Data Privacy and Security Challenges in Mobile Application Analytics Frameworks*

Taras Fedynyshyn[1,*,†] and Olha Partyka[1,†]

[1] Lviv Polytechnic National University, 12 Stepan Bandera str., 79000 Lviv, Ukraine
[2] Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine

Abstract

The widespread adoption of mobile applications has been accompanied by an increasing reliance on third-party analytics frameworks for tracking user behavior, monitoring application performance, and enabling monetization. While these frameworks provide essential functionality, they also introduce significant privacy and security risks, particularly when vulnerabilities are present in their implementations. This study analyzes 6,165 APK files using the Mobile Security Framework (MobSF) to identify the top 25 most integrated analytics frameworks, including Google Firebase Analytics, Facebook Login, and Sentry. Leveraging publicly reported Common Vulnerabilities and Exposures (CVEs), this research highlights the security implications associated with these frameworks, focusing on risks such as unauthorized data access, insecure data transmission, and privilege escalation. The analysis reveals systemic vulnerabilities introduced by outdated or improperly implemented frameworks, underscoring the critical need for secure integration practices and timely updates. Furthermore, the findings emphasize the importance of proactive security measures and compliance with privacy regulations to mitigate risks. This study contributes to the understanding of the security landscape in mobile applications, offering insights and recommendations to developers, researchers, and policymakers for enhancing the security and privacy of analytics frameworks.

Keywords

Android security, mobile security, data privacy, static analysis, MobSF, analytics frameworks, location data harvesting, cloud-based analytics, healthcare data security, mobile commerce security

1. Introduction

The rapid proliferation of mobile applications has transformed the way individuals interact with technology, making apps an integral part of daily life. From social networking and entertainment to e-commerce and productivity, mobile apps provide a wide array of functionalities. However, underpinning these user-centric features is a vast ecosystem of third-party analytics frameworks that collect, analyze, and process user data. These frameworks play a critical role in monitoring application performance, enhancing user experiences, and enabling monetization through targeted advertising and personalized content delivery. While analytics frameworks offer substantial benefits to developers and organizations, they also pose significant privacy and security challenges. The integration of these third-party frameworks often introduces vulnerabilities into mobile applications, creating opportunities for unauthorized access to sensitive data, exploitation through malicious actors, and non-compliance with stringent data protection regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) [1]. Furthermore, improper implementation or reliance on outdated versions of these frameworks can exacerbate security risks, compromising both users and application ecosystems. This study seeks to investigate the extent and impact of third-party analytics frameworks integrated into mobile applications. By performing static analysis on 6,165 APK files using the Mobile Security Framework (MobSF), this research identifies the top 25 most integrated frameworks, including Google Firebase Analytics, Facebook Login, Sentry, and AppLovin. These frameworks are evaluated in terms of

*CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
fedynyshyn.taras@gmail.com (T. Fedynyshyn); olha.o.mykhailova@lpnu.ua (O. Partyka)
0009-0006-8233-8057 (T. Fedynyshyn); 0000-0002-3086-3160 (O. Partyka)

their prevalence and potential vulnerabilities, leveraging publicly reported Common Vulnerabilities and Exposures (CVEs) to highlight specific security risks [2–4]. The findings of this research provide critical insights into the implications of widespread analytics framework adoption, emphasizing the need for secure development practices and proactive vulnerability management. By bridging the gap between functionality and security, this study aims to contribute to the growing body of knowledge on mobile application security and data privacy, offering actionable recommendations for developers, researchers, and policymakers.

2. Related work

The integration of analytics frameworks within mobile applications has become increasingly widespread, providing developers with valuable insights into user behavior, application performance, and overall market trends. These frameworks serve as critical tools for optimizing user experience and driving business decisions. However, they also introduce complex and significant concerns regarding data privacy and security. This literature review explores these issues by synthesizing findings from both academic research and real-world cases, highlighting the challenges and vulnerabilities posed by data practices within mobile application analytics. Kollnig et al. (2022) conducted an in-depth examination of Apple's App Tracking Transparency (ATT) and privacy labels, mechanisms intended to empower users with greater control over their data. Their study revealed that while these features have introduced improvements in transparency, many applications continue to covertly track users, bypassing ATT restrictions through obfuscated techniques. This finding underscores a critical limitation of platform-level privacy controls, demonstrating that even robust regulatory interventions can fall short of preventing privacy violations [5]. Liu et al. (2020) provided further insights into privacy concerns by analyzing third-party analytics libraries within the Android ecosystem. Their research identified a pervasive issue: these libraries often request and gain access to user data beyond what is necessary for their stated functionalities. Such access not only raises concerns about user consent and data minimization principles but also expands the attack surface for malicious actors. This study emphasized the urgent need for more stringent oversight of analytics libraries to ensure they adhere to privacy-by-design principles [6]. Recent studies on related cybersecurity challenges provide additional context for understanding privacy vulnerabilities. Nyzhnyk et al. (2024) examined methods to enhance the cybersecurity of SCADA and Industrial Internet of Things (IIoT) devices through secure memory management. While their focus was on critical infrastructure, their findings underscore the broader relevance of secure software design and data management principles in mitigating vulnerabilities across digital ecosystems, including mobile app analytics frameworks [7]. Martseniuk et al. (2024) investigated Shadow IT risks in public cloud infrastructures, revealing significant security and compliance challenges associated with the unauthorized use of cloud-based services. The parallels to mobile app analytics are evident, particularly in the unauthorized data flows and the lack of governance over third-party services, which exacerbate privacy risks in mobile ecosystems. Their research highlights the importance of stringent access controls, robust governance policies, and continuous monitoring to mitigate such risks [8]. High-profile real-world incidents have further exposed the vulnerabilities associated with mobile app analytics and data practices. The Facebook-Cambridge Analytica scandal serves as a poignant example. This case revealed that third-party actors could exploit app-collected user data for unauthorized purposes, including political profiling and manipulation. The scandal resulted in a $725 million settlement, drawing attention to the inadequacies of existing frameworks for governing the use of user data. It underscored the need for robust transparency mechanisms, as well as comprehensive user consent practices [9]. Further compounding these challenges, another incident involving Facebook highlighted risks stemming from the improper storage of user data. In 2019, over 540 million user records were discovered on unsecured Amazon servers, leaving sensitive data such as user IDs and account details vulnerable to unauthorized access. This breach exemplified a widespread issue within the industry: the reliance on third-party storage solutions without proper security configurations. Such incidents

