2024 International Conference on Communication, Control, and Intelligent Systems (CCIS) | 979-8-3315-2820-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/CCIS63231.2024.10932131

A Study of the Security and Privacy Risks in Health-Related Mobile Applications in India

Yash Dhingra
Department of Information Technology
Delhi Technological University
Delhi, India
yashdhingra_2k22phdit04@dtu.ac.in

Virender Ranga
Department of Information Technology
Delhi Technological University
Delhi, India
virenderranga@dtu.ac.in

Dinesh Kumar Vishwakarma
Department of Information Technology
Delhi Technological University
Delhi, India
dinesh@dtu.ac.in

***Abstract*—With the increased adoption of mobile devices in the current scenario, the number of applications in every category has also skyrocketed. In recent years, health-related applications have also become increasingly common. This paper aims to investigate whether the increasing prevalence of health-related applications has been accompanied by the implementation of robust cyber-security and privacy measures. In our analysis of the 21 most popular health-related Android applications available on the Google Play Store in India, it has been observed that 95% of the applications have the M8: Security Misconfiguration vulnerability of the OWASP Mobile Top 10 – 2024. It was also found that 90% of the applications have embedded trackers, which can have tremendous privacy and security implications, given the sensitive nature of health-related information. These trackers may collect sensitive user information, often without user consent and may introduce additional vulnerabilities into the application. These findings underscore the need for the adoption of security best practices in the development of health-related applications. It also shows the need for effective implementation of security and privacy regulations such as the Digital Personal Data Protection Act (India) 2023.**

***Index Terms*—health, Android, security, privacy, OWASP**

I. Introduction

Health-related applications provide users with several features, from fitness tracking to doctor consultations, booking diagnostic tests, and managing chronic diseases. Health-related data is highly personal as it contains intimate details about a user's physical and mental health. Certain health conditions may even create social stigma and discrimination. At the same time, incorrect or tampered health records may lead to inaccurate diagnoses. This is why it is absolutely critical to secure users' health-related information.

The Open Web Application Security Project's (OWASP) [1] Mobile Top 10 [2] is a widely recognised standard for mobile application security risks. The latest version of the list – OWASP Mobile Top 10 2024 – was released recently. This list defines the ten most common vulnerabilities found in applications.

For this work, the Android platform and the OWASP Mobile Top 10 (2024) have been taken as the foundation. The Android platform was selected for its openness and ease of testing.

II. Related Work

The effect of the introduction of GDPR in Europe has been studied in [3]. The authors have shown that there has been little change in the presence of third-party tracking in apps when compared to the scenario before the introduction of GDPR. In [4], it has been shown that many applications on both iOS and Android platforms potentially violate privacy laws and regulations. A novel automated method for detecting third-party tracking and advertising services inside apps has been proposed in [5]. By analysing the business relationships between these providers, the authors have shown that sharing harvested data with subsidiaries and third-party affiliates is very common. This is a worrying fact, given that a user may never be aware of the number of providers with access to their data, even without explicit consent. In [6], it has been shown that the introduction of Apple's App-Tracking Transparency policy, a mandatory opt-in system for enabling tracking, in iOS 14 has made user tracking significantly more challenging. However, it has also been pointed out that this move has prompted app developers to figure out ways to circumvent this change. Reference [7] demonstrates how commonly the OWASP Mobile Top 10 [2] can be found in applications downloaded from the Google Play Store. Through [8], the authors have identified several vulnerabilities in popular mobile commerce applications, particularly in authentication architecture and data storage. Privacy International, in [9], has found that 61% of the studied apps transfer data to Facebook as soon as the app is opened. This data is, at times, quite detailed and contains sensitive user information. It has also been shown how combining such data from 2 applications can help in the detailed profiling of users.

III. Key Concepts

A. Android Platform

Android is an open-source operating system developed by Google. It was designed for touchscreen devices. Ever since it was launched in 2008, Android has become the world's most popular mobile operating system. Currently, billions of devices run on Android.

