Privacy Threats and Profiling Risks in Free Android Applications

Musa Ibrahim Kamba[1]; Aminu Dauda[2]

[1,2]Department of Computer Science, Waziri Umaru Federal Polytechnic Birnin Kebbi, 862106, Nigeria

Publication Date: 2026/01/08

Abstract: The widespread adoption of free Android applications in low- and middle-income communities has transformed communication, entertainment, and access to services, but it has also introduced significant privacy and security risks. This study investigates the usage patterns, privacy awareness, permission-granting behaviors, and exposure to data exploitation among Android users in Birnin Kebbi, Nigeria. Employing a mixed-methods approach, data were collected through structured questionnaires (n = 200), semi-structured interviews (n = 20), and direct observations. Findings reveal that 92% of respondents use free apps daily, with social media (85%) and entertainment apps (78%) dominating usage. Despite this, digital literacy and awareness of data protection regulations remain low, with only 27% understanding app data collection practices and 12% aware of the Nigeria Data Protection Regulation (NDPR). The study also identified prevalent user-permission fatigue, with 68% of respondents routinely granting broad permissions—including access to contacts, camera, microphone, location, and storage—without full comprehension of implications. Third-party SDKs and trackers further exacerbate data exposure, while 31% of respondents reported experiences of digital fraud, such as unauthorized social media access, phishing, and unexpected mobile wallet deductions. The results highlight the cyclical relationship between high app dependence, low privacy awareness, and limited digital literacy, which collectively heighten vulnerability to profiling, surveillance, and fraud. The study recommends targeted digital literacy programs, NDPR awareness campaigns, promotion of privacy-preserving practices, integration of privacy-by-design in app development, and accessible mechanisms for monitoring and reporting digital fraud to strengthen user protection in the Nigerian mobile ecosystem.

Keywords: *Privacy Threats, User Profiling, Free Android Applications.*

How to Cite: Musa Ibrahim Kamba; Aminu Dauda (2026) Privacy Threats and Profiling Risks in Free Android Applications. *International Journal of Innovative Science and Research Technology,* 11(1), 158-164.
https://doi.org/10.38124/ijisrt/26jan005

I. INTRODUCTION

Mobile applications have become integral to daily life worldwide, facilitating communication, entertainment, financial transactions, and access to essential services. In particular, Android-based smartphones dominate the mobile ecosystem due to their affordability, diverse functionality, and availability of free applications. Free Android apps—ranging from social media and messaging platforms to utility and entertainment tools—have grown tremendously in adoption, especially among users in low- and middle-income communities where cost is a key consideration [1,2].

While free apps provide significant benefits, they often operate on data-driven business models that rely heavily on the collection, processing, and monetization of user information. Personal data collected may include device identifiers, geolocation, contacts, camera and microphone access, usage patterns, and demographic information [3,4]. In many cases, third-party libraries and software development kits (SDKs) embedded within apps further amplify data collection and introduce additional privacy risks, often without users' explicit consent or awareness [5,6].

The risks of excessive data collection and poor privacy practices are compounded by low digital literacy, limited user awareness of regulatory protections such as the Nigeria Data Protection Regulation (NDPR), and the prevalence of user-permission fatigue, where individuals grant broad access to app permissions without understanding their implications [4,7]. Such practices expose users to profiling, targeted advertising, identity theft, phishing, digital fraud, and unauthorized data sharing [8,9].

Despite the global attention on mobile app privacy and security, empirical studies focusing on the Nigerian context remain limited, particularly those that examine user behavior, awareness, permission practices, and exposure to data exploitation within free Android app ecosystems. Understanding these patterns is critical for developing effective interventions, including user education, privacy-by-design frameworks, regulatory enforcement, and the promotion of privacy-preserving technologies [10,11].

Against this backdrop, this study investigates the usage patterns, privacy awareness, permission-granting behaviors, and exposure to data exploitation among Android users in Birnin Kebbi. The study employs a mixed-methods approach, integrating structured questionnaires, semi-structured interviews, and direct observations to generate a comprehensive understanding of user practices and risks. Findings from this study aim to inform policymakers, developers, and users about the vulnerabilities inherent in free app usage and provide evidence-based recommendations for enhancing privacy and digital security in the Nigerian mobile context.

