Play Store	Pearson Correlation	.554**	.966**	.939**	1	.919**
	Sig. (2-tailed)	.000	.000	.000		.000
	N	100	100	214	411	203
Top App Permissions That Could Access User Information	Pearson Correlation	.844**	.715**	.980**	.919**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	100	100	203	203	203
**. Correlation is significant at the 0.01 level (2-tailed).						

Source: Google Play Store, 2014; www.pewresearch.org, 2015;

https://github.com/gauthamp10/android-permissions-dataset

From the table 5 it can be inferred that there is a positive co-relationship between the variables of user concerns, type of apps and permissions amongst the android users.

Table 6: Frequency of Top App Permissions that Could Access User Information

Top App Permissions That Could Access User Information					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Modify or delete the contents of your USB storage	54	26.6	26.6	26.6
	Read phone status and identity	35	17.2	17.2	43.8
	Precise location (GPS and network based)	24	11.8	11.8	55.7
	View Wi-Fi connections	23	11.3	11.3	67.0
	Approximate location (network based)	21	10.3	10.3	77.3
	Find accounts on the device	16	7.9	7.9	85.2
	Take pictures and videos	12	5.9	5.9	91.1
	Directly call phone numbers	8	3.9	3.9	95.1
	Read your contacts	6	3.0	3.0	98.0
	Read call log	4	2.0	2.0	100.0
	Total	203	100.0	100.0	

Source: Google Play Store, 2014; www.pewresearch.org, 2015;

https://github.com/gauthamp10/android-permissions-dataset

A significant focus is on documentation of varied permission for the user access for different types of apps. This study looks at the various permission for apps available in the play store along with an emphasis on rights they allow apps for collecting or sharing personal information from users.

It is quite difficult to assess the possible harm for the smart phones by the user result from user access for information collected by phone and a piece of personal information. A permission like "View Wi-Fi connections" will surely disclose to few users' information for the specific app downloaded, as privacy policy only provides the access to app check. However, not proper understanding the way applications use the information the app gathers and difficult for determine the information of data is "sensitive," hence all information is classified as potential for purposes of the quantitative analysis. As well as judgement for highly context and the user will not regarding the malicious permissions related to the privacy.

"Modify or erase the contents of your USB storage," the prevalent permissions for app which potentially access the information of the user required by 54% of programmes (Table 6). The app permissions allow the app to information access saved in the external storage of the device for the removal and modification.

Further, the results of table 6 revealed that the app permissions "Read phone status and identity," which allowed access to user information, were accountable for the second-highest percentage (35%), followed by "Precise location (GPS and network based)" (24%), "View Wi-Fi connections" (23%), "Approximate location (network based)" (21%), "Find accounts on the device" (16%), "Take pictures and videos" (12%), "Directly call phone numbers" (8%), "Read your contacts" (6%), and "Read call log" (4%).

The app permission exemplifies for the existing permissions for continuum. The "exposure level" user may experience is determined by the type of information saved on their external storage as well as the device's configuration. Few devices save the information on the external storage, but some devices lack external storage. Finally, the app permission can grant user access for information although the possibility extremely depends on the type of user unique scenario of the device.

The current study collected data on "permissions" the Android app users which requires consent to the using conditions. It could involve basic permissions for hardware. Other permits need more specific and maybe sensitive personal information. This can be critical to an app's basic functionality at times. In some cases, the user access considered to be useful convenient for allowing the app permission to work extensively, and it is not vital for the app's basic process. These permissions have far-reaching ramifications for personal type of information from the user of android phones share with creator of app.

We creatively create frequency, time series and Boolean functions using the API information. For malware detection in terms of API sequence, API calls and API frequency are built based on three types of data sets on the privacy policy. In the end, a conformance ensemble model is built. 10010 good applications and 10683 bad apps were used in the studies. The findings demonstrate that our detection model has good accuracy and stability while achieving a detection precision of 98.98% (Ma et al., 2019).

5 Conclusion

The study offers the complete analysis of three current research topics of comprehensive use of machine learning, NLP and other technologies for privacy policy and behaviours and covers the pertinent cutting-

edge literature. The outlining each technology's key attributes before talking about its most prevalent and practical variations and different types of regulations. In order to benefit effectively, we also foresee the integration of such technology and quantitative analysis of regulatory acts of European Union. In fact, Security is taken into account by using them in groups or individually based on the requirement for stronger privacy and security. The application areas for each of these technologies separately and collectively are discussed. The study concludes by going over the unresolved problems raised by the examined research and outlining potential future possibilities for merging ML, NLP and other technologies. The outcome of the study thus identified the level of concern about apps and personal information and evidenced its significant influence amongst the android users. Therefore, the research findings reveal the major parameters for the app permissions and the quantitative analysis of the privacy policies and behaviour for the information security.

6 Acknowledgements

This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444)

Authors' Contributions

Alcides Bernardo Tello, Archana Ravindra Salve, Kusuma Kumari B M and Meena Arora contributed toward data analysis, drafting and revising the paper and agreed to be responsible for all aspects of this work. Sohaib Alam has done the formatting, and language editing and has taken care of the references.

Declaration of Conflicts of Interests

Authors declare that they have no conflict of interest.

Consent for Publication

All authors read and are aware of publishing the manuscript in the Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications Data Availability.

Statement

The database generated and /or analyzed during the current study are not publicly available due to privacy, but are available from the corresponding author on reasonable request.

Declarations

Author(s) declare that all works are original and this manuscript has not been published in any other journal.