1) Android Versions and API Levels: The first version of Android, viz. Android 1 was released in September 2008. Each Android release is associated with an API (Application Programming Interface) level. The API level (also referred to as SDK version) is a unique identifier for each version of the Android framework API. It defines the set of capabilities

TABLE I
ANDROID VERSION NAMES, API LEVELS AND STATUS OF SECURITY SUPPORT

Android Version	Release Date	API Level	Security Support
1	Sep 23, 2008	1	Ended
1.1	Feb 9, 2009	2	Ended
1.5	Apr 27, 2009	3	Ended
1.6	Sep 15, 2009	4	Ended
2.0 – 2.1	Oct 26, 2009	5 – 7	Ended
2.2 – 2.2.3	May 20, 2010	8	Ended
2.3 – 2.3.7	Dec 6, 2010	9 – 10	Ended
3.0 – 3.2.6	Feb 22, 2011	11 – 13	Ended
4.0 – 4.0.4	Oct 18, 2011	14 – 15	Ended
4.1 – 4.3.1	Jul 9, 2012	16 – 18	Ended
4.4 – 4.4.4	Oct 31, 2013	19 – 20	Ended (01 Oct 2017)
5.0 – 5.1.1	Nov 12, 2014	21 – 22	Ended (01 Mar 2018)
6.0 – 6.0.1	Oct 5, 2015	23	Ended (01 Aug 2018)
7.0 – 7.1.2	Aug 22, 2016	24 – 25	Ended (01 Oct 2019)
8.0 – 8.1	Aug 21, 2017	26 – 27	Ended (10 Jan 2021)
9	Aug 6, 2018	28	Ended (01 Jan 2022)
10	Sep 3, 2019	29	Ended (06 Mar 2023)
11	Sep 8, 2020	30	Ended (05 Feb 2024)
12	Oct 4, 2021	31 – 32	Yes
13	Aug 15, 2022	33	Yes
14	Oct 4, 2023	34	Yes

and features available in a particular version of the Android operating system.

As with all software, each Android version is maintained by the developer for a finite amount of time. Once an Android version is out of support, it stops receiving the latest updates and patches, which exposes it to known vulnerabilities that may possibly be exploited by attackers.

The list of all Android version names, API Levels and status of security support is given in Table I [10] [11].

2) About APK Files: An APK (Android Package) file is essentially a ZIP file that contains all the necessary code, resources and libraries for running an Android application on a device [12].

Since 2018, developers have the option of creating an Android App Bundle (AAB) instead of packaging everything into a single APK. The AAB contains the Base APK and several Configuration APKs [13]. The Base APK (file-name base.apk) contains the fundamental code and resources required for the app to function. Each Configuration APK contains resources for a specific device configuration (language, screen density CPU architecture, etc.

3) Minimum and Target SDK: Every Android application is designed to be compatible with a finite set of Android versions. Each application specifies its compatibility through two parameters – 'minSdkVersion' and 'targetSdkVersion' [14].

a) Target SDK Version ('targetSdkVersion'): This parameter specifies the Android version for which the application has been designed and against which it has been tested. This is usually the latest version of Android for most applications.

b) Minimum SDK Version ('minSdkVersion'): This is the oldest version of Android on which the application can run. Setting a lower minimum SDK version increases the market reach of the application since it would support a larger number of applications. However, it also adds to the complexity of the application's development and testing. Supporting older Android versions can also increase security risks since they may no longer be under support from the OEM and, hence, would not receive regular security updates.

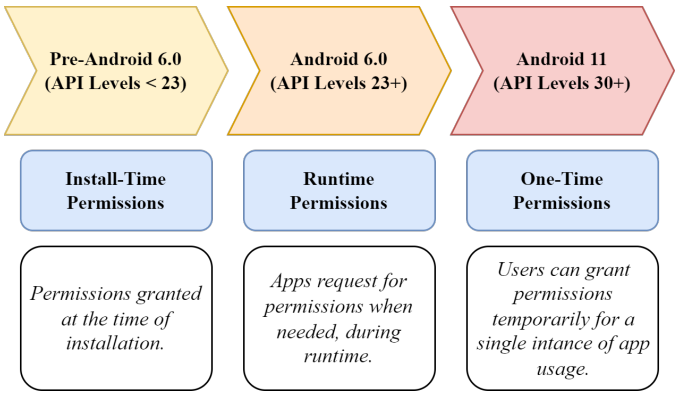

Fig. 1. Evolution of Android Permission Model

4) Permissions: Permissions are crucial mechanisms in mobile operating systems for safeguarding user privacy and security. Permissions control the interactions between apps and sensitive data or features on a mobile device [15]. This includes access to personal data (contacts, messages, photos, etc.) and system features and hardware (camera, microphone, sensors, storage, network access, etc.). By requiring explicit user consent to access these resources, permissions help mitigate risks such as data breaches, unauthorised tracking, and malware.