II. REVIEW OF RELATED WORK

➢ *Data Collection Practices in Free Android Apps*

Free Android applications commonly rely on data-driven business models, collecting and transmitting rich personal information to external servers for purposes such as analytics, advertising, and tracking. [1] showed that many pre-installed or system-level apps send device identifiers, geolocation, and usage data to third-party servers. Similarly, [12] found that OEMs (device manufacturers) and app developers log sensitive data including persistent IDs, advertising IDs, and location, often without transparent user consent.

Globally, large-scale studies have documented widespread collection of identifiers, location, and other personal data across apps [1,12]. In the Nigerian context, while empirical app-level measurement work is still emerging, legal and policy analyses have highlighted how weak enforcement of data protection exposes users: [9] argued that insufficient enforcement of the NDPR leaves Nigerian users vulnerable to surveillance and data misuse.

➢ *User Profiling and Behavioral Tracking*

Profiling through behavioral tracking remains a major privacy threat, particularly in advertising-driven ecosystems. [4] demonstrated that mobile applications can build detailed user profiles by combining behavioral data with demographic information, enabling predictive advertising. In developing contexts, such profiling intersects with low user awareness and consent. [8] documented that Nigerian users frequently grant broad permissions without fully understanding the consequences, increasing their exposure to identity theft, fraud, and targeted manipulation.

Moreover, cross-device tracking techniques amplify profiling risks, as persistent identifiers allow companies to link user behavior across multiple devices [4,13].

➢ *Third-Party Libraries and SDK Risks*

Third-party SDKs (Software Development Kits) embedded within Android apps are a major vector for privacy risks. Many SDKs collect data independently of the host app's primary function, often accessing sensitive APIs and extracting device identifiers, location, or behavioral data [3]. Large-scale studies of 158 widely used SDKs have revealed hundreds of instances of data exfiltration, misrepresented data access, or lack of privacy policies [14].

[4] developed ATPChecker, a tool to statically analyze TPLs' (Third-Party Libraries) compliance with privacy regulations, finding discrepancies between declared behavior and actual data flows. Privacy risks are further compounded when developers leave SDK settings at default, less secure configurations. For example, studies of Facebook SDK integration across thousands of apps found that most developers do not change default privacy settings [6]. Systematic literature reviews also note that third-party libraries increase attack surfaces and permission overreach since they inherit permissions granted to the host app [4].

➢ *Regulatory Gaps and NDPR Enforcement Challenges*

Regulatory frameworks are essential for controlling how user data is collected and used, yet gaps remain, especially in Nigeria. Although the NDPR was introduced to establish baseline protections, enforcement and compliance remain limited. [15] found significant disparities in compliance across sectors, with SMEs and public institutions showing weak adherence. Many organizations lack capacity to implement meaningful data protection measures, and penalties under the NDPR have limited deterrent effect.

The recent Nigeria Data Protection Act [16], strengthens institutional frameworks, such as the Nigeria Data Protection Commission, but challenges in guidance, technical capacity, and enforcement persist [17].

➢ *User Awareness and Digital Literacy*

User behavior significantly affects data protection outcomes. Empirical research in Nigeria shows that low digital literacy contributes to uninformed consent: [7] found that many smartphone users do not read or understand app privacy policies and routinely grant permissions without full awareness. Related studies support this finding, showing that gaps in understanding how apps store and share data increase exposure to profiling, data misuse, and fraud [18].

➢ *Emerging Privacy-Preserving Technologies*

Globally, privacy-preserving technologies (PPTs) such as privacy-by-design, anonymization, differential privacy, and decentralized identity systems are gaining adoption [10]. These frameworks embed privacy at the architectural level, minimizing data collection and using pseudonymized identifiers.

In the Nigerian mobile app ecosystem, adoption of these technologies remains limited. Legal and policy commentators highlight a technological gap compounded by low regulatory capacity, which hinders meaningful deployment of PPTs. [11] note that few local developers or institutions integrate privacy-by-design in app development, leaving users exposed despite global advances.

III. METHODOLOGY

The study employed a mixed-method research design**,** integrating quantitative and qualitative approaches to obtain both breadth and depth of insight. The quantitative component, collected through structured questionnaires, enabled the measurement of trends in app usage, privacy awareness, and permission-granting behavior. The qualitative component, based on semi-structured interviews and direct observation, provided deeper contextual understanding of user experiences, perceptions, and privacy decision-making processes. This triangulation strengthened the reliability and validity of the findings by allowing cross-verification of results from multiple sources. High levels of smartphone penetration and the popularity of free mobile applications among residents provide a representative context for understanding mobile privacy practices in northern Nigeria.

