

Privacy and Security in Mobile Applications Assisted by Artificial Intelligence [†]

Sandra Pérez Arteaga [‡], Ana Lucila Sandoval Orozco [‡] and Luis Javier García Villalba ^{*,‡}

Group of Analysis, Security and Systems (GASS), Department of Software Engineering and Artificial Intelligence (DISIA), Faculty of Computer Science and Engineering, Office 431, Universidad Complutense de Madrid (UCM), Calle Profesor José García Santesmases, 9, Ciudad Universitaria, 28040 Madrid, Spain; sandrp08@ucm.es (S.P.A.); asandoval@fdi.ucm.es (A.L.S.O.)

* Correspondence: javiergv@fdi.ucm.es; Tel.: +34-91-394-7638

[†] Presented at the First Summer School on Artificial Intelligence in Cybersecurity, Cancun, Mexico, 3–7 November 2025.

[‡] These authors contributed equally to this work.

Abstract

The use of technology in mobile devices and the integration of Artificial Intelligence offers a wide range of benefits and personalised services that help users perform countless activities that assist them in their daily lives, such as at work, school, and when communicating with friends and loved ones. However, this technological evolution poses significant challenges and risks in terms of user privacy, as the personal data and information that may be shared or stored must be taken into account in order to preserve the physical and psychological integrity of users. Balancing innovation and privacy is essential to maximise the benefits of AI on mobile devices while protecting the rights and security of users. This requires a comprehensive approach involving multiple stakeholders working together to create a secure, user-centred digital environment and implement security measures to preserve that data security.

Keywords: artificial intelligence; best practices; device security; mobile applications; mobile devices; personal data; privacy; risks; vulnerabilities

1. Introduction

Digital technology has transformed the way goods and services are produced and marketed. The Internet has changed entertainment and communication habits and the way companies interact with users. These changes are generating new consumption patterns, forcing organisations to develop innovative business models or adapt existing ones to respond to customer needs and maintain their growth in the digital age. The use of artificial intelligence (AI) in mobile devices is highly beneficial, as it improves their functionality by integrating advanced technologies, making them smarter, more efficient and significantly faster. This optimises the user experience and turns devices into truly intelligent electronic systems. The most advanced forms of AI also enable mobile devices to recognise user behaviour and understand their needs [1].

The everyday use of information and communication technologies has become an essential tool for improving communication processes and the exchange of information through various means, such as mobile devices, tablets, computers, and other technological equipment connected to the internet. Users employ different types of devices to access the



Academic Editors: Héctor Manuel Pérez Meana and Gabriel Sánchez Pérez

Published: 5 February 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

network, the most common being mobile phones. These devices offer multiple functionalities, allowing users to perform tasks such as keeping in touch with friends and family and completing school or work activities, among many others. Their use ranges from minors to adults. Constant internet connection and daily use of mobile devices, together with applications that incorporate artificial intelligence (AI) to perform various tasks, can generate great benefits for users; however, they also involve risks and threats [2]. Among these is the possible collection and storage of personal and sensitive information within the device itself, which can put the physical and psychological integrity of users at risk. It is therefore essential to pay special attention to the security and privacy of mobile devices, especially when using applications and services based on AI techniques.

Security in AI applications must be a priority in order to protect the information that is stored and shared with the applications, as well as with external users, family members or friends. Users must be informed about the risks involved in sharing sensitive information and have clear control over their personal data, including the ability to access, modify or delete such information as necessary. AI applications must offer clear options for users to manage their privacy preferences. It is important for developers and companies to adopt strict privacy and security practices to ensure user trust and compliance with applicable data protection regulations.

This paper reviews the security and privacy of information shared on mobile devices that use artificial intelligence (AI), describing how they work, the privacy risks faced by users, and the technologies that can help maintain security on such devices.

The rest of the paper is organised as follows: Section 2 details how artificial intelligence (AI) has contributed to mobile devices assisting users in performing various tasks. Section 3 addresses the risks related to user privacy arising from the use of AI in mobile devices. Section 4 describes some technologies that can be implemented in both AI and device architecture to strengthen their security. Finally, Section 5 presents the conclusions of the paper.