The permission model of Android has evolved significantly over the years. This is explained in detail in Figure 1 [16] [17].

B. Trackers

Mobile applications often include embedded trackers to collect various types of data from users. These trackers serve different purposes, ranging from improving user experience to targeted advertising. While embedded trackers in mobile applications offer valuable insights and services, they also pose significant privacy risks. Following are the different types of trackers [18].

1) Analytics Trackers: Collect data on how users interact with the app, such as screen views, button clicks, session duration, and user flow.
2) Advertising Trackers: Deliver targeted ads based on user behaviour and demographics. Trackers collect data to build user profiles and deliver personalised advertising.
3) Identification: Verify the digital identity of the user. This may be an official identity or a social media identity.
4) Crash Reporting: Monitor app performance and report crashes to developers to improve app stability and performance.

TABLE II
OWASP MOBILE TOP 10 - 2024

M1	Improper Credential Usage
M2	Inadequate Supply Chain Security
M3	Insecure Authentication/Authorization
M4	Insufficient Input/Output Validation
M5	Insecure Communication
M6	Inadequate Privacy Controls
M7	Insufficient Binary Protections
M8	Security Misconfiguration
M9	Insecure Data Storage
M10	Insufficient Cryptography

5) Profiling: Gather as much user information as possible in order to build a virtual profile. The tracker may look at various factors, including the browsing history and the list of installed applications on the device.
6) Location Trackers Provide location-based services and content, such as maps, local recommendations, or geofencing.

Impact on User Privacy

Trackers collect extensive data about users, which can be aggregated for user profiling and targeted advertising, often without user awareness or consent. Most users do not read privacy policies, although most policy documents are vague and difficult to understand, leading to a lack of awareness about the extent and nature of the data being collected by embedded trackers.

Data collected by trackers is frequently shared with third-party companies, including advertisers, analytics firms, and social media platforms, which may put the data at risk of unauthorised access.

Embedded trackers can introduce security vulnerabilities. If a tracker code is compromised, it can provide attackers with access to a large amount of user data.

C. OWASP

The Open Web Application Security Project (OWASP) [1] is a non-profit foundation that aims to improve software security. OWASP develops free and open-source tools, documentation and community resources aimed at enhancing the security of software applications and promoting the importance of secure coding practices.

1) OWASP Mobile Top 10: The OWASP Mobile Top 10 [2] is a list developed by OWASP that outlines the most critical security risks to mobile applications. By following the recommendations and best practices in this list, organisations can prioritise and mitigate these risks to improve the overall security posture of their mobile apps. OWASP updates its guidelines and lists from time to time to reflect the evolving threat landscape.

Three versions of OWASP Mobile Top 10 have been released in 2014, 2016 and 2024. The latest OWASP Mobile Top 10 (2024) risks (Table II) [19] are explained below:

- *M1. Improper Credential Usage:* Developers often mishandle sensitive data like passwords or tokens. For example, hardcoding API keys in the application code or storing credentials in plain text files can lead to unauthorised access.
- *M2. Inadequate Supply Chain Security:* This risk involves vulnerabilities in third-party components. For example, if an app relies on outdated libraries or frameworks, attackers can exploit known security flaws.
- *M3. Insecure Authentication/Authorization:* Weak authentication mechanisms allow unauthorised users to gain access. For instance, using weak passwords, not implementing multi-factor authentication, or failing to validate user roles can lead to security breaches.
- *M4. Insufficient Input/Output Validation:* Failing to validate user inputs can result in vulnerabilities such as SQL injection and cross-site scripting (XSS).
- *M5. Insecure Communication:* Transmitting sensitive data over unencrypted channels such as HTTP exposes it to interception by attackers.
- *M6. Inadequate Privacy Controls:* Mishandling user privacy can lead to legal issues and reputation damage. For example, collecting personal data without user consent or sharing it with a third party may violate privacy regulations.
- *M7. Insufficient Binary Protections:* Lack of app hardening allows attackers to reverse-engineer the app. Implementing obfuscation, anti-tampering measures, and runtime protections can mitigate this risk.
- *M8. Security Misconfiguration:* Incorrect security settings can expose sensitive data. For instance, leaving debug mode enabled in production can lead to data leaks.
- *M9. Insecure Data Storage:* Improperly storing sensitive data can result in data breaches. For example, saving unencrypted sensitive information in local databases puts the data at risk.
- *M10. Insufficient Cryptography:* Using weak encryption algorithms or misconfiguring encryption settings can compromise data confidentiality and expose user data to unauthorised access.