A. Study Populations

The study population comprised Android smartphone users residing in Birnin Kebbi across varied socioeconomic and demographic categories. These included students, civil servants, traders, ICT workers, business professionals, and unemployed youths. Android users were specifically targeted because Android is the most commonly used operating system in Birnin Kebbi due to its affordability and wide availability. Participants were drawn from major activity centers such as:

- Waziri Umaru Federal Polytechnic Birnin Kebbi
- Urban markets and commercial districts
- Residential neighborhoods
- Cyber cafés and ICT centers
- Government and private-sector offices

This ensured the inclusion of participants with diverse app usage patterns and levels of digital literacy.

B. Sampling Technique and Sample Size

The study adopted a multistage sampling technique to ensure representativeness and systematic selection of respondents in three stages.

➢ *Stage One: Selection of Sampling Clusters*

Key urban clusters—including educational institutions, markets, residential areas, and ICT centers—were purposively selected based on high concentrations of smartphone users.

➢ *Stage Two: Selection of Participants*

Within each cluster, convenience and purposive sampling techniques were used to identify individuals who actively use free Android applications, such as social media, entertainment, communication, gaming, and utility apps.

➢ *Stage Three: Determination of Sample Size*

A total of 200 participants were targeted for the questionnaire survey to provide adequate statistical representation. In addition, 20 participants were purposively selected for in-depth interviews based on their willingness and ability to articulate their app usage experiences and privacy concerns. This multi-level sampling strategy ensured comprehensive coverage of user perspectives relevant to privacy risks.

IV. RESULT

This section presents the major findings of the study, derived from structured questionnaires, semi-structured interviews, and direct observation of Android users in Birnin Kebbi. The results illuminate patterns of free Android application usage, levels of privacy awareness, permission-granting behavior, and exposure to data exploitation risks. The discussion contextualizes these findings within existing literature and the socio-digital environment of Birnin Kebbi.

A. App Usage Patterns Among Residents of Birnin Kebbi

The questionnaire data revealed that free Android applications are deeply embedded in the daily routines of residents in Birnin Kebbi. Approximately 92% of respondents reported daily use of free apps, reflecting the pervasive nature of such applications in everyday life. Analysis of app categories indicated that social media applications (Facebook, WhatsApp, TikTok, Instagram, X) were the most frequently used, with 85% of respondents reporting regular engagement. Entertainment applications, including video streaming, music, and gaming apps, were used by 78% of respondents, particularly among youths, highlighting their central role in leisure activities. Additionally, utility apps (e.g., Opera Mini, flashlights, calculators, and other tools) were used by 65% of respondents, while communication apps (SMS, email, VoIP services) were utilized by 60%, indicating that these apps remain relevant but slightly less prioritized compared to social and entertainment apps.

Interviews indicated that the preference for free applications is primarily driven by the elimination of financial barriers and the minimal reliance on mobile data. Users reported that free apps provide convenient access to essential services and entertainment without incurring additional costs. However, this reliance on free apps also increases users' exposure to extensive data collection and privacy risks, as many of these applications employ aggressive data harvesting strategies.

These findings align with prior research by [19], who noted that heavy dependence on free applications amplifies susceptibility to privacy risks, particularly in low-income communities. The high adoption rates of social media and entertainment apps underscore the importance of raising awareness about privacy practices and encouraging users to adopt protective behaviors while using free applications as shown in the Figure 1.

