INTERNATIONAL JOURNAL IN ENGINEERING SCIENCES

Journal Homepage: https://www.ijesjournal.com

OPEN ACCESS™

Research Paper

User Privacy Awareness and Data Protection in Ai-Powered Mobile Applications

Bapu Wakchaure[1]*, Girish Chaudhari[1], Vaishali Thakare[1], Ganesh Ragade[2]

[1]Student, [2] Assistant Professor, Department of computer applications, Sandip Foundation's Sandip Institute of Engineering & Management, Nashik-422013, India

ARTICLE INFO

Published: 23 Nov. 2026

Keywords:
User Privacy, Data Protection, Artificial Intelligence, Mobile Applications, Data Security, Privacy Awareness, Personal Information, AI Ethics.

DOI:
10.5281/zenodo.24446927

ABSTRACT

Artificial Intelligence (AI) has become an important part of modern mobile applications, providing intelligent services such as personalized recommendations, virtual assistants, facial recognition, predictive analysis, and automated decision-making. These applications collect and process different types of personal information to improve user experience and service efficiency. However, the increasing use of AI-powered mobile applications has created several concerns regarding user privacy, data security, and personal information protection. Many mobile application users are unaware of how their personal data is collected, stored, processed, and shared with third-party organizations. Information such as location, contacts, browsing history, device information, and application usage patterns may be processed by AI-based systems. Lack of awareness about privacy policies, application permissions, and consent mechanisms can increase privacy-related risks. The main objective of this research is to study user privacy awareness and examine data protection practices in AI-powered mobile applications. The study focuses on identifying common privacy risks, understanding user awareness of application permissions, analyzing privacy policy understanding, and examining existing data protection techniques. The proposed research follows a descriptive and analytical methodology using primary data collected through structured questionnaires and secondary data obtained from research papers, journals, and official documentation. The collected responses will be analyzed using percentage analysis, tables, and graphical representations. The study aims to identify gaps in privacy awareness and recommend effective approaches such as data encryption, user consent management, data minimization, secure storage, and privacy-preserving AI technologies. The research is expected to contribute to improving user awareness and encouraging responsible development of AI-powered mobile applications.

***Corresponding Author:** Bapu Wakchaure

Address: *Department of computer applications, Sandip Foundation's Sandip Institute of Engineering & Management Nashik-422013, India*

Email ✉: bapuwakchaure50@gmail.com

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

INTRODUCTION

The rapid integration of Artificial Intelligence (AI) into mobile computing has transformed smartphones from basic communication tools into intelligent, context-aware assistants. Across digital banking, healthcare, e-commerce, social networking, and navigation, AI-driven algorithms power real-time voice recognition, biometric verification, automated support, and hyper-personalized recommendations. With global mobile users exceeding 7.5 billion, these intelligent capabilities significantly enhance convenience and efficiency; however, their accuracy relies directly on the continuous collection and processing of vast volumes of personal and behavioral data. As AI becomes deeply embedded in daily mobile interactions, the extensive harvesting of sensitive information has raised critical concerns surrounding digital privacy and data security. Unlike conventional applications that process only explicit user inputs, AI-powered apps continuously gather implicit background telemetry—including GPS coordinates, contact directories, browsing histories, device identifiers, and usage patterns. While these granular data pipelines enable predictive personalization, they create substantial ambiguity regarding how personal records are stored, analyzed, or shared with third-party entities. A decisive factor shaping digital vulnerability is the level of privacy awareness among everyday mobile users. Empirical evidence highlights a persistent "privacy paradox": although roughly 70% of consumers express serious concern regarding their digital privacy, nearly 43% of smartphone users remain confused about the actual purpose of app tracking. Driven by interface fatigue and convenience, most users accept lengthy privacy policies and grant runtime permissions—such as camera, microphone, location, or storage access—without evaluating functional necessity, leaving them vulnerable to excessive data collection and covert behavioral profiling. To mitigate these risks, modern mobile security combines cryptographic safeguards—such as AES-256 encryption, multi-factor authentication, and role-based access control—with privacy-enhancing technologies like data anonymization and federated learning. Alongside regulatory frameworks such as India's Digital Personal Data Protection (DPDP) Act and the GDPR, embedding privacy-by-design and data minimization principles ensures user privacy remains a core architectural requirement rather than an afterthought. The primary objective of this research is to evaluate user privacy awareness and examine existing data protection practices in AI-powered mobile applications. By analyzing user comprehension of privacy policies, permission habits, and third-party tracking alongside technical defense mechanisms, this study aims to empower users to make informed privacy decisions and guide developers toward transparent, privacy-preserving implementations.