2) MobSF: Mobile Security Framework (MobSF) is an open-source, automated security testing framework for mobile applications [20]. It is widely used by security professionals to identify security vulnerabilities, misconfigurations and compliance issues in mobile applications. It is one of the tools recommended by OWASP's Mobile Application Security Testing Guide (MASTG) [21] for security analysis of mobile applications. MobSF is designated as MASTG-TOOL-0035 in MASTG [22].

MobSF can be used for both Static and Dynamic analysis of mobile applications and malware. It has the capability to analyse the trackers embedded in the application and the API levels supported and targeted by the application, among others.

D. Data Privacy & Regulations

1) User privacy: User privacy is a critical aspect of our digital lives. With more and more data being put up online, the need for robust privacy measures also increases. User privacy is foundational to individual freedom. It allows an individual to control who can access their personal information. Protection of sensitive information such as health-related data, personal communications and financial data from malicious actors is a key aspect of user privacy.

On each application page, Google Play Store has a specific section called *"Data Safety"*, which specifies the data collected and shared by the application. The Apple App Store has a similar section called *"App Privacy"*.

Despite its importance, user privacy faces numerous challenges, such as data breaches through cyber-attacks on organisations handling user data and monetisation of the user data for revenue by large corporations. Many businesses rely on data collection and analysis for revenue, leading to invasive tracking and profiling practices.

2) Data Privacy Regulations: Various laws and regulations have been enacted around the world with the aim of protecting user privacy. Some of these are the General Data Protection Regulation (GDPR, Europe) [23], California Consumer Privacy Act (CCPA, California, USA) [24], Health Insurance Portability and Accountability Act (HIPAA, USA) [25], Digital Personal Data Protection Act (DPDPA, India) [26] and Information Technology Act (IT Act, India) [27].

In India, the IT Act (2000) mandates that all organisations that own, control, or operate data systems must implement "reasonable security practices and procedures" to protect sensitive personal data. It criminalises unauthorised access to personal information. To put an even stronger focus on privacy, the DPDPA (2023) was enacted.

However, laws and regulations are often not enough to prevent the unconsented processing of personal data. It is very easy for developers and companies to circumvent the regulations due to various ambiguities, as shown by [3] and [4].

IV. Methodology

For the purpose of this paper, health-related applications active in India have been selected from the Google Play Store based on the criterion that the total number of installs of the application must be more than one lakh (one hundred thousand). The number of installs value displays the number of times an application has been downloaded and installed from the Google Play Store. This is the most common metric for comparing the popularity of applications.

Based on this criterion, 22 such applications were found. One of the applications was later identified as malware and removed from the Play Store. This highlights how malware can find its way onto the Google Play Store despite all the security checks by Google.

The remaining 21 applications were then installed on a test Android Device. Thereafter, the APKs of these applications were extracted from the test device using scripts. Table III lists the analysed Android applications.

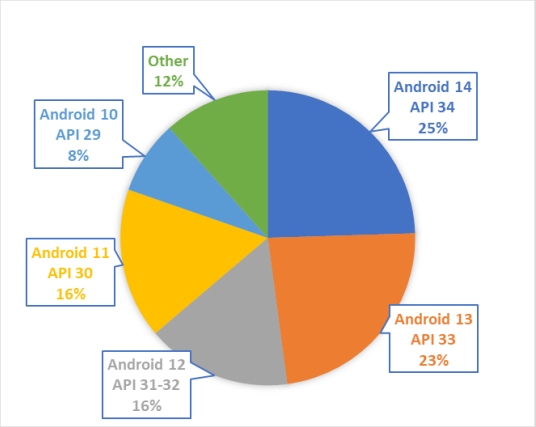

Fig. 2. Market share of different Android versions in India (June 2024)

The 'base.apk' files from the Android App Bundle (AAB) were then analysed for the Android API levels supported by the application and the trackers embedded in the application.