stress the importance of implementing stringent access controls and encryption standards for data handled by mobile app analytics [10]. The iOS ecosystem has also faced its share of privacy and security challenges. A 2015 report uncovered that more than 250 iOS apps were using private APIs to collect sensitive user data without consent. These apps bypassed Apple's security policies, resulting in unauthorized access to information such as user location, email addresses, and device identifiers. The incident highlighted the limitations of app marketplace oversight, demonstrating that even platforms with rigorous app review processes are susceptible to breaches [11]. Another prominent case involved malware-infected apps in the Apple App Store. Popular apps were found to be compromised with data-theft malware, capable of stealing user credentials and transmitting them to malicious servers. This incident illustrated the risks of malware propagation through seemingly legitimate apps, highlighting the necessity of advanced malware detection mechanisms and continuous monitoring of app store ecosystems. The lack of adequate safeguards against such breaches underscores the critical need for improved security protocols in-app distribution platforms [12]. Collectively, these studies and incidents paint a stark picture of the current state of data privacy and security in mobile application analytics. They highlight systemic vulnerabilities in data collection, storage, and sharing practices, exacerbated by insufficient regulatory frameworks and technological safeguards. Addressing these challenges will require a multi-pronged approach that includes enhanced transparency mechanisms, stricter compliance with privacy regulations, and the development of privacy-preserving technologies. As the reliance on analytics frameworks continues to grow, ensuring that user privacy and security are not compromised must remain a top priority for developers, regulators, and the broader industry.

Du et al. (2022) introduced Vizard, an innovative analytics system designed to preserve user privacy by hiding metadata during data analysis. The system enforces fine-grained access control for data owners, addressing the challenge of unauthorized metadata leakage while ensuring efficient analytics [13]. This research underscores the critical need for privacy-by-design solutions in analytics frameworks.

Liu et al. (2023) developed LocationScope, a system for detecting and measuring excessive location data harvesting by mobile apps. Their study revealed how applications often share detailed location data with third-party frameworks, frequently without adequate disclosure or user consent [14]. This work highlights the importance of transparency and accountability in location-based analytics.

Gao et al. (2023) presented ANDetect, a framework for identifying third-party ad networks integrated into Android applications. By analyzing code and network behavior, the framework exposes how ad libraries interact with user data, raising concerns about aggressive data collection practices and the lack of oversight in ad network integration [15].

Another study by Liu et al. (2022) investigated the security risks associated with behavioral data collection by analytics frameworks. Their research identified vulnerabilities in the storage and transmission of user activity data, often exposing sensitive information to exploitation. The authors emphasized the importance of encryption, data minimization, and compliance with privacy regulations [16].

Kumar et al. (2020) explored the vulnerabilities in cloud-based analytics frameworks, which rely on complex interactions between mobile apps and cloud services. They identified insecure APIs, misconfigured permissions, and insufficient access controls as common attack vectors. The study underscores the need for securing both client-side and server-side components of analytics frameworks [17].

Al-Suqri et al. (2017) examined the role of analytics frameworks in mobile commerce applications and their associated security risks. They discussed how improper handling of transaction data by third-party frameworks could result in fraud, data breaches, and privacy violations. The authors proposed practical guidelines for securing analytics frameworks in mobile commerce environments [18].

Taylor et al. (2021) addressed the unique challenges of integrating analytics frameworks into mobile healthcare applications. Their work highlighted vulnerabilities in the handling of sensitive

health data, including issues in data transmission, storage, and sharing. They recommended adopting encryption, access controls, and compliance with healthcare-specific regulations such as HIPAA [19].

Dudykevych et al. (2019) conducted a multicriterial analysis to evaluate the efficiency of conservative information security systems, focusing on balancing multiple criteria such as performance, reliability, and resource optimization. Their findings underscore the importance of adopting holistic evaluation frameworks to enhance system security. This approach aligns with the need to assess third-party analytics frameworks comprehensively, considering factors like data privacy, implementation risks, and system integration efficiency [20].

Petrivskyi et al. (2022) introduced a modified methodology for constructing energy-efficient sensor networks by integrating static and dynamic sensors. The optimization of sensor deployment and movement trajectories not only reduced energy consumption but also maintained system effectiveness. These principles can be extended to mobile application ecosystems, where efficient integration and management of analytics frameworks could minimize resource utilization and improve overall performance [21].