References

[1] Del Alamo, J.M., Guaman, D., Balmori, B., & Diez, A. (2021). Privacy Assessment in Android Apps: A Systematic Mapping Study. *Electronics*, *10*(16), 1-32.
[2] Determann, L., Ruan, Z.J., Gao, T., & Tam, J. (2021). China’s draft personal information protection law. *Journal of Data Protection & Privacy*, *4*(3), 235-259.
[3] Dixon, R.B.L. (2023). A principled governance for emerging AI regimes: lessons from China, the European Union, and the United States. *AI and Ethics*, *3*(3), 793-810.

[4] Guamán, D.S., Del Alamo, J.M., & Caiza, J.C. (2021). GDPR compliance assessment for cross-border personal data transfers in android apps. *IEEE Access*, *9*, 15961-15982.
[5] Kununka, S., Mehandjiev, N., & Sampaio, P. (2018). A comparative study of Android and iOS mobile applications' data handling practices versus compliance to privacy policy. *Privacy and Identity Management. The Smart Revolution: 12th International Summer School, Ispra, Italy, Revised Selected Papers 12*, 301-313.
[6] Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, *22*(1), 1-6.
[7] Lin, X., Liu, H., Li, Z., Xiong, G., & Gou, G. (2022). Privacy protection of China's top websites: A Multi-layer privacy measurement via network behaviours and privacy policies. *Computers & Security*, *114*.
[8] Ma, Z., Ge, H., Liu, Y., Zhao, M., & Ma, J. (2019). A combination method for android malware detection based on control flow graphs and machine learning algorithms. *IEEE access*, *7*, 21235-21245.
[9] Momen, N., Hatamian, M., & Fritsch, L. (2019). Did app privacy improve after the GDPR?. *IEEE Security & Privacy*, *17*(6), 10-20.
[10] Rahmawan, S., Tandiyo, R., Sugiharto & Setyawati, H. (2023). Software Development Tools with Android Base for Skills Data Collection in Physical Education. *Journal of Internet Services and Information Security (JISIS)*, *13*(1), 22-33.
[11] Regola, N., & Chawla, N. V. (2013). Storing and using health data in a virtual private cloud. *Journal of medical Internet research*, *15*(3), 1-12.
[12] Sagar, R., Jhaveri, R., & Borrego, C. (2020). Applications in security and evasions in machine learning: a survey. *Electronics*, *9*(1), 1-42.
[13] Slavin, R., Wang, X., Hosseini, M.B., Hester, J., Krishnan, R., Bhatia, J., & Niu, J. (2016). Toward a framework for detecting privacy policy violations in android application code. *In Proceedings of the 38th International Conference on Software Engineering*, 25-36.
[14] Tang, J., Shoemaker, H., Lerner, A., & Birrell, E. (2021). Defining privacy: How users interpret technical terms in privacy policies. *Proceedings on Privacy Enhancing Technologies*, *2021*(3), 1-25.
[15] Weber, P.A., Zhang, N., & Wu, H. (2020). A comparative analysis of personal data protection regulations between the EU and China. *Electronic Commerce Research*, *20*, 565-587.

Author Biography

Alcides Bernardo Tello is currently working as a full Professor at both Universities of Huanuco-Peru: Universidad de Huanuco and Universidad Nacional Hermilio Valdizan. He has more than 20 years of experience in teaching and ten years in research. However, his early professional life started as a software engineer and computer programmer. His current research interest involves areas in Artificial intelligence, including Data Science, Natural Language processing, mobile computing, Data Analytics, the Internet of Things (IoT) and its application to aim for precision agriculture, neuroscience, healthcare and education.

Dr. Sohaib Alam is currently working as an Assistant Professor of English at the Department of English, College of Science and Humanities, Prince Sattam bin Abdulaziz University, Saudi Arabia. He holds a Ph.D. in English Language Teaching (ELT) from Aligarh Muslim University, India. His areas of interest are Applied Linguistics, Pragmatics, Teaching Methods, Blended Learning, and Pedagogic Theory. He has presented papers at both national and international conferences, published research articles and papers in various indexed journals. He has been teaching English for over 4 years.

Dr Archana Salve is working as an Professor & Head of the Department, Department of MBA, Indira College of Engineering and Management Pune. She has got more than 21 years of Teaching and industry experience. Her area of interest is Human Resource Management, Business Research Methodology, and Organization Behavior, Emotional Intelligence& Life skills. She has presented published more than 30 Research papers in the National and International Conferences in Scopus indexed, UGC care listed journals etc. She has authored 8 text and reference books for MBA.

Dr. Kusuma Kumari B.M. is working as an MCA Coordinator and Assistant Professor in the Department of Studies and Research in Computer Applications at Tumkur University. She was awarded her doctorate from Tumkur University and has 17 years of teaching experience in academics. Her most recent research interests are in digital image processing, Artificial Intelligence and software engineering. She has presented 22 papers at national and international conferences and published more than 25 research papers in reputed refereed journals.

Dr. Meena Arora received her B.E (CSE) in 1993, M.Tech (CSE) in 2007 and PhD (CSE) in 2012. She is currently working as an Associate Professor in the IT department at JSS Academy of Technical Education, Noida. She has done her PhD & Masters in Computer Science & Engineering. She has more than 25 years of experience in academics. She was awarded the best Faculty award in 2001. She has presented many papers in National & International conferences. She has also published many papers in reputed Scopus & WoS/ESCI Journals.