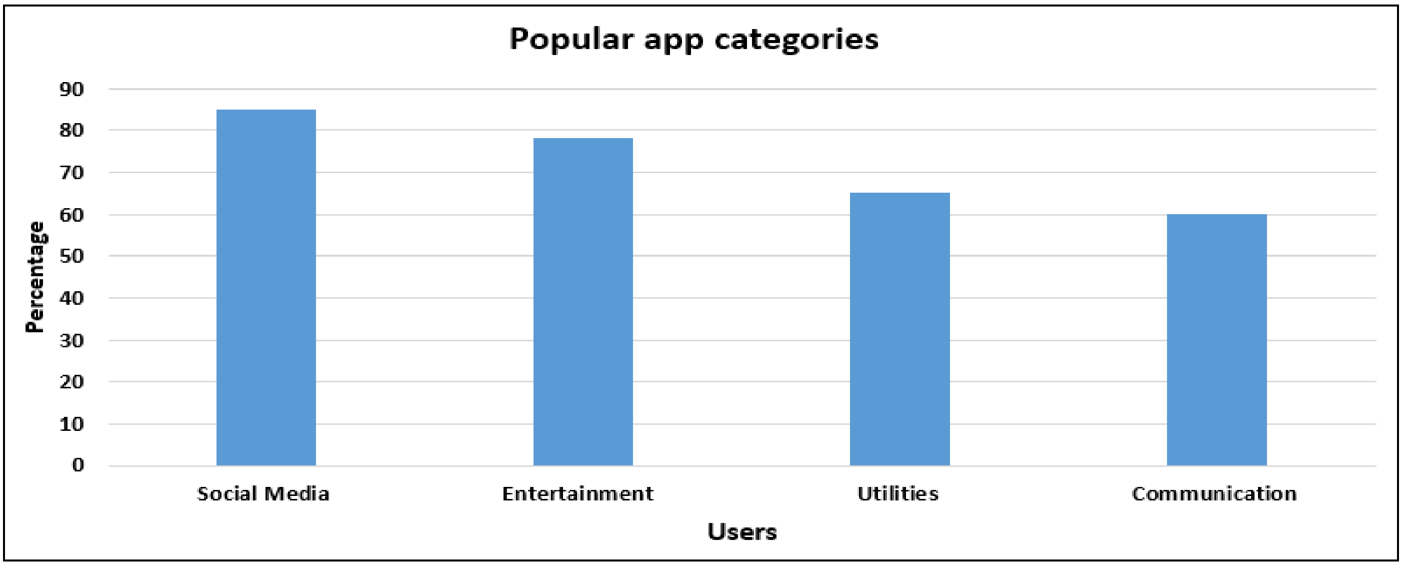

Fig 1 Popular App Categories

B. Awareness of Privacy Risks and NDPR Compliance

The study found low levels of privacy awareness among Android users in Birnin Kebbi with **27%** demonstrated a basic understanding of app data collection practices, and only 12% were aware of the Nigeria Data Protection Regulation (NDPR).

Interviews revealed a common misconception as shown below in Figure 2: users generally assume that app developers, the Google Play Store, or mobile network providers automatically safeguard their data. This belief contributes to uninformed consent, with users frequently selecting "Allow" without reading permission prompts.

These results align with [7], who emphasize that deficits in digital literacy heighten the risk of personal data misuse in Nigeria.