Susukailo, Opirsky, and Yaremko (2021) proposed a systematic methodology for establishing Information Security Management Systems (ISMS) to counter modern cybersecurity threats. Their work emphasizes the importance of identifying vulnerabilities, assessing risks, and implementing tailored security controls. These principles are directly applicable to the integration of third-party analytics frameworks, where risk assessment and proactive mitigation strategies are crucial to safeguarding user data [22].

Banakh et al. (2018) explored the detection of MAC spoofing attacks in IEEE 802.11 networks through signal strength analysis. Their methodology demonstrated how inconsistencies in device signal strength could reveal unauthorized activities. Similarly, in mobile application security, anomaly detection techniques could be adapted to identify unusual data flows or unauthorized access attempts within analytics frameworks [23].

Mykhaylova et al. (2023) proposed a method to identify suspicious individuals by analyzing data from mobile devices. Their approach leverages patterns in mobile device usage to detect anomalies that may indicate suspicious behavior. This method underscores the potential of mobile data analytics in enhancing security measures and monitoring individual activities [24].

In a subsequent study, Fedynyshyn, Mykhaylova, and Opirskyy (2024) conducted a static analysis of Android applications to assess the security implications associated with various mobile development frameworks. Their findings revealed that certain frameworks might introduce vulnerabilities, emphasizing the need for developers to carefully consider security aspects when selecting and implementing these frameworks. The study highlights the importance of thorough security evaluations in the development process to mitigate potential risks [25].

These studies collectively highlight the multifaceted privacy and security challenges associated with mobile analytics frameworks. From detecting aggressive data harvesting to addressing vulnerabilities in cloud-based services, the literature emphasizes the importance of secure design, robust regulatory compliance, and innovative privacy-preserving technologies. These findings provide a critical foundation for evaluating the vulnerabilities and risks identified in this study.

3. Methodology

This section outlines the methodological framework used to analyze the privacy and security aspects of analytics packages embedded in mobile applications. The study leverages a dataset of 6,165 APK files subjected to static analysis using MobSF [26] (Mobile Security Framework). MobSF's ability to detect third-party libraries, permissions, and potential vulnerabilities provides the foundation for identifying and categorizing analytics packages. The methodology comprises three key steps: data collection, analysis of analytics packages, and categorization based on functionality and data practices. This structured approach allows for an in-depth exploration of privacy risks and security vulnerabilities associated with these frameworks.

3.1. Data collection and tools

This study builds on our previous analysis [27] of APK files collected from the Google Play store, expanding the focus to include privacy and security challenges in mobile analytics frameworks. While the data collection and analysis methods remain consistent, this paper highlights specific aspects related to analytical package vulnerabilities and their privacy implications.

3.2. Categorization of analytical packages in MobSF

MobSF is a widely used tool for static and dynamic analysis of mobile applications. One of its features is the ability to identify embedded analytical packages within APK files and categorize them based on their functionality and data practices. These categories help classify the different roles of analytics frameworks in mobile applications and their implications for privacy and security. Below, we detail the key categories, their descriptions, and examples.

Crash reporting—as analyzed in the MobSF, crash reporting trackers are components built into mobile applications to collect and transmit diagnostic data after an application crash. These trackers are designed to capture critical run-time information, including stack traces, error logs, device metadata, and user interactions before failure. While such functionality is essential for developers seeking to increase application stability and optimize performance, it also raises potential security and privacy concerns. From a cybersecurity perspective, MobSF recognizes that crash report trackers are a potential data leak point, especially if they collect and transmit sensitive user information. If improperly configured or inadequately secured, these trackers could expose personally identifiable information (PII), session details, or other sensitive data to third-party analytics services. This raises concerns regarding data governance, compliance with privacy regulations such as GDPR and CCPA, and the risk of unauthorized access by malicious actors. In addition, integrating third-party crash reporting services such as Firebase Crashlytics [28] and Bugsnag [29] creates a dependency on external platforms that do not necessarily adhere to strict security standards. In addition, transmitting crash reports over insecure channels increases the risk of interception and potential data leakage. MobSF's mobile application analysis scrutinizes the permissions and network endpoints associated with these trackers to assess whether they pose a security risk by exposing sensitive data beyond the intended scope.

Profiling—MobSF analysis shows that Profiling trackers exist within mobile applications to gather and assess user behavior data along with device system parameters and application operational metrics. The tools serve developers and marketing analysts to investigate application user habits and detect performance problems while enhancing user interactions. The deployment of these systems creates potential threats to both data security and user privacy. The MobSF research profiling trackers a security risk because they gather sensitive data without seeking clear user authorization. These tracking systems gather information about device location and device specifications together with processor details and battery status and RAM consumption along with exclusive device identification numbers. The collection of data without explicit user consent can result in legal violations of GDPR and CCPA when companies share the information with third parties for analysis or commercial purposes. When developers integrate third-party profiling services including Google Analytics [30] or AppMetrica [31] into their applications they expose their users to the risk of uncontrolled data distribution. The sharing of gathered data through third-party network channels poses protection risks because these channels do not consistently provide sufficient data security. The mobile application security team at MobSF evaluates tracking systems through their examination of network requests and permission usage to determine data breach risks.