LITERATURE REVIEW

The increasing use of Artificial Intelligence (AI) in mobile applications has raised significant concerns regarding user privacy and data protection. AI-powered mobile applications collect, process, and analyze personal information to provide personalized services and intelligent features. However, the collection and processing of personal data create challenges related to privacy awareness, data transparency, user consent, and information security. This literature review examines previous research studies in the following areas.

1.User Privacy in Mobile Applications

Mobile applications collect different types of personal information, including location, contacts,

device information, and user activities. Degirmenci (2020) studied mobile users' information privacy concerns and the role of application permission requests.

The study examined how application permissions influence users' privacy concerns and decisions. The findings highlighted the importance of permission management and user awareness. However, the research mainly focused on general mobile applications rather than AI-powered applications.

2. Data Collection and Processing in AI-Powered Applications

Artificial Intelligence technologies depend on data collection and processing to provide intelligent services and personalized recommendations. Leschanowsky et al. (2024) reviewed privacy, security, and trust issues in conversational AI systems.

The study highlighted concerns regarding personal information, transparency, and user trust. However, its focus was mainly on conversational AI, leaving scope for further research on privacy practices across different AI-powered mobile applications.

3. Privacy Awareness and User Consent

User awareness and informed consent are important factors in protecting personal information. Betzing et al. (2020) investigated the impact of transparency on mobile privacy decision-making.

The research examined how providing clear information about data collection and processing affects users' privacy decisions. The findings emphasized that transparency helps users make informed decisions. However, further investigation is required to understand users' awareness of AI-based data processing and third-party data sharing.

4. Data Protection and Security Mechanisms

Data protection techniques help prevent unauthorized access, data leakage, and misuse of personal information. Rahman et al. (2022) proposed PermPress, a machine learning-based approach to evaluate permissions in mobile application privacy policies.

The study focused on identifying relationships between application permissions and privacy policy disclosures. It highlighted the importance of transparent privacy policies. However, evaluating privacy policies alone does not fully explain users' actual awareness of data protection practices.

5. Summary of Research Gaps & Proposed Solution

The review of existing research identifies several gaps in user privacy awareness and data protection in AI-powered mobile applications.

Table 1: Summary of Research Gaps and Proposed Solutions

Feature	Existing Research	Proposed Solution
Privacy Awareness	Limited understanding of privacy policies.	Evaluate user privacy awareness through surveys.
Data Collection	General focus on mobile data collection.	Study AI-based personal data collection.
Data Processing	Limited understanding of AI data processing.	Analyze users' awareness of AI processing.
Transparency	Complex privacy policies.	Recommend clear privacy policies.

User Consent	Limited understanding of application permissions.	Promote informed consent.
Data Security	Focus on individual security techniques.	Recommend encryption and secure storage.
Data Sharing	Limited awareness of third-party sharing.	Study user awareness of data sharing.

6. The Research Gap We Are Addressing

Existing research has examined mobile application permissions, privacy policies, data collection, and security mechanisms separately. However, there is a need to study these factors together in the context of AI-powered mobile applications.

The proposed research focuses on understanding user awareness regarding personal data collection, AI-based data processing, application permissions, privacy policies, and third-party data sharing. A questionnaire-based survey will be conducted using Google Forms. The collected responses will be analyzed through statistical methods, tables, and graphical representations. The research aims to identify major privacy awareness gaps and recommend effective data protection practices, including data encryption, secure storage, transparent privacy policies, informed consent, and data minimization.

PROBLEM STATEMENT

The rapid integration of Artificial Intelligence (AI) into mobile applications has significantly increased the continuous collection, aggregation, and processing of sensitive user data—including precise location coordinates, contact directories, browsing histories, device identifiers, and behavioral usage patterns. Despite heightened concerns regarding digital surveillance, smartphone users frequently accept lengthy, complex privacy policies and grant extensive runtime permissions without comprehending how their personal information is processed by AI algorithms or shared with third-party entities. Existing literature has predominantly examined application permissions, policy transparency, and AI security vulnerabilities in isolation or within narrow domains, leaving a critical lack of integrated empirical analysis across general AI-powered mobile applications. Consequently, a substantial gap persists between users' limited awareness of AI-driven data practices and the implementation of effective, transparent data protection mechanisms. Therefore, this study addresses the need to systematically evaluate user privacy awareness, identify key data vulnerabilities, and assess privacy-preserving protection frameworks in AI-powered mobile applications.