V. Results

A. Android Version Support

Each of the applications being considered for this study was tested for the value of the parameter 'minSdkVersion'. The values are provided in Table III. Applications have been sorted by the number of installs in descending order.

Ideally, an application should stop supporting an Android version when its security support has ended. However, this is not immediately feasible as the recent end-of-life versions might have a significant number of Android users. For instance, the two most recent end-of-life (refer Table I) API levels 29 (Android version 10) and 30 (Android version 11) together have a market share of 24% in India as of June 2024 as per [28], illustrated in Figure 2. Given this significant user base, it is understandable to continue supporting them despite them being end-of-life.

Of the 21 applications that have been studied, 20 applications (95%) have the 'minSdkVersion' less than 29 (marked in red in Table III). This means they support an Android version older than 10. Just 1 application has 'minSdkVersion' 30 (marked in green in Table III).

As of 2024, any smartphone that is running on an API level older than 29 would not have received Android security updates for over 2 years (refer Table I). The most common value of 'minSdkVersion' seen in the studied applications is 21. API Level 21 has not received security updates for over 6 years. Further, as shown in Figure 1, API Level 21 does not support Runtime Permissions. This means that the user would have to accept all permissions, including the optional ones, at the time of application installation.

Most modern smartphones use lithium-ion batteries, which typically last between 2-3 years. This may vary slightly depending on several factors like environment and usage

TABLE III
MINSDKVERSION OF HEALTH-RELATED APPLICATIONS

S. No.	Application Name	Package Name	Version	No. of Installs	*minSdkVersion*
1	HealthifyMe	com.healthifyme.basic	v23.6	37018916	21
2	PharmEasy	com.phonegap.rxpal	5.35.0	32711078	23
3	Tata 1mg	com.aranoah.healthkart.plus	17.13.1	31077435	23
4	Apollo 247	com.apollo.patientapp	7.0.3	24168279	26
5	Netmeds	com.NetmedsMarketplace.Netmeds	8.2.70	20974794	21
6	Practo	com.practo.fabric	5.96.3	12591689	26
7	Flipkart Health+	com.mhbl.sastasundar	5.1.9	12562744	22
8	Truemeds	com.intellihealth.truemeds	6.7.1	7673796	21
9	MediBuddy	in.medibuddy	3.2.72	7569750	21
10	ABHA	in.ndhm.phr	2.4.3	7057111	21
11	Healthkart	com.healthkart.healthkart	19.8.2	6612441	24
12	Airtel Merchant	com.apbl.merchant	23.6.5	5117835	21
13	Dr Lal PathLabs	pathlabs.com.pathlabs	8.14.1	5047641	24
14	DRiefcase	apps.driefcase.com	3.78	4890580	21
15	Aarogyasri	com.sritindiapvtltd.ysraarogyasri_app	1.1.5	2533011	21
16	myFortis	com.fortis.myFortis	16.0.0	2194361	22
17	Railways HMIS	com.cdac.mconsultancyrailwayhmis	4.6	995667	23
18	Max MyHealth	com.maxhealthcare	7.9.0	772564	30
19	AIIMS Gorakhpur	com.cdac.aiimsgorakhpur	4.4	425140	23
20	ECHS Beneficiaries App	com.sourceinfosys.echsbenappv2	2.7	286269	24
21	AIIMS Bhopal Swasthya	com.cdac.aiimsbhopal	2.8	230407	23

patterns. Based on this, a smartphone's maximum practical lifespan can be considered 4 years. Since Android 10 was released in September 2019 (Table I), it is likely that most smartphones that were launched with Android 10 are now approaching the end of their functional lifespan.

Even considering the market share of older Android versions, there appears to be no justifiable reason for supporting versions older than 10 since the combined market share of all these versions is just 12% (Figure 2).

Supporting older Android versions in the configuration of the application can be categorised as 'Security Misconfiguration' M8 – OWASP Mobile Top 10 2024 [29]. Of the 21 applications that are a part of this study, 20 applications are vulnerable to OWASP 2024 – M8.

Health applications store users' confidential personally identifiable information (PII). Such information can be easily misused if it is breached.