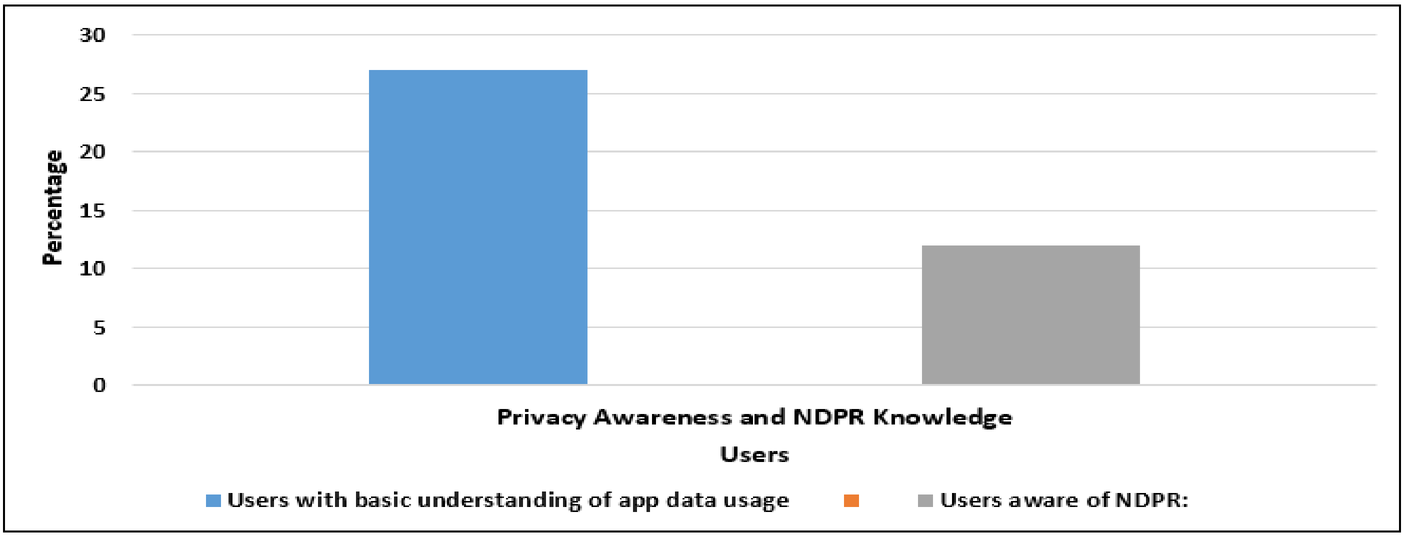

Fig 2 Privacy Awareness and NDPR Knowledge

C. Permission-Granting Behavior and Exposure to Intrusive Access

The survey results in Figure 3, revealed that 68% of respondents routinely grant all requested permissions without fully understanding their implications. Users often justified this behavior by expressing concerns that applications might malfunction or lose functionality if permissions were denied. Analysis of specific permissions granted shows that access to contacts was approved by 72% of respondents, camera and microphone by 65%, storage by 60%, precise location by 58%, and SMS and call logs by 50%.

Direct observations confirmed that users frequently approved high-risk permissions for applications that did not require them to function properly—for instance, flashlight or utility apps requesting access to contacts or location data. This trend indicates a pervasive pattern of user-permission fatigue, as described by [4], whereby users habitually accept permission requests without critical evaluation. Such behavior significantly increases the likelihood of profiling, surveillance, and data exploitation, placing users at elevated privacy risk.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan005

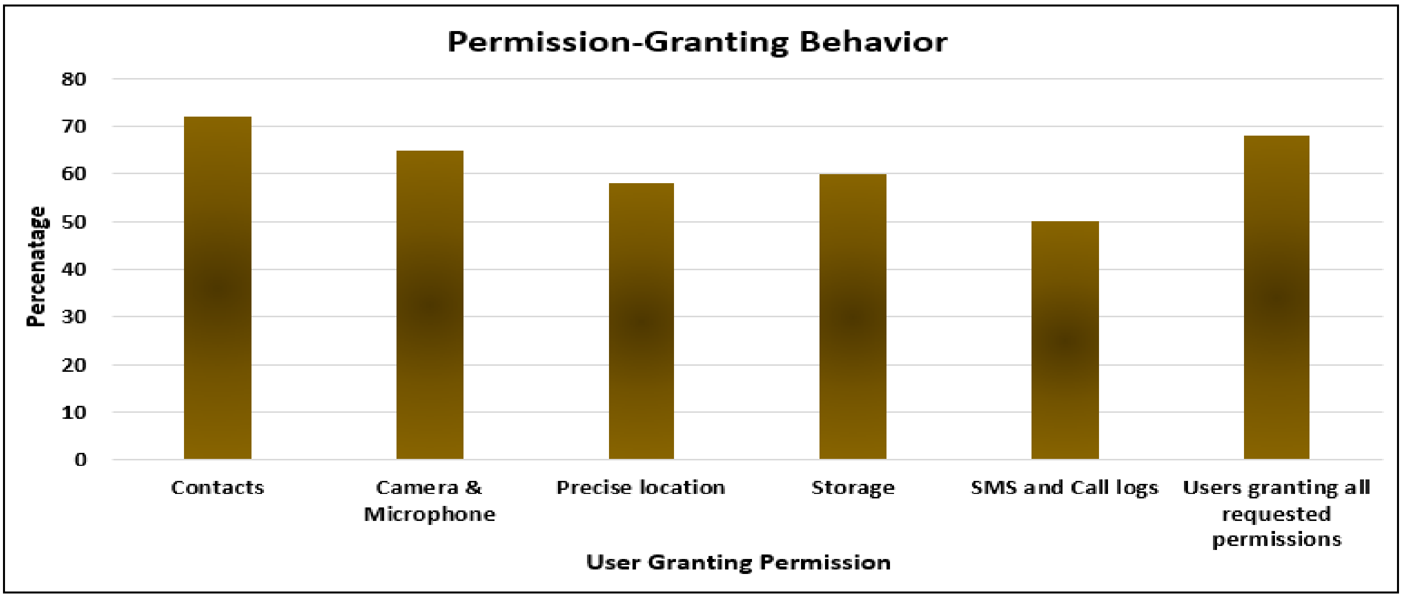

Fig 3 Percentages of Permissions Commonly Granted by Users

D. Prevalence of Third-Party Trackers

Interviews and app observations indicated that many popular free applications embed third-party SDKs, which facilitate:

- Targeted advertising
- Analytic data collection
- Background tracking

Most users were unaware of these trackers. Several expressed surprise upon learning that SDKs often transmit data to foreign servers, sometimes in regions with weak privacy protections. These findings support the conclusions of [3] and [5], highlighting the pervasive use of undocumented SDKs in free Android apps, particularly in African contexts.

E. Experiences with Data Breaches and Fraud

The survey findings indicated that approximately 31% of respondents reported experiencing some form of digital fraud linked to mobile application usage. Specific types of incidents included unauthorized access to social media accounts (45%), phishing messages containing personal information (35%), unexpected deductions from mobile wallets (30%), cloned WhatsApp lines (25%), and unsolicited loan messages (20%).

Interviews revealed that users frequently attribute these incidents to network failures rather than vulnerabilities in the applications themselves. This misconception limits the adoption of proactive security measures and increases ongoing susceptibility to fraud.

These observations align with the findings of [8], who reported high levels of mobile-related fraud in Nigeria, often linked to user profiling and data harvesting practices. The results underscore the need for greater user awareness regarding application security risks and the implementation of preventive strategies to mitigate exposure to digital fraud as shown in Figure 4 below.

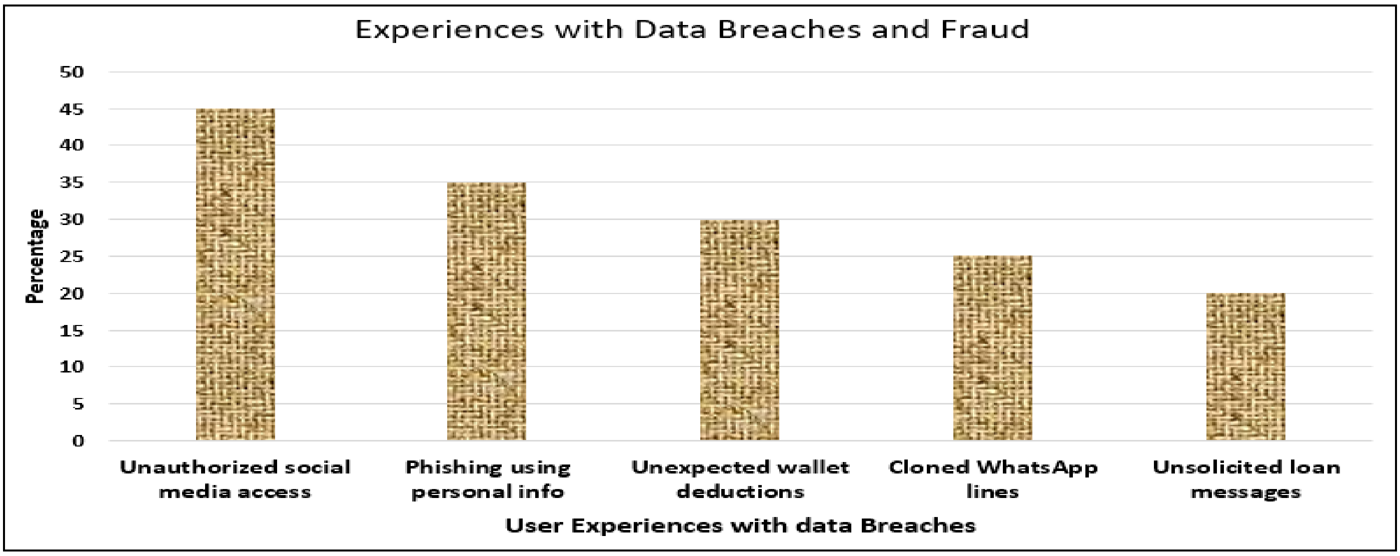

Fig 4 Experience with Data Breaches and Fraud

F. Digital Literacy and User Practices

Digital literacy among residents was uneven and generally low, particularly among traders, artisans, and older adults. Observed practices included:

- Limited ability to configure privacy settings
- Neglecting to review app permissions
- Unawareness of app data storage practices
- Inability to identify malicious or cloned applications

Direct observations also showed that users rarely updated their apps or Android operating system, increasing their vulnerability to security threats. These findings align with [11], who link low adoption of privacy-preserving technologies in Nigeria to inadequate digital literacy.