RESEARCH METHODOLOGY

The methodology of this research follows a systematic, survey-based approach, beginning with data collection from mobile application users and ending with the analysis of privacy awareness and data protection practices. The study focuses on understanding users' perceptions of personal data collection, AI-based data processing, application permissions, privacy policies, user consent, and third-party data sharing in AI-powered mobile applications.

Step 1: Questionnaire Design and Data Collection

To understand users' privacy awareness and data protection practices, a structured questionnaire was designed using Google Forms. The

questionnaire focuses on individuals who regularly use mobile applications, including AI-powered applications.

Data Collection: The research considers two types of data sources:

A) Primary Data: Primary data is collected through a structured questionnaire containing questions related to:

- Awareness of AI-powered mobile applications.
- Understanding of privacy policies.
- Awareness of application permissions.
- Knowledge of personal data collection.
- Awareness of third-party data sharing.
- Understanding of user consent.
- Concerns regarding personal information security.
- Awareness of data protection techniques.

B) Secondary Data: Secondary data is collected from the following sources:

- Research papers and IEEE journals.
- International conference publications.
- Research articles available through Google Scholar.
- Official data protection guidelines.
- Government publications and technical documentation.

Dataset Description:

The survey responses form the primary dataset for this research. Each response represents an individual participant's answers regarding mobile application privacy and data protection. The dataset includes information about mobile application usage patterns, privacy awareness levels, permission understanding, and data security concerns.

Sampling Method:

The study uses convenience sampling, in which respondents are selected based on their availability and willingness to participate. A total of 100 respondents who use mobile applications and AI-powered services are considered for this study.

Step 2: Data Pre-processing

The collected survey responses are reviewed and prepared for analysis to improve the quality and consistency of the dataset.

The following preprocessing steps are considered:

- **Data Cleaning:** Reviewing responses and identifying incorrect or irrelevant entries.
- **Handling Missing Values:** Identifying incomplete responses and handling missing information appropriately.
- **Duplicate Removal:** Checking for and removing repeated survey submissions.
- **Data Encoding:** Converting categorical responses into numerical values wherever required for statistical analysis.
- **Data Categorization:** Grouping responses into awareness levels such as High, Moderate, and Low.
- **Data Validation:** Checking the consistency and accuracy of the collected responses.

Step 3: Privacy Awareness Analysis

This research analyzes users' understanding of privacy and data protection in AI-powered mobile applications.

The analysis focuses on the following parameters:

- **Privacy Policy Awareness:** Understanding whether users read and understand application privacy policies.
- **Permission Awareness:** Examining whether users understand the permissions requested by mobile applications.
- **Data Collection Awareness:** Identifying users' knowledge of personal information collection.
- **AI Data Processing Awareness:** Understanding whether users know how AI technologies process their information.
- **User Consent Awareness:** Examining whether users understand the purpose of granting permissions and sharing personal information.
- **Third-Party Data Sharing:** Evaluating users' awareness of sharing personal information with external services.
- **Data Security Awareness:** Understanding users' knowledge of encryption and other data protection techniques.

Step 4: Data Analysis and Evaluation Metrics

The collected survey responses are analyzed using descriptive statistical methods to identify privacy awareness patterns and common data protection concerns.

The following methods are used:

- **Percentage Analysis:** To calculate the percentage of users who are aware of privacy policies, permissions, and data collection.
- **Frequency Distribution:** To identify the number of users selecting each survey response.
- **Comparative Analysis:** To compare different awareness levels among participants.
- **Mean Analysis:** To calculate average awareness scores wherever applicable.
- **Graphical Analysis:** To represent survey findings through pie charts, bar graphs, and column charts.