Supporting end-of-life versions of Android can have significant security and privacy ramifications. Without security updates, these versions are exposed to known vulnerabilities that can be exploited by attackers. Older versions may not support the latest encryption standards, making data transmission less secure.

B. Embedded Trackers

Each of the applications being considered for this study has been tested for the presence of embedded trackers. The number and type (functionality) of trackers embedded in the test applications are provided in Table IV. Table IV also displays the number of applications with each type of tracker. The applications are sorted in descending order based on the total number of installs. It may be noted that the same tracker may have more than one functionality.

Other than crash reporting, all other types of trackers can collect confidential information that can involve potential privacy risks. Trackers are a common feature in most applications. However, considering the criticality of data that a user stores in a health-related application, it is highly concerning that 19 of the 21 applications studied contain trackers, with the maximum number in a single application being 12. Only 2 applications do not have any trackers. Of particular concern are the 11 applications with profiling trackers and 8 applications with identification trackers.

VI. CONCLUSION AND FUTURE SCOPE

The security and privacy implications of an insecure health-related application are tremendous. It can lead to a breach of the users' confidential information, which could be misused for malicious purposes. Through this study, it has been observed that the security posture of the most downloaded health-related applications in India is abysmal. 20 of the 21 studied applications support old and end-of-life Android versions, which no longer receive security updates. These versions may not support the latest security features and algorithms, leading to enhanced risk to the users' confidential information. 19 of the 21 studied applications have embedded trackers that collect confidential user information, at times without explicit consent. These third-party trackers may also introduce additional security vulnerabilities, even unknown to the application developer. Thus, there is an urgent need on the part of the developers of health-related applications to review the security posture of their applications. There is also a need for a multi-faceted analysis of health-related applications, especially those with a large number of active users. Users must, on their part, go through the data being collected and shared by an application before downloading and using it.

TABLE IV
LIST OF EMBEDDED TRACKERS

S. No.	Application Name	Total Trackers	Analytics	Advertisement	Identification	Profiling	Location	Crash Reporting
1	HealthifyMe	10	Yes	Yes	Yes	Yes	Yes	Yes
2	PharmEasy	9	Yes	No	Yes	Yes	Yes	Yes
3	Tata 1mg	9	Yes	Yes	No	Yes	Yes	Yes
4	Apollo 247	9	Yes	No	Yes	Yes	Yes	Yes
5	Netmeds	7	Yes	No	Yes	No	No	Yes
6	Practo	10	Yes	No	Yes	Yes	Yes	Yes
7	Flipkart Health+	5	Yes	No	No	No	No	Yes
8	Truemeds	12	Yes	Yes	Yes	Yes	Yes	Yes
9	MediBuddy	11	Yes	Yes	No	Yes	Yes	Yes
10	ABHA	2	Yes	No	No	No	No	Yes
11	Healthkart	8	Yes	Yes	No	No	Yes	Yes
12	Airtel Merchant	2	Yes	No	No	No	No	Yes
13	Dr Lal PathLabs	2	Yes	No	No	No	No	Yes
14	DRiefcase	6	Yes	No	Yes	Yes	Yes	Yes
15	Aarogyasri	0	No	No	No	No	No	No
16	myFortis	5	Yes	No	Yes	No	No	No
17	Railways HMIS	1	Yes	No	No	Yes	No	No
18	Max MyHealth	4	Yes	No	No	No	No	Yes
19	AIIMS Gorakhpur	2	Yes	No	No	Yes	No	No
20	ECHS Beneficiaries App	0	No	No	No	No	No	No
21	AIIMS Bhopal Swasthya	2	Yes	No	No	Yes	No	No
			19	5	8	11	9	15

REFERENCES

[1] "Open Web Application Security Project." https://owasp.org/. Accessed: 2024-08-02.

[2] "OWASP Mobile Top 10." https://owasp.org/www-project-mobile-top-10/. Accessed: 2024-08-02.

[3] K. Kollnig, R. Binns, M. Van Kleek, U. Lyngs, J. Zhao, C. Tinsman, and N. Shadbolt, "Before and after GDPR: tracking in mobile apps," *arXiv preprint arXiv:2112.11117*, 2021.

[4] K. Kollnig, A. Shuba, R. Binns, M. Van Kleek, and N. Shadbolt, "Are iphones really better for privacy? comparative study of ios and android apps," *arXiv preprint arXiv:2109.13722*, 2021.