V. DISCUSSION

The findings of this study provide a comprehensive picture of Android app usage, privacy awareness, permission behaviors, and exposure to data exploitation among residents of Birnin Kebbi. The results indicate that free Android applications are deeply embedded in daily routines, with 92% of respondents reporting daily use. Social media and entertainment apps dominate usage patterns, highlighting their central role in both communication and leisure activities. This widespread adoption reflects the affordability and accessibility of free apps but simultaneously underscores the heightened exposure of users to data collection practices, consistent with prior studies in low-income and digitally emerging communities [19].

Despite the pervasive use of apps, privacy awareness remains low. Only 27% of respondents demonstrated basic understanding of app data collection practices, and a mere 12% were aware of the Nigeria Data Protection Regulation (NDPR). This deficit in digital literacy contributes to uninformed consent, with users habitually granting permissions without consideration of the implications. The study further revealed that 68% of respondents routinely grant all requested permissions, often approving access to sensitive information such as contacts, camera, microphone, location, storage, and SMS logs. Such behavior, reinforced by concerns about app functionality, reflects user-permission fatigue [4] and substantially increases vulnerability to profiling, surveillance, and other forms of data exploitation.

The investigation also highlighted the prevalence of third-party trackers and embedded SDKs in free applications. Many users were unaware that data collected by these SDKs is frequently transmitted to foreign servers, potentially circumventing local privacy protections. Combined with low digital literacy and misattribution of security incidents to network failures, these factors leave users highly exposed to data breaches, fraud, and other cyber risks. Approximately 31% of respondents reported experiencing digital fraud, including unauthorized access to social media accounts, phishing, unexpected mobile wallet deductions, cloned accounts, and unsolicited loan messages, reinforcing concerns about the tangible consequences of poor privacy practices [8].

Furthermore, observed practices such as neglecting app updates, failing to configure privacy settings, and inability to identify malicious applications underscore the interconnectedness of digital literacy and security behavior. Residents' limited knowledge about app permissions, data storage, and potential risks reflects broader challenges in cultivating privacy-conscious behaviors in contexts where technology adoption outpaces digital education [7,11].

Overall, these findings suggest a cyclical relationship in which high dependence on free applications, low privacy awareness, and limited digital literacy mutually reinforce user vulnerability. This situation calls for targeted interventions, including awareness campaigns, user education on permission management, and the promotion of privacy-preserving practices, to mitigate risks associated with mobile app usage in Birnin Kebbi. In addition, app developers and policymakers should consider incorporating privacy-by-design principles and ensuring NDPR compliance to protect users effectively.

VI. CONCLUSION

This study explored free Android application usage, privacy awareness, permission-granting behavior, and exposure to data exploitation among residents of Birnin Kebbi. The findings reveal that free apps, particularly social media and entertainment platforms, are deeply integrated into daily routines, with most users prioritizing convenience and cost savings over privacy considerations. Despite high usage, digital literacy and awareness of data protection practices remain low, with only a small fraction of users understanding app data collection processes or the Nigeria Data Protection Regulation (NDPR).

The study also highlighted a prevalent pattern of user-permission fatigue, with many respondents granting extensive access to sensitive information without understanding the implications. This behavior, coupled with the widespread presence of third-party trackers and SDKs, significantly increases the risk of profiling, fraud, and other forms of data exploitation. Additionally, observed misconceptions—such as attributing security incidents to network failures rather than app vulnerabilities—limit proactive protective behaviors.

Overall, the findings underscore the urgent need for educational interventions, privacy-aware design, and regulatory enforcement to safeguard user data and enhance digital security practices in Birnin Kebbi.

RECOMMENDATIONS

➢ *The Study Recommends the Followings:*

- Digital Literacy Programs: Implement community-based and online training initiatives to educate users about app permissions, data collection practices, and the risks associated with free Android applications.
- Awareness Campaigns on NDPR Compliance: Conduct targeted awareness campaigns to familiarize users with

the Nigeria Data Protection Regulation (NDPR) and encourage the adoption of privacy-conscious practices.