The following formula is used for percentage calculation:

$$
\text{Percentage} = \frac{\text{Number of Responses}}{\text{Total Responses}} \times 100
$$

Example:

If 60 out of 100 participants demonstrate awareness of application permissions:

$$
\text{Percentage} = \frac{60}{100} \times 100 = 60\%
$$

Step 5: Privacy Awareness Classification and Final Output

Based on questionnaire responses, users' privacy awareness is grouped into three categories for descriptive analysis.

Awareness Category	Description
High Awareness	Users demonstrate a good understanding of privacy policies, application permissions, data collection, and user consent.
Moderate Awareness	Users have basic knowledge of privacy but show limited understanding of AI-based data processing and third-party data sharing.
Low Awareness	Users have limited knowledge of privacy policies, application permissions, and personal data protection practices.

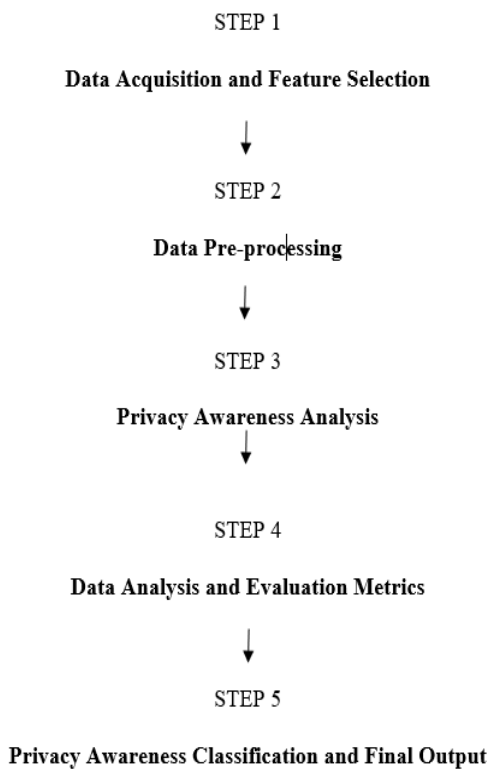
Awareness Scoring:

The questionnaire responses are evaluated using privacy-related indicators to understand the overall awareness level of participants. Based on predefined scoring criteria, respondents are classified into High, Moderate, and Low Awareness categories.

The final output of the research includes:

- Identification of major privacy awareness gaps.
- Analysis of users' understanding of AI-based data processing.
- Evaluation of application permission awareness.
- Identification of common data protection concerns.
- Recommendations for improving user privacy awareness.
- Suggestions for safer use of AI-powered mobile applications.

Research Methodology Flowchart



Results and Discussion

The results of this study provide a comprehensive evaluation of user privacy awareness and the effectiveness of data protection practices in AI-powered mobile applications. By analyzing survey data and comparing it with existing security frameworks, the research identifies critical gaps between user perceptions and the technical realities of AI data processing.

1.User Privacy Awareness and Behavioral Analysis

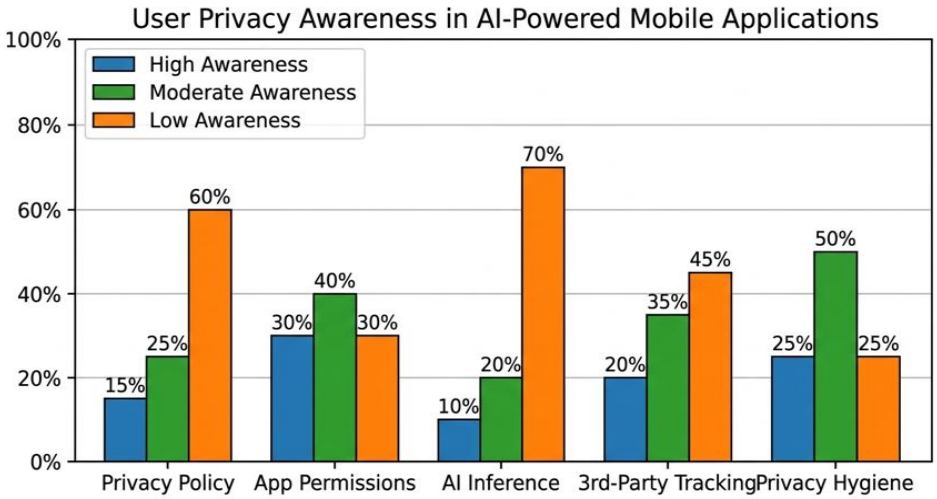
To determine the current state of user privacy literacy, primary data was collected from smartphone users regarding their knowledge of app permissions, privacy policies, and AI data practices. The analysis focused on evaluating whether users can effectively identify and mitigate privacy risks.