2. Artificial Intelligence in Mobile Devices

The growing use of generative artificial intelligence (AI) applications is significantly transforming the digital landscape, offering advanced tools ranging from content creation to service personalisation on mobile devices. However, this expansion also poses significant challenges in terms of data privacy. Generative AI applications often require access to large volumes of personal information to function optimally, including sensitive data stored on mobile devices. This collection of information can compromise user privacy if strict security and transparency measures are not in place. Therefore, developers and regulators must work together to ensure that these applications implement robust data protection practices, minimising the risk of leaks and ensuring that users retain control over the use of their information. While AI significantly improves the functionality of mobile devices, it is essential to verify and cross-check the information obtained through these technologies. It should always be borne in mind that AI is not infallible and can make mistakes; therefore, it is essential to use our judgement and question the information we receive.

3. Risks to User Privacy

With the current boom in AI, new gaps and challenges are also emerging. The most notable of these is the threat of new monopolistic practices in which large companies control the data that can be used to train and improve AI models. In addition to considering the quality of the data used to train models, there is also the issue of data overfitting, where the model is so closely fitted to the training data that it does not generalise well to test data [3].

To preserve data privacy on mobile devices that use applications with artificial intelligence (AI) modules, it is essential to implement practices that help protect personal information and maintain data security. In addition, physical security measures such as data encryption and access control should be implemented to prevent unauthorised access to hardware, as well as the use of antivirus software, strong passwords, regular software and hardware updates, and user education on good IT security practices.

Vulnerabilities in Mobile Environments

The increase in the number of mobile device users has also been accompanied by an increase in vulnerabilities and threats, which can compromise system security, allow unauthorised access to the device, and jeopardise user privacy, as shown in Figure 1.

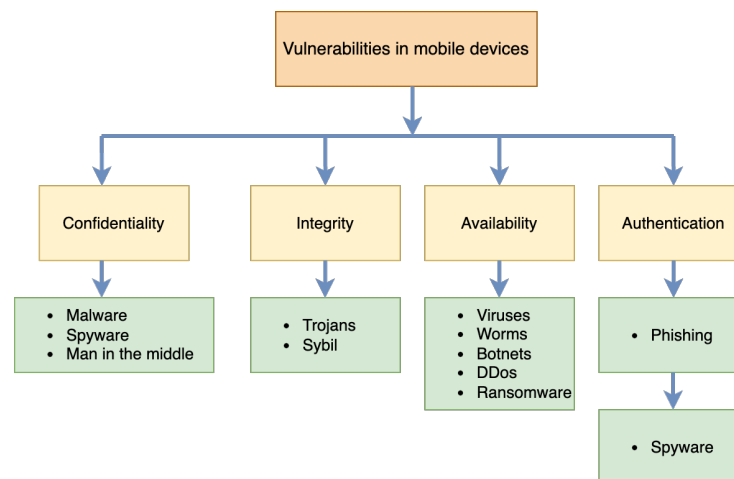


Figure 1. Vulnerabilities in Mobile Devices.

These vulnerabilities can arise from design, implementation, or configuration errors in the software, and can be found in any component of the system, including source code, user interfaces, communication protocols, and security configurations.

4. Emerging Technologies for Privacy

Applications based on artificial intelligence (AI) present particular privacy challenges due to the collection and processing of large volumes of sensitive data. However, new technologies are emerging that help address these challenges and improve privacy in AI applications.

4.1. Federated Learning

Federated learning is a machine learning (ML) approach in which different clients collaborate to train a centralised model, while keeping each client's data decentralised [4].

This approach allows mobile phones to collaboratively participate in training a shared prediction model. Artificial intelligence models are trained in a distributed manner across multiple devices without the data leaving the user's devices. This preserves privacy, as each device keeps its data private and local, preventing sensitive information from being shared with the central server.

4.2. Differential Privacy

This is achieved through various complex techniques involving the use of multiple statistical tools. Essentially, a calculated amount of noise (random data) is added to the database. This makes it difficult to link an individual to their data points; however, when applied in a controlled manner, the data remains accurate enough to be useful in many

situations. Data privacy protection ensures that interested parties cannot determine whether an individual record participated in the learning process. By injecting random noise into the data or model parameters, differential privacy provides statistical privacy guarantees for each record and protects against inference attacks on the model. Due to the inclusion of noise during learning, these systems tend to generate slightly less accurate models.