- Promotion of Privacy-Preserving App Practices: Encourage users to regularly review and configure app permissions, update applications and the Android operating system, and avoid granting unnecessary access to sensitive information.
- Integration of Privacy-by-Design in App Development: App developers should embed privacy-preserving features by default, minimize data collection, and provide transparent information on how user data is processed, including third-party SDK usage.
- Monitoring and Reporting Mechanisms for Digital Fraud: Establish accessible channels for reporting digital fraud and provide guidance on identifying suspicious apps, phishing attempts, and other threats to enhance proactive user protection.

REFERENCES

[1]. Gamba, J.; Smith, R.; Zhou, L. Data collection practices in pre-installed and system-level Android apps. IMDEA Networks Digital Repository. Available online: https://dspace.networks.imdea.org (accessed on 24 October).

[2]. Olufemi, T.; Olatunde, S. Free mobile applications and privacy risks in Nigeria. Nigerian Journal of Information Technology 2021, 12, 12-27.

[3]. Ren, J.; Wu, Y.; Li, H.; Chen, K. Third-party libraries in mobile applications: A privacy perspective. IEEE Transactions on Mobile Computing 2016, 15, 1895-1907.

[4]. Zang, J.; Dummit, K.; Graves, J.; McGee, M. Who knows what about me? A survey of behind-the-scenes personal data sharing to third parties by mobile apps. Technology Science Journal 2015, 12, 33-46.

[5]. Ezeh, C.; Obi, M. Third-party SDKs and mobile privacy in African apps. Journal of Cybersecurity in Africa 2021, 3, 55-70.

[6]. Pet, S. Privacy-related SDK defaults in Android applications. Proceedings of the Privacy Enhancing Technologies Symposium. Available online: https://petsymposium.org (accessed on 24 October).

[7]. Abdulhamid, S.; Bello, A.; Okoye, P. Digital literacy and mobile privacy awareness among Nigerian smartphone users. Journal of Information Privacy, 8(2), 45–61 2022, 8, 45-61.

[8]. Adegoke, T.; Aluko, F. User profiling and behavioral tracking risks in mobile applications: Evidence from Nigeria. African Journal of Computing & ICT 2022, 15, 23-36.

[9]. Chika, C.; Tochukwu, O. Assessment of NDPR compliance and enforcement in Nigerian mobile apps. RSIS International Journal 2020, 4, 377-382.

[10]. Narayanan, A.; Bonawitz, K.; Wood, A. Privacy-preserving frameworks for mobile and web applications. IEEE Transactions on Privacy and Security 2020, 18, 1-15.

[11]. Okeke, J.; Uche, N. Adoption of privacy-preserving technologies in Nigerian app development. Journal of ICT Policy in Africa 2023, 7, 33-48.

[12]. Lyons, M.; Zhao, T.; Reardon, J. Measuring sensitive data logging in Android ecosystems. Federal Trade Commission Report. . Available online: https://www.ftc.gov (accessed on 24 October).

[13]. Wikipedia. Cross-device tracking. Available online: https://en.wikipedia.org/wiki/Cross-device_tracking (accessed on 24 October).

[14]. Adeoye, A.; Balogun, M.; Ojo, T. Nigeria Data Protection Regulation: Challenges and enforcement gaps. International Journal of Law and Cybersecurity 2020, 6, 12-29.

[15]. Asere, O.G.F.; Bello, T.; Ibrahim, S. Organizational compliance with NDPR in Nigeria: Evidence from SMEs and public institutions TechScience Journal of ICT Policy 2025, 7, 22-39.

[16]. NDPA. Nigeria Data Protection Act 2023. Thisday Live. Available online: https://www.thisdaylive.com (accessed on 24 October).

[17]. Thisdaylive. Nigeria Data Protection Act: Challenges and regulatory capacity. Available online: https://www.thisdaylive.com (accessed on 24 October).

[18]. Zenodo. Digital literacy and mobile app privacy awareness in Nigeria. Available online: https://zenodo.org (accessed on 24 November).

[19]. Binns, R.; Lyngs, U.; Van-Kleek, M.; Zhao, J.; Libert, T.; Shadbolt, N. Third party tracking in the mobile ecosystem. Available online: https://arxiv.org/abs/1804.03603 (accessed on 24 October).