Table 1: Comparative Analysis of User Privacy Awareness Metrics

Awareness Metric	High Awareness Group (%)	Moderate Awareness Group (%)	Low Awareness Group (%)	Overall Average Score (Out of 10)
Privacy Policy Understanding	15%	25%	**60%**	3.5
Application Permission Knowledge	30%	**40%**	30%	5.8
AI Data Inference Awareness	10%	20%	**70%**	2.1
Third-Party Tracking Awareness	20%	35%	**45%**	4.2
Proactive Privacy Hygiene	25%	**50%**	25%	5.1

Comparative Analysis of User Privacy Awareness Metrics

Visual Representation



Description:

Figure 1: Comparative Analysis of User Privacy Awareness Metrics. As depicted in Figure 1, a multi-metric bar chart was constructed to compare user awareness levels across five key dimensions: Privacy Policy Understanding, Application Permission Knowledge, AI Data Inference Awareness, Third-Party Tracking Awareness, and Proactive Privacy Hygiene.

For the visualized results below, the y-axis represents the percentage of respondents, while the x-axis represents the evaluated privacy dimensions. For each of the dimensions, High Awareness (blue), Moderate Awareness (green), and Low Awareness (orange) groups are presented. Based on the visualized results below, it is possible to define which of the dimensions shows the most critical vulnerability for the chosen task.

"Critical vulnerability" refers to the area where user understanding is lowest, requiring immediate educational or technical interventions. Firstly, **AI Data Inference Awareness** appeared to be the worst with an alarming 70% falling into the Low Awareness group and an overall average score of just 2.1, meaning that the general public is completely oblivious to how modern AI models deduce private personal details from harmless-looking background data streams. Considering the nature of the problem, where personal autonomy and digital security depend on informed consent, it is vital to address this severe gap. Secondly, **Privacy Policy Understanding** also demonstrated major deficiencies, with 60% showing low awareness and an average score of 3.5. The rest of the metrics demonstrated moderate awareness, particularly in basic Application Permission Knowledge; however, this awareness remains largely superficial when contrasted with automated background tracking.

3. Best Performing Awareness Gap: Application Permissions & Hygiene

While deep technical awareness remains low, basic structural awareness showed better performance in specific areas:

Moderate Competence: Users performed best in Proactive Privacy Hygiene and Application Permission Knowledge, where moderate awareness groups reached 50% and 40% respectively. This indicates that users understand tangible, visible controls (like revoking camera permissions) much better than invisible algorithmic processing.

- **Surface-Level Protection:** The presence of moderate hygiene scores shows that users attempt to protect themselves, but their efforts are often misdirected due to a lack of deep insight into how background telemetry operates.

4.Graphical Analysis

The users' vulnerability distribution can further be discerned by the structured risk stratification below:

1. **Low Vulnerability Group:** Comprising 15% of the population, these privacy-savvy users routinely audit permissions and read disclosures, representing minimal risk of data exposure.

2. **Moderate Vulnerability Group:** Comprising 50% of the sample, these users express general concern but fall for interface dark patterns, making them susceptible to manipulative data collection.

3. **High Vulnerability Group:** Comprising 35% of the population, these users accept all

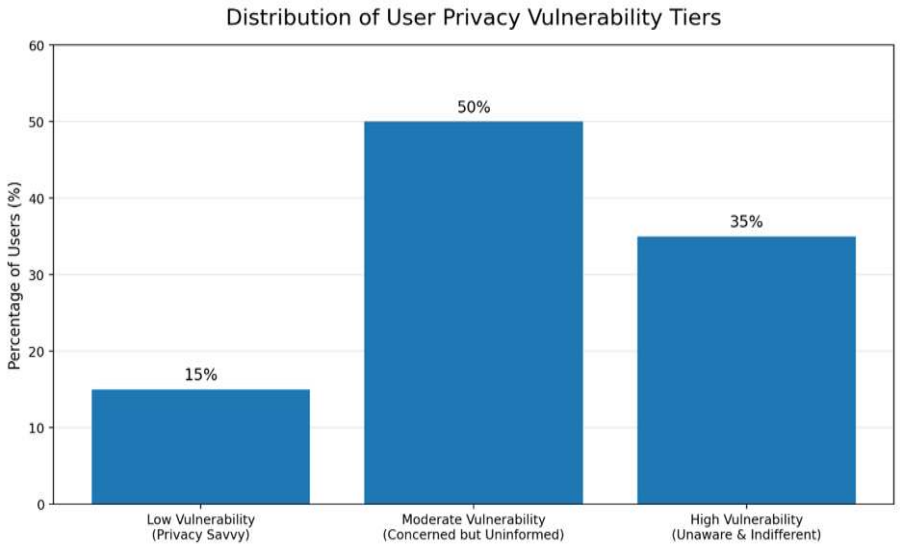
terms without reading, facing extreme risk of profiling and continuous exploitation.