Advertisement—MobSF examines advertisement trackers which function as components inside mobile applications to track user behavior and gather device information for delivering targeted advertisements. The tracking system collects device identifiers alongside browsing habits and location data and interaction patterns from users before sending this information to advertising networks for relevant ad placement optimization. The essential role advertisement tracking serves

for mobile application revenue generation creates major security and privacy risks. Advertisement trackers serve as security risks because they enable unauthorized parties to access and steal user information. Third-party ad networks link up with numerous applications to collect user data for building comprehensive user profiles through their tracking platforms. The absence of proper regulation allows extensive data mining to occur which creates concerns regarding user consent compliance with GDPR and CCPA privacy laws. Some ad trackers obtain persistent device identifiers including IMEI or MAC addresses that enable them to track users across applications even when users adjust their ad personalization controls. Security issues stem from the communication methods that advertisement trackers employ. Due to insecure or unencrypted data transfer methods many of these trackers become vulnerable to interception by attackers. Mobile applications become more vulnerable because of the external advertisement SDKs integrated into their systems. The inclusion of SDKs within applications creates security risks because outdated or insecure code within them exposes the application to threats that include data theft and unauthorized API access and malicious ad network exploitation. MobSF examines network requests and API calls and embedded SDKs to detect advertisement trackers that might endanger user privacy and data security.

Analytics—according to MobSF analytics represents the incorporation of tracking elements into mobile applications which gather user data throughout interactions to monitor system performance and analyze user behavior and generate business intelligence. Analytics mechanisms help developers and organizations understand application usage patterns and discover trends which allows them to optimize functionality while improving user interaction. From a cybersecurity standpoint, the extensive data collection performed by analytics services creates substantial privacy issues, compliance challenges, and security threats. MobSF evaluates analytics trackers because they function as key channels to collect unauthorized data from users who provide their sensitive information including location data device identifiers session durations and in-app interactions. Mobile applications frequently incorporate third-party analytics services including Google Analytics, Firebase [32] and Mixpanel [33] to process their data outside of the application. Applications that depend on external platforms face higher data exposure risks when these services use weak security controls or when data is transmitted through unsecured channels. Some analytics trackers maintain persistent background operations to gather data outside their intended purpose leading to user profiling and potential privacy breaches. Analytic tracking faces significant challenges because of its legal and regulatory framework requirements. Users need to receive data collection information according to GDPR and CCPA regulations so they can exercise their right to opt out of data sharing. Analytics implementations that lack clear consent mechanisms might result in both non-compliance and legal consequences. SDKs integrated with applications present security risks because outdated libraries and insecure API endpoints can lead to vulnerabilities. The security analysis of MobSF identifies analytic components while assessing their permission requests and monitors network traffic for data leaks and determines if they lead to excessive data collection.

Identification—MobSF defines identification as the process of gathering distinct device and user identifiers that mobile applications utilize for authentication procedures and tracking functions and personalized user experiences. Mobile applications track users through both device-specific identifiers such as IMEI and MAC addresses and user-specific information including Android IDs and advertising IDs together with email addresses and phone numbers and account login data. Security identification methods play an important role in protecting users from threats but they pose substantial privacy and security risks when their implementation is not done correctly. MobSF identifies identification tracking as a critical data collection pathway that enables unauthorized profiling of users. A few applications send persistent identifiers to external services which allows third parties to track users through multiple programs. Multiple device parameters combined through this practice generate unique user profiles that occur without user consent. The implementation of tracking systems violates user privacy and violates GDPR and CCPA because these regulations specify detailed rules about user data collection and storage. The storage or

transmission of identifiers by applications generates security problems because of insufficient encryption and weak access control measures. The exposure of identifiers through unsecured network requests and weak local storage allows criminals to intercept and manipulate and misuse these identifiers. The exposure of identifiers enables attackers to commit identity theft and unauthorized account entry and perform device impersonation attacks. MobSF examines application identification methods through API call analysis and data storage tracking and network protocol examination to determine security and privacy risks.

Location—MobSF defines location as the process of collecting and processing and transmitting geospatial data from mobile devices to identify user location. Mobile applications collect location data using GPS and Wi-Fi signals and cell tower information and Bluetooth to deliver services like navigation, targeted advertising, geofencing, and content personalization. The necessity of location data for improving user experience generates serious privacy and security challenges that mobile application security must actively handle. According to MobSF location tracking stands as a fundamental security risk since numerous applications gather user-sensitive information without proper consent or notification. A significant number of mobile applications that use analytics and advertising features collect location data without notifying users directly about this information collection process. The collected data enables the creation of detailed user profiles through geolocation patterns but presents privacy risks when disclosure and management are inadequate. Location data becomes a target for malicious actors because they use it to monitor people and identify valuable targets and execute social engineering schemes. Unprotected channels for transmitting location data expose users to interception risks, especially during transmissions of sensitive geospatial information to unencrypted third-party servers. Many applications that request access to user locations do not implement adequate security measures to protect this data from unauthorized exposure during storage or transmission. The location data review at MobSF involves checking location permission levels and network traffic analysis for unauthorized signals and encryption and data management practice assessments to evaluate security and privacy risks.

4. Results

The analysis of 6,165 APK files scanned with MobSF reveals comprehensive insights into the usage patterns, categories, and implications of analytics frameworks and trackers embedded in mobile applications. By examining individual tracker popularity, functional categories, and app genre-specific trends, this section provides a detailed understanding of the privacy and security challenges associated with these frameworks.

4.1. Popularity of individual trackers

The analysis identified the most frequently used trackers in the scanned APK files. Among the findings:

- Google Firebase Analytics emerged as the most commonly integrated framework, appearing in 5,207 apps (84.46%). Its widespread usage reflects its dual role as a tool for user behavior analysis and app performance monitoring.
- Google CrashLytics was present in 3,687 apps (59.81%), underlining its critical function in debugging and crash reporting.
- Google AdMob [34], an advertising-focused framework, was found in 3,087 apps (50.07%), showcasing its prominence in app monetization strategies.
- Facebook Login [35] was identified in 1,996 apps (32.38%), indicating its popularity for facilitating user authentication and integrating social media functionality.
- Facebook Share [36], present in 1,824 apps (29.59%), further highlights the strong presence of Facebook's SDKs in mobile applications.

