Research on Privacy and Security Protection in Multi-App Human-Computer Interaction Based on User Experience

Xuantong Guo
Institute of Technology, Tianjin University of Finance and Economics, Tianjin, China

Keywords: Multi-Platform Human-Computer Interaction, Privacy and Security Safeguarding, User Experience, Privacy by Design.

Abstract: With the popularization of muti-platform interaction technology, the widespread use of applications has increased the risk of privacy leakage, and user privacy security has become a key issue affecting user experience. This paper, from the user's perspective, systematically analyzes the challenges of privacy security protection in a multi-app environment. By integrating privacy security design principles and technical means of privacy protection in a multi-app situation, this paper proposes a solution centered on user perception optimization, based on full life cycle data protection, and supported by cross-platform collaboration. This paper finds that the adoption of dynamic permission control and privacy computing technology can reduce the risk of leakage while ensuring data value. At the same time, through cross-app data sharing standards (e.g., OAuth 2.0) and unified privacy management interface design, user operation efficiency and trust can be improved. In addition, this paper suggests building a centralized privacy framework to address the risks of intelligent agent authentication and XR environments. This paper provides a systematic path for balancing privacy security and user experience, which is of great practical value for building a sustainable multi-platform interaction ecology.

1 INTRODUCTION

Under the impetus of digitalization, mobile applications permeated social, healthcare, and financial and other fields, fundamentally transforming human lifestyles and work patterns. Social media platforms optimize user social experience through behavioral data analytics, medical detection procedures deliver personalized services by leveraging individual health data, and mobile payment platforms reshape consumption patterns with their unparalleled convenience. However, behind this technological empowerment lies a severe risk of privacy leakage (Smith & Brown, 2021).Statistics reveal that the average number of applications installed by users has reached 31, and cross-app data interaction is frequent. However, due to differences in technical standards and encryption protocols across platforms, the risk of data leakage has increased several times (Bitkom Research, 2023). Relevant reports further indicate that the privacy risk index in 2019 increased by 26.66% compared with 2019, highlighting the escalating trend of privacy threats (China Academy of Information and Communications Technology, 2020).

Although enterprises and developers attempt to enhance technical measures (e.g., advanced encryption algorithms), these strategies often neglect user-centric requirements, resulting in a disconnection between privacy protection and user experience (Nissenbaum, 2010). Therefore, how to strike a balance between user experience and privacy protection has become the core issue of current research.

Currently, the academic community has begun to explore the balance between privacy and experience. For instance, Acquisti et al. revealed the "privacy paradox" phenomenon through behavioral experiments, indicating that although users claim to value privacy, they often voluntarily share sensitive information for convenience (Acquisti, Brandimarte, & Loewenstein, 2015). Zhang et al. proposed optimizing privacy interfaces through visual icons and hierarchical menu designs, which increased privacy protection functions by 40%(Zhang & Liu, 2020). Additionally, research indicates that the heterogeneity of user preferences (e.