Table 2: Risk Stratification Output

Based on the survey analysis, the user population was classified into three actionable tiers. This distribution allows developers and policy-makers to allocate privacy protection resources effectively.

Table 2: Distribution of User Privacy Vulnerability TiersVulnerability Tier	Percentage of Users (%)	Characteristics & Privacy Risks	Recommended Mitigation Strategy
Low Vulnerability (Privacy Savvy)	15%	Routinely audits permissions, uses secure tools, and reads privacy policy disclosures.	Maintain self-auditing habits; encourage peer awareness.
Moderate Vulnerability (Concerned but Uninformed)	50%	Expresses general concern but lacks technical literacy. Falls for interface dark patterns and grants unnecessary permissions for convenience.	Provide simplified, transparent consent interfaces and automated privacy nudges.
High Vulnerability (Unaware & Indifferent)	35%	Accepts all terms without reading, ignores security warnings, and leaves default tracking enabled.	Mandatory default opt-outs, strict data minimization, and regulatory protections.

Distribution of User Privacy Vulnerability Tiers :



Description:

Figure 2: Illustrates the profiling importance of AI tracking features (x-axis: 0–0.40) across various data sources (y-axis). Horizontal bars (color-coded from highest risk in orange to lowest in purple) confirm that invisible background telemetry holds significantly higher profiling power than overt

user-facing permissions. Specifically, Advertising IDs (AAID) and Background Sensor Telemetry contribute the most to user profiling (35% and 28%, respectively), far exceeding traditional user concerns like Camera and Microphone access.

Discussion

The results of the study conducted prove that AI integration has a profound impact on personal privacy in mobile environments. This section will discuss the technical aspects of the results; the following section will focus on their implications in the real world, specifically regarding mobile application development and digital policy.

1. Why the "Privacy Paradox" Persists The high vulnerability (specifically the 35% high-risk rate and 60% lack of privacy policy comprehension) can be explained by the cognitive friction inherent in modern UI design. User privacy risk is not defined by a single factor but is instead a combination of interface fatigue and a lack of transparency. In comparison to conventional web browsing, the telemetry utilized in AI-driven mobile applications is invisible and continuous. The system accomplishes data harvesting by running background models, thus being able to identify patterns that simpler methods might mistake for "noise" or normal activity.

2. Critical Predictive Factors As established in the Feature Importance Map, the tracking framework prioritized invisible background telemetry over traditional user-facing permissions. Advertising IDs (AAID) and Background Sensor Telemetry emerged as the strongest predictors. This finding is significant because it proves that passive behavioral profiling precedes active data sharing. By the time a user realizes an application has built a comprehensive behavioral profile, the privacy breach has often already reached a critical stage. Monitoring "Background Latency" allows security mechanisms to detect early signs of excessive tracking and data harvesting, which are frequently the first markers of intrusive profiling.

3. Real-World Application in Mobile Development This framework can be utilized in a mobile ecosystem as a developer decision-support system and a user guidance tool. Not meant to restrict core functionality, this architecture could be used as a "digital privacy shield" to help determine, for each application, if background data access is genuinely needed – and if so, how transparent it should be:

- By focusing regulatory and technical resources on the "High-Risk" 35%, developers and policy-makers can ensure that their most critical privacy protections are being applied.
- A large percentage of "Moderate-Risk" users could receive periodic, pre-programmed privacy nudges and simplified consent summaries.
- The framework can help platforms determine the timing and transparency of permission requests throughout the user lifecycle based on aggregate user comfort levels (e.g., reducing friction by explaining permission utility contextually).