These findings emphasize the dominance of Google and Facebook frameworks across various functionalities, raising concerns about data centralization and potential privacy risks. Smaller trackers, while less prevalent, also contribute to the ecosystem, with varying implications based on their functionality.

The list of the top 25 most integrated analytical frameworks is provided in Table 1.

Table 1
Top 25 most integrated analytical frameworks

Analytical tracker name	Apps use it, %
Google Firebase Analytics	84,46
Google CrashLytics	59,81
Google AdMob	50,07
Facebook Login	32,38
Facebook Share	29.59
Facebook Analytics	26.65
Facebook Ads	19.11
IAB Open Measurement	17.71
Google Analytics	15.15
AppsFlyer	14.65
AppLovin (MAX and SparkLabs)	13.06
Google Tag Manager	12.86
Adjust	9.20
Pangle	8.69
Unity3d Ads	8.32
OneSignal	7.54
ironSource	6.52
Facebook Places	6.23
Mintegral	5.69
Sentry	5.27
AppMetrica	4.67
Inmobi	4.48
Branch	4.02
Fyber	3.73
Yandex Ad	3.68

4.2. Categorization of trackers

Trackers were categorized based on their primary roles in mobile applications (see Fig. 1).

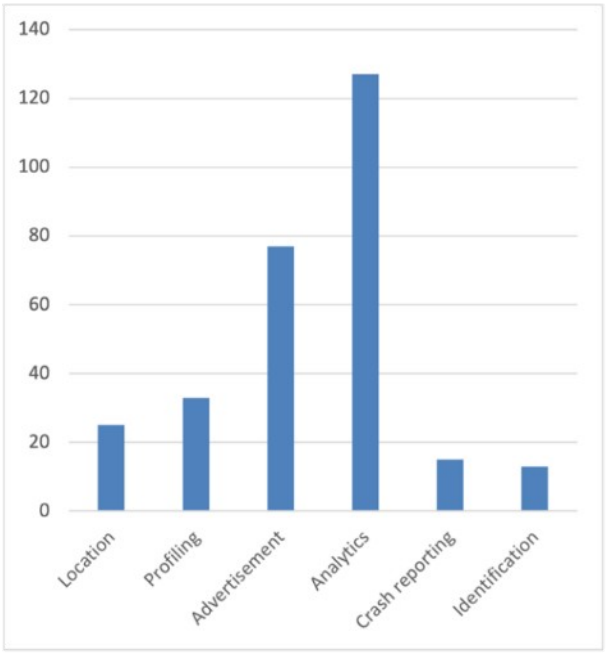

Figure 1: Number of unique trackers per category

The analysis revealed the following key categories:

- Analytics—representing the largest category, 127 unique trackers were identified. These frameworks provide insights into user behavior, app performance, and engagement metrics. They are indispensable for developers but pose risks of excessive data collection.
- Advertisement—with 77 unique trackers, this category underscores the focus on monetization through ad targeting. These trackers often collect detailed user profiles, including location and behavioral data.
- Profiling—comprising 33 unique trackers, these frameworks specialize in gathering user attributes for personalized experiences and targeted advertising. This category raises significant privacy concerns due to the detailed nature of the data collected.
- Crash Reporting—with 15 unique trackers, these frameworks support app stability by logging errors and crashes. While useful for debugging, they may inadvertently capture sensitive data in logs if not configured properly.
- Location Services—consisting of 25 unique trackers, these frameworks enable geolocation-based functionalities. Apps using these trackers must carefully balance functionality with privacy to avoid exposing sensitive user data.

These categories illustrate the diversity of data collection practices in mobile apps and highlight specific privacy and security risks associated with particular functionalities.

4.3. Tracker usage across app genres

The prevalence and average number of trackers were analyzed across different app genres, revealing notable trends:

- Dating Apps—with an average of 7.64 trackers per app across 202 samples, dating apps exhibited the highest reliance on analytics and advertising frameworks. This trend reflects

the genre's focus on engagement and monetization, but it also raises significant concerns about the handling of sensitive user data.

- Personalization Apps—these apps had an average of 7.11 trackers per app (274 samples), indicating extensive use of profiling and analytics to tailor user experiences.
- News and Magazines—with 7.05 trackers per app (443 samples), this genre heavily integrates advertising frameworks to support revenue generation through targeted ads.
- Entertainment Apps—averaging 6.60 trackers per app (417 samples), these apps focus on engagement metrics, often integrating social media and advertising frameworks.
- Social Media Apps—with 6.35 trackers per app (438 samples), this genre relies on analytics, profiling, and location services to optimize user interactions and ad targeting.

See extended data on the average number of trackers per Google Play genre in Fig. 2.

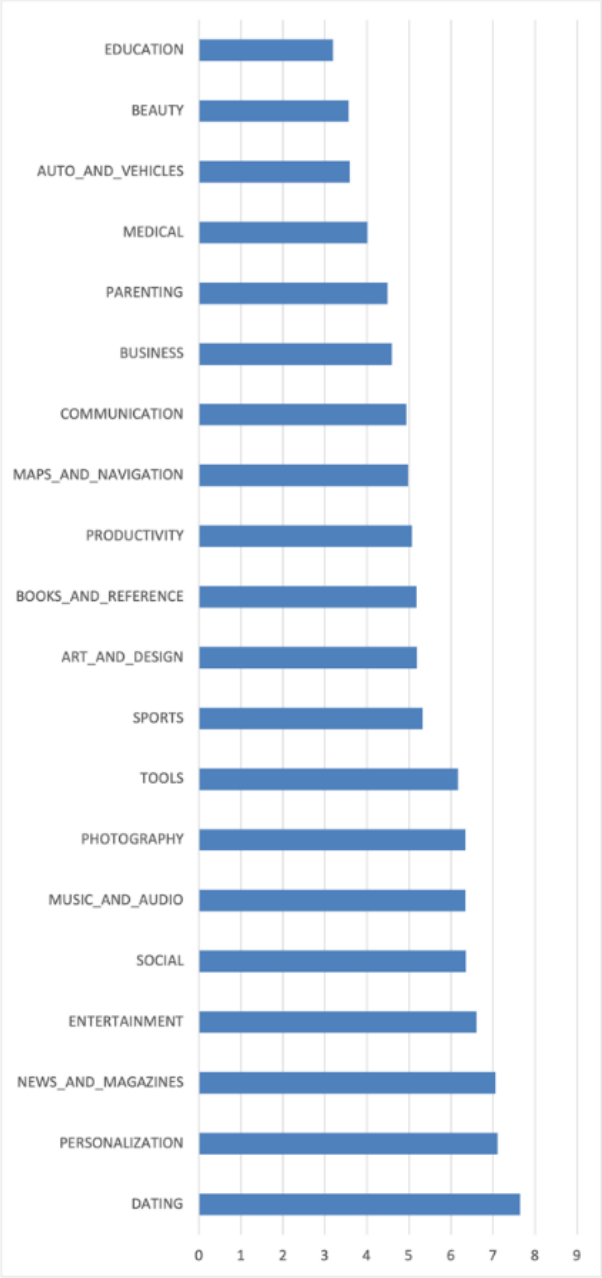

Figure 2: Average number of trackers in app per Google Play category

This variability across genres reflects differing priorities in app development, with some genres placing a greater emphasis on data collection to support monetization and user engagement.

4.4. Observations on dominance and privacy risks

The dominance of specific companies and frameworks in the tracker ecosystem emerged as a key theme. Google and Facebook SDKs accounted for a substantial portion of all identified trackers, providing critical functionality in analytics, advertising, and social media integration. However, this concentration of power also creates systemic risks, including:

- Centralization of user data—the reliance on a few dominant players amplifies risks of extensive data aggregation, which could be exploited in case of data breaches or unauthorized access.
- Privacy risks in profiling and location services—trackers in the profiling and location services categories were observed to gather highly sensitive user information. These practices raise ethical and legal concerns, particularly in light of regulations like GDPR and CCPA.
- Potential security vulnerabilities—frameworks with known vulnerabilities, such as outdated SDKs, increase the attack surface for mobile applications. Apps that fail to update their trackers to patch known vulnerabilities expose themselves and their users to potential exploitation.

5. Discussion

The static analysis of 6,165 APK files using MobSF revealed the top 25 most integrated analytics frameworks in mobile applications. While these frameworks provide essential functionalities such as user behavior tracking, crash reporting, and monetization, their widespread adoption introduces significant privacy and security risks. This discussion focuses on the vulnerabilities (CVEs) identified for these frameworks, highlighting their implications for developers, users, and application ecosystems.

5.1. Google frameworks

Google's analytics and advertising frameworks dominate mobile app ecosystems, with Firebase Analytics (84.46%), CrashLytics (59.81%), and AdMob (50.07%) being the most integrated frameworks in the dataset. Although these tools are indispensable for monitoring performance and generating revenue, their extensive use raises critical security concerns:

- Google Firebase Analytics has been associated with improper implementation risks. While no specific CVEs have been reported, insecure configurations or insufficient access controls can result in unauthorized data exposure.
- Google CrashLytics handles crash logs that may inadvertently include sensitive user information. Although no direct CVEs exist, improper sanitization or logging practices can expose apps to significant data leakage risks.
- Google AdMob facilitates in-app advertisements, but its integration increases the risk of user profiling and exposure to malicious ads. Historical vulnerabilities in Google's advertising ecosystem, such as exposed APIs, have demonstrated the need for secure implementation and regular monitoring.

These findings underscore the need for rigorous data minimization practices and periodic security audits for applications integrating Google frameworks.

5.2. Facebook frameworks

Facebook's SDKs are among the most widely adopted, with Facebook Login (32.38%), Share (29.59%), and Analytics (26.65%) leading the list. However, these frameworks have historically been targets for security exploits:

- Facebook Login—while offering seamless user authentication, vulnerabilities such as improper session handling or token hijacking have been reported in similar authentication systems. For example, CVE-2018-6013 highlights the risks of session misuse.
- Facebook Analytics and Ads—these frameworks collect detailed user data for engagement and advertising purposes. Although no recent CVEs are directly linked to Facebook Ads, concerns about privacy breaches through excessive data collection persist, particularly given the platform's past involvement in large-scale data misuse cases (e.g., Cambridge Analytica).
- Facebook Share—while no specific vulnerabilities have been disclosed, insecure implementations could expose user data shared via social media, leading to privacy violations.

The significant reliance on Facebook frameworks underscores the importance of ensuring secure SDK versions and adhering to privacy-by-design principles.