4.3. Homomorphic Encryption

This technique is used to protect data privacy, allowing users to perform calculations on confidential information without revealing its content. Unlike traditional cryptography, where data must be decrypted in order to perform operations, homomorphic encryption allows calculations to be performed directly on encrypted data. In this way, the data remains protected throughout the calculation process and is only decrypted once the calculations have been completed.

4.4. Architectures for Preserving Data Privacy

The architecture used in mobile devices allows these technologies to be applied and guarantees the security of both the infrastructure and artificial intelligence (AI) services. Testing on the device with pre-trained models offers several advantages when making predictions directly on the device. First, privacy is improved, as data never leaves the device. In addition, no API is required for the application to communicate with the model, avoiding the need to incorporate an element into the architecture that could compromise user data security.

To perform inference on a given image, the application loads the pre-trained model from internal storage and performs the necessary calculations locally on the device. The architecture, Testing and Inference on the Device, is perhaps the most suitable for small-scale data processing, as it preserves user privacy by performing both training and inference on the device, enabling the application to continue learning from data stored directly on the mobile phone.

5. Conclusions

Privacy and security are fundamental aspects of mobile devices and artificial intelligence (AI)-based applications, due to the growing volume of personal data that is processed and stored. While AI offers vast opportunities for innovation and improvement in technological interaction, it also poses risks associated with the exposure of sensitive information and potential vulnerabilities to cyber attacks. The adoption of secure design practices, robust data protection policies, and the use of technologies such as encryption, differential privacy, and federated learning can mitigate these risks, ensuring confidentiality and user control over their information. The integration of these strategies into mobile devices not only protects users' rights, but also maximises the benefits of AI, promoting a more secure, reliable and efficient digital environment. The implementation of these technologies also allows for the establishment of a robust architecture for the secure handling of user information when using mobile devices.

Author Contributions: Conceptualization, S.P.A., A.L.S.O. and L.J.G.V.; methodology, S.P.A., A.L.S.O. and L.J.G.V.; validation, S.P.A., A.L.S.O. and L.J.G.V.; investigation, S.P.A., A.L.S.O. and L.J.G.V. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the European Commission under the Horizon 2020 research and innovation programme, as part of the project HEROES (<https://heroes-fct.eu>, Grant Agreement no. 101021801) and of the project ALUNA (<https://aluna-isf.eu/>, Grant Agreement no. 101084929). This work was also carried out with funding from the Recovery, Transformation and Resilience Plan, financed by the European Union (Next Generation EU), through the Chair "Cybersecurity

for Innovation and Digital Protection” INCIBE-UCM. In addition this work has been supported by Comunidad Autonoma de Madrid, CIRMA-CM Project (TEC-2024/COM-404). The content of this article does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zambrano, A.E.D.; Cedeño, A.N.S.; López, M.C.F.; Cedeño, M.J.E.; Sardi, G.A.S. Theoretical foundation of artificial intelligence in the development of mobile applications at the Admission and Leveling Institute of the Technical University of Manabí (Fundamentación teórica de la inteligencia artificial en el desarrollo de aplicaciones móviles en el Instituto de Admisión y Nivelación de la Universidad Técnica de Manabí). *Tesla Rev. Científica* **2023**, *3*, e223. (In Spanish)
2. Macías García, M.d.C. Artificial intelligence. Safeguarding the safety and health of workers (La inteligencia artificial. Custodia de la seguridad y salud de las personas trabajadoras). *e-Rev. Int. Prot. Soc.* **2023**, *extra 1*, 219–237. (In Spanish)
3. Abarca, J.E.O. Analysis of the experience of Spanish-speaking users of Artificial Intelligence mobile applications (Análisis de la experiencia de usuarios hispanoparlantes de aplicaciones móviles de Inteligencia Artificial). *Economía Creat.* **2023**, *extra 1*, 79–103. (In Spanish)
4. Banabilah, S.; Aloqaily, M.; Alsayed, E.; Malik, N.; Jararweh, Y. Federated learning review: Fundamentals, enabling technologies, and future applications. *Inf. Process. Manag.* **2022**, *59*, 103061. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.