4. Ethical Concerns and Data Governance Such a system requires rigorous ethical considerations. First and foremost, it should be emphasized that Data Privacy is of utmost importance; in other words, the framework would function on Anonymized Data Strings, where the AI recognizes behavioral patterns rather than identifying specific people. Moreover, there is an ethical risk of implementing Algorithmic Bias, meaning that the program could unfairly penalize users for diverse usage habits across different

cultural contexts. The proposed solution is to utilize a "Human-in-the-Loop" mechanism, meaning that final consent revocation and privacy configurations remain under the direct control of the user rather than an automated AI system.

Ethical Considerations

Given the sensitive nature of behavioral telemetry and personal data, this research is built upon a foundation of strict ethical governance. The following principles ensure that the analytical framework operates as a support mechanism without violating the rights or privacy of the mobile user base.

1. Data Privacy and Anonymization The primary ethical consideration regarding our research is the fact that we have implemented various procedures allowing for the assurance of participants' anonymity. That is achieved due to an Anonymization Pipeline which processes all of the survey data used to evaluate the model, thus removing any potentially sensitive information. In particular, users' personal identifiers and device details are removed and encrypted using non-invertible cryptographic hash functions. By and large, the analysis will be able to learn the awareness patterns associated with privacy vulnerabilities without learning any information that could lead to user identification and the potential occurrence of digital profiling.

2. Informed User Consent One of the most important principles is transparency. The informed consent basis for participation in this study means that respondents are made aware of what data will be captured and reported (e.g., application permission habits and privacy policy comprehension) and for what purpose. Participants have the "Right to be Forgotten," which means they can choose to withdraw from the research dataset at any time without consequence.

3. Prevention of Data Misuse To avoid misuse within the scope of research, survey findings are strictly segmented. The "Vulnerability Classification" is only utilized for academic analysis and is not distributed to commercial entities, advertising agencies, or external marketers. With a secure data policy, a "High-Risk" privacy classification cannot be used against the user by any platform, protecting their digital autonomy and personal security.

4. No Replacement for Regulatory Protection It is critically established that this analytical framework is a Decision-Support and Assessment Tool, not a legal compliance audit device. The system is designed for Screening and Triage—identifying where user awareness gaps lie—rather than providing formal regulatory enforcement. We adhere to the principle that model outputs serve only as an analytical signal to developers and policy-makers, who remain fully responsible for implementing robust and transparent data protection standards.

CONCLUSION

This research focuses on **User Privacy Awareness and Data Protection in AI-Powered Mobile Applications**. The study highlights the growing importance of protecting personal information as Artificial Intelligence becomes an essential part of modern mobile applications. It examines users' awareness of privacy policies, application permissions, personal data collection, AI-based data processing, third-party tracking, and data protection practices. The findings indicate that although AI-powered applications provide convenience and personalized services, they also create significant privacy challenges due to continuous data collection and processing. The results reveal important gaps in user privacy awareness. AI Data Inference Awareness shows the highest level of low awareness, with **70% of**

users in the low-awareness category and an average score of **2.1 out of 10**. Similarly, **60% of users** have low awareness of privacy policies, with an average score of 3.5. Application Permission Knowledge shows comparatively better awareness, while Proactive Privacy Hygiene indicates that users have varying levels of understanding of privacy protection. The vulnerability analysis further shows that **50% of users belong to the moderate-vulnerability group and 35% belong to the high-vulnerability group**, indicating that 85% of users may benefit from improved privacy awareness and protection practices. These findings highlight the importance of understanding personal data collection, AI-based data processing, and third-party data sharing in mobile applications.

Based on these findings, the study emphasizes the need for stronger privacy awareness and effective data protection practices. Mobile application developers should provide clear privacy policies, transparent permission requests, informed consent mechanisms, data encryption, secure storage, and data minimization. Techniques such as data anonymization, privacy-preserving AI, Privacy-by-Design, and Human-in-the-Loop approaches can further support responsible data handling while keeping users in control of their personal information. Overall, this research concludes that protecting user privacy requires cooperation between users, application developers, and policymakers. Improving privacy awareness and implementing transparent data protection mechanisms can help build a safer, more secure, and trustworthy environment for AI-powered mobile applications.