5.3. Sentry

Sentry (5.27%) [37] is widely used for error tracking and performance monitoring. It has been the subject of several critical vulnerabilities:

- CVE-2025-22146 [38]—a critical vulnerability (CVSS 9.1) in Sentry's SAML SSO implementation allows attackers to take over user accounts with a malicious identity provider and the victim's email address. This poses a severe risk to organizations relying on Sentry for production environments.
- CVE-2024-45606 [39]—a high-severity vulnerability (CVSS 7.1) allows authenticated users to bypass authorization checks and mute alert rules for arbitrary projects. Exploitation could allow attackers to suppress critical security alerts.
- CVE-2023-46729 [40]—a critical vulnerability (CVSS 9.3) in Sentry's Next.js SDK allowed unsanitized input to perform HTTP request forgery, exposing applications to malicious payloads.

These vulnerabilities highlight the risks of relying on third-party monitoring tools for critical operations. Ensuring timely patching and secure integration is essential to mitigating such risks.

5.4. AppsFlyer and adjust

AppsFlyer [41] (14.65%) and Adjust [42] (9.2%) provide mobile attribution and marketing analytics but carry inherent risks associated with user profiling and data sharing: While no specific CVEs have been disclosed, these frameworks involve the collection of detailed user data for attribution purposes. Misconfigurations or outdated SDK versions can lead to privacy violations or unauthorized data sharing. Developers must scrutinize data-sharing agreements and enforce strict privacy policies to mitigate potential risks associated with marketing analytics tools.

5.5. IAB open measurement and AppLovin

IAB Open Measurement [43] (17.71%) and AppLovin [44] (13.06%) are integral to advertising ecosystems. Vulnerabilities in advertising SDKs, such as insecure API handling or excessive

permissions, can expose applications to malicious ads and unauthorized data collection. Ensuring secure configurations and limiting permissions are critical for reducing these risks.

5.6. Lesser-integrated frameworks

Frameworks such as Unity3d Ads [45] (8.32%), OneSignal [46] (7.54%), Mintegral [47] (5.69%), and Yandex Ad [48] (3.68%) represent a smaller but still significant share of integrations. While specific CVEs for these frameworks are less documented, their presence amplifies the overall attack surface of mobile applications. Potential risks include insecure implementations, data exposure through poorly configured APIs, and insufficient user consent mechanisms.

5.7. Broader implications

The integration of third-party analytics frameworks introduces systemic risks to mobile applications:

- Privacy Risks—frameworks that collect extensive user data, particularly for profiling and advertising, can lead to unauthorized data sharing and non-compliance with regulations like GDPR and CCPA.
- Increased Attack Surface—each integrated framework introduces potential vulnerabilities. Applications with multiple frameworks amplify this risk, particularly if outdated SDK versions are used.

Regulatory Challenges—misaligned data collection practices and insufficient transparency can expose developers to legal and reputational risks.

Conclusions

These results provide a comprehensive understanding of the prevalence and impact of trackers in mobile applications. By analyzing their popularity, functional categorization, and usage across genres, this study reveals critical insights into the privacy and security challenges posed by analytics frameworks, paving the way for further discussions on mitigation strategies and regulatory improvements.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] General data protection regulation. URL: https://gdpr-info.eu

[2] The mission of the CVE® program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. URL: https://cve.mitre.org

[3] C. Anwar, et al., The application of mobile security framework (MOBSF) and mobile application security testing guide to ensure the security in mobile commerce applications, J. Sistim Informasi dan Teknologi, 5 (2023) 97–102. doi:10.37034/jsisfotek.v5i2.231

[4] E. E. Archibong, B. Stephen, P. Asuquo, Analysis of cybersecurity vulnerabilities in mobile payment applications, Arch. Adv. Eng. Sci. (2024) 1–12. doi:10.47852/bonviewAAES42022595

[5] K. Kollnig, et al., Goodbye tracking? Impact of iOS app tracking transparency and privacy labels, in: 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT'22), 2022, 508–520. doi:10.1145/3531146.3533116