[5] A. Razaghpanah, R. Nithyanand, N. Vallina-Rodriguez, S. Sundaresan, M. Allman, C. Kreibich, P. Gill, *et al.*, "Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem," in *The 25th annual network and distributed system security symposium (NDSS 2018)*, 2018.

[6] K. Kollnig, A. Shuba, M. Van Kleek, R. Binns, and N. Shadbolt, "Goodbye tracking? Impact of iOS app tracking transparency and privacy labels," in *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, pp. 508–520, 2022.

[7] A. Alanda, D. Satria, H. Mooduto, and B. Kurniawan, "Mobile application security penetration testing based on OWASP," in *IOP Conference Series: Materials Science and Engineering*, vol. 846, p. 012036, IOP Publishing, 2020.

[8] C. Anwar, S. Hady, N. Rahayu, K. Kraugusteeliana, *et al.*, "The Application of Mobile Security Framework (MOBSF) and Mobile Application Security Testing Guide to Ensure the Security in Mobile Commerce Applications," *Jurnal Sistim Informasi dan Teknologi*, pp. 97–102, 2023.

[9] P. Frederike, "How Apps on Android Share Data with Facebook," *Privacy International*, 2018.

[10] "Android Versions." https://developer.android.com/about/versions. Accessed: 2024-08-02.

[11] End Of Life (EOL), "Android Versions end-of-life dates." https://endoflife.date/android. Accessed: 2024-08-02.

[12] "APK Architecture." https://developer.android.com/topic/performance/reduce-apk-size#apk-structure. Accessed: 2024-08-02.

[13] "Android App Bundle (AAB)." https://developer.android.com/guide/app-bundle/app-bundle-format. Accessed: 2024-08-02.

[14] "Android Minimum, Target and Maximum SDK versions." https://developer.android.com/guide/topics/manifest/uses-sdk-element. Accessed: 2024-08-02.

[15] "Android Permissions Overview." https://developer.android.com/guide/topics/permissions/overview. Accessed: 2024-08-02.

[16] "Android 6.0 Permissions." https://developer.android.com/about/versions/marshmallow/android-6.0-changes. Accessed: 2024-08-02.

[17] "Android 11 Permissions." https://developer.android.com/about/versions/11/privacy/permissions. Accessed: 2024-08-02.

[18] Exodus Privacy, "Types of Trackers." https://reports.exodus-privacy.eu.org/en/info/trackers/. Accessed: 2024-08-02.

[19] "OWASP Mobile Top 10 - 2024." https://owasp.org/www-project-mobile-top-10/2023-risks. Accessed: 2024-08-02.

[20] Mobile Security Framework (MobSF), "MobSF." https://mobsf.github.io/docs/, 2024. Accessed: 2024-08-02.

[21] "OWASP Mobile Application Security Testing Guide (MASTG)." https://mas.owasp.org/MASTG/, 2024. Accessed: 2024-08-02.

[22] "OWASP MASTG Tool: MobSF." https://mas.owasp.org/MASTG/tools/generic/MASTG-TOOL-0035/, 2024. Accessed: 2024-08-02.

[23] GDPR, "General Data Protection Regulation." https://gdpr-info.eu/, 2024. Accessed: 2024-08-02.

[24] CCPA, "California Consumer Privacy Act (CCPA)." https://oag.ca.gov/privacy/ccpa, 2024. Accessed: 2024-08-02.

[25] HIPAA, "Health Insurance Portability and Accountability Act (HIPAA)." https://www.hhs.gov/hipaa/index.html, 2024. Accessed: 2024-08-02.

[26] Ministry of Electronics & Information Technology, Government of India, "Digital Personal Data Protection Act (DPDPA)." https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf, 2024. Accessed: 2024-08-02.

[27] Ministry of Electronics & Information Technology, Government of India, "Information Technology Act." https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf, 2000. Accessed: 2024-08-02.

[28] "Market share of different Android versions in India, June 2024." https://gs.statcounter.com/android-version-market-share/mobile/india/, 2024. Accessed: 2024-08-02.

[29] "OWASP Mobile Top 10 (2024) - M8: Security Misconfiguration." https://owasp.org/www-project-mobile-top-10/2023-risks/m8-security-misconfiguration.html. Accessed: 2024-08-02.