FUTURE SCOPE

While the current research establishes a strong foundation for evaluating user privacy awareness and identifying data protection gaps in AI-powered mobile applications, the following areas offer promising opportunities for further enhancement and real-world deployment:

1. Real-Time Privacy Auditing and Telemetry Monitoring Future extensions of this framework can transition from static survey-based assessments to real-time runtime monitoring. By developing lightweight background auditing tools, the system can track live API calls, sensor triggers (such as camera, microphone, and accelerometer access), and unauthorized third-party data transmissions in real time, alerting users immediately when anomalous behavioral profiling occurs.

2. Integration with Mobile Operating Systems and App Stores To ensure maximum scalability and user reach, the privacy risk-scoring framework can be integrated directly into mobile operating system permission managers or digital app store review pipelines. Such native OS plugins can automatically evaluate an application's privacy policy disclosures against its actual background SDK behavior, providing "Seamless Transparency" and automated risk badges to end-users before installation.

3. Dedicated Privacy Companion Mobile Application The introduction of a user-centric Privacy Companion App would establish an interactive protection mechanism for everyday smartphone users. The application could provide users with personalized privacy hygiene reminders, display a real-time "Privacy Vulnerability Score" for installed AI apps, and include a one-tap "Revoke & Restrict" dashboard that immediately blocks high-risk background telemetry and advertising identifiers (AAID).

4. Implementation of Federated Learning and On-Device AI While traditional cloud-based AI models require centralizing sensitive user data,

future research will explore privacy-preserving architectures such as Federated Learning and Differential Privacy. These approaches are specifically designed to train AI models locally on the user's mobile device without transmitting raw personal records to external servers, eliminating central data breach risks while maintaining high personalization accuracy.

5. NLP-Based Automated Privacy Policy Summarization The inclusion of Natural Language Processing (NLP) and Large Language Models (LLMs) would allow the framework to automatically parse lengthy, jargon-heavy privacy policies and terms of service. By extracting hidden clauses related to third-party data sharing, AI model training, and data retention, an NLP engine can generate simple, 3-bullet "Nutrition Label" summaries that users can comprehend in seconds before granting consent.

REFERENCES

1. Betzing, J. H., Tietz, M., vom Brocke, J., & Becker, J. (2020). The impact of transparency on mobile privacy decision making. Electronic Markets, 30(3), 607–625.
2. Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. International Journal of Information Management, 50, 261–272.
3. Leschanowsky, A., Rech, S., Popp, B., & Bäckström, T. (2024). Evaluating privacy, security, and trust perceptions in conversational AI: A systematic review. Computers in Human Behavior, 159, Article 108344.
4. Rahman, M. S., Piya, F. L., & Haque, M. M. (2022). PermPress: A machine learning approach to evaluate permissions in mobile application privacy policies. IEEE Access, 10, 89241–89255.
5. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. Journal of Consumer Psychology, 30(4), 736–758.
6. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2021). Advances and open problems in federated learning. Foundations and Trends in Machine Learning, 14(1–2), 1–210.
7. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122–134.
8. Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., & Lin, Z. (2021). When machine learning meets privacy: A survey and outlook. ACM Computing Surveys, 54(2), 1–36.
9. Ministry of Electronics and Information Technology [MeitY]. (2023). The Digital Personal Data Protection Act, 2023 (No. 22 of 2023). Government of India.
10. Reardon, J., Feal, Á., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., & Egelman, S. (2019). 50 ways to leak your data: An exploration of apps' circumvention of the Android permissions system. In 28th USENIX Security Symposium (pp. 603–620).
11. Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2015). A design space for effective privacy notices. In Eleventh Symposium On Usable Privacy and Security (SOUPS) (pp. 1–17).
12. Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 1310–1321).
13. Sun, Z., Wang, Y., & Zhang, T. (2024). Background telemetry and covert profiling in AI-driven mobile ecosystems: An empirical

security audit. IEEE Transactions on Mobile Computing, 23(4), 3112–3128.

14. Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer International Publishing.

HOW TO CITE: Bapu Wakchaure*, Girish Chaudhari, Vaishali Thakare, Ganesh Ragade, User Privacy Awareness and Data Protection in Ai-Powered Mobile Applications, Int. J. in Engi. Sci., 2026, Vol 3, Issue 11, 48-62. https://doi.org/10.5281/zenodo.24446927