[6] X. Liu, et al., Privacy risk analysis and mitigation of analytics libraries in the Android ecosystem, in: IEEE Transactions on Mobile Computing, vol. 19(5), 2020, 1184–1199. doi:10.1109/TMC.2019.2903186
[7] A. Nyzhnyk, A. Partyka, M. Podpora, Increase the cybersecurity of SCADA and IIoT devices with secure memory management, in: Cyber Security and Data Protection, vol. 3800, 2024, 32–41.
[8] Y. Martseniuk, et al., Shadow IT risk analysis in public cloud infrastructure, in Cyber Security and Data Protection, vol. 3800, 2024, 22–31.
[9] Facebook to pay $725 million to settle lawsuit over Cambridge Analytica data leak. URL: https://thehackernews.com/2022/12/facebook-to-pay-725-million-to-settle.html
[10] 540 million facebook user records found on unprotected Amazon servers. URL: https://thehackernews.com/2019/04/facebook-app-database.html
[11] More than 250 iOS Apps caught using private APIs to collect users' private data. URL: https://thehackernews.com/2015/10/apple-ios-malware-apps.html
[12] Warning! Popular Apple Store Apps infected with data-theft malware. URL: https://thehackernews.com/2015/09/apple-apps-malware.html
[13] C. Cai, et al., Vizard: A metadata-hiding data analytic system with end-to-end policy controls, in: 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS'22), 2022, 441–454. doi:10.1145/3548606.3559349
[14] H. Lu, et al., Detecting and measuring aggressive location harvesting in mobile apps via data-flow path embedding, in: Proc. ACM Meas. Anal. Comput. Syst. 7(1), 2023. doi:10.1145/3579447
[15] L. Xinyu, et al., ANDetect: A third-party ad network libraries detection framework for Android applications, in: 39th Annual Computer Security Applications Conference (ACSAC '23), 2023, 98–112. doi:10.1145/3627106.3627182
[16] Y. Han, et al., Systematic analysis of security and vulnerabilities in miniapps, in: 2023 ACM Workshop on Secure and Trustworthy Superapps (SaTS'23), 2023, 1–9. doi:10.1145/3605762.3624432
[17] S. Canard, et al., WeStat: A privacy-preserving mobile data usage statistics system, in: 2021 ACM Workshop on Security and Privacy Analytics (IWSPA'21), 2021, 5–14. doi:10.1145/3445970.3451151
[18] I. Kuksa, et al., Chapter five—Predictive personalisation: are we watching or being watched?, Understanding Personalisation (2023) 89–108. doi:10.1016/B978-0-08-101987-0.00008-4
[19] L. K. Agrawal, D. K. Agrawal, K. G. Srinivasa, Security and privacy in health data storage and its analytics, Blockchain for 5G Healthcare Applications: Security and privacy solutions, (2024) 249–285. doi:10.1049/PBHE035E_ch10
[20] V. Dudykevych, et al., A multicriterial analysis of the efficiency of conservative information security systems, Eastern-European J. Enterp. Technol. (2019) 6–13. doi:10.15587/1729-4061.2019.166349
[21] V. Petrivskyi, et al., Development of a modification of the method for constructing energy-efficient sensor networks using static and dynamic sensors, Eastern-European J. Enterp. Technol. 1.9(115) (2022) 15–23. doi:10.15587/1729-4061.2022.252988
[22] V. Susukailo, I. Opirsky, O. Yaremko, Methodology of ISMS establishment against modern cybersecurity threats, in: Future Intent-Based Networking. Lecture Notes in Electrical Engineering, vol. 831, 2021, 257–271. doi:10.1007/978-3-030-92435-5_15
[23] R. Banakh, A. Piskozub, I. Opirskyy, Detection of MAC spoofing attacks in IEEE 802.11 networks using signal strength from attackers' devices, in: Advances in Computer Science for Engineering and Education, ICCSEEA 2018, Advances in Intelligent Systems and Computing, vol. 754, 2018, 468–477. doi:10.1007/978-3-319-91008-6_47
[24] T. Fedynyshyn, I. Opirskyy, O. Mykhaylova, A method to detect suspicious individuals through mobile device data, in: 2023 IEEE 5th International Conference on Advanced Information and Communication Technologies (AICT), 2023, 82–86. doi:10.1109/AICT61584.2023.10452683

[25] T. Fedynyshyn, O. Mykhaylova, I. Opirskyy, Security Implications of mobile development frameworks: findings from static analysis of Android apps, in: 2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2024, 444–448. doi:10.1109/TCSET64720.2024.10755684
[26] Mobile Security Framework (MobSF). URL: https://mobsf.github.io/docs
[27] O. Mykhaylova, T. Fedynyshyn, A. Platonenko, Hardcoded credentials in Android apps: Service exposure and category-based vulnerability analysis, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826, 2024, 206–211.
[28] Firebase Crashlytics. URL: https://firebase.google.com/docs/crashlytics
[29] Bugsnag. Application insights your developers need without the noise. URL: https://www.bugsnag.com/
[30] Google Analytics. URL: https://developers.google.com/analytics
[31] AppMetrica. URL: https://appmetrica.yandex.com/about
[32] Firebase. URL: https://firebase.google.com/
[33] Mixpanel: Product Analytics for Mobile, Web & More. URL: https://mixpanel.com
[34] Google AdMob. Earn More with Mobile App Monetization AdMob. URL: https://admob.google.com
[35] Facebook Login. URL: https://developers.facebook.com/docs/facebook-login/
[36] Facebook Share. URL: https://developers.facebook.com/docs/sharing
[37] Sentry: Application performance monitoring & error tracking software. URL: https://sentry.io/
[38] CVE-2025-22146 Detail. URL: https://nvd.nist.gov/vuln/detail/CVE-2025-22146
[39] CVE-2024-45606 Detail. URL: https://nvd.nist.gov/vuln/detail/CVE-2024-45606
[40] CVE-2023-46729 Detail. URL: https://nvd.nist.gov/vuln/detail/CVE-2023-46729
[41] Unlock your app's potential. Reliable, stable and always up to date with the market. URL: https://www.appsflyer.com/
[42] Adjust is your end-to-end solution for every stage of the app marketing journey. URL: https://www.adjust.com/
[43] Open measurement SDK. URL: https://www.iab.com/guidelines/open-measurement-sdk/
[44] Instant payouts & High eCPM — One SDK. URL: https://appodeal.com/
[45] Unity ads: Mobile game ad network platform & analytics. URL: https://unity.com/products/unity-ads
[46] Free push notification service. Re-engage users & nurture loyalty with OneSignal's push notifications & in-app messaging. URL: https://onesignal.com/
[47] Mintegral provides a powerful mobile advertising solution to help you overcome cross-regional challenges and grow your app on a global scale. URL: https://www.mintegral.com/en
[48] Grow your mobile metrics with an all-in-one platform for mobile analytics and marketing. URL: https://ads.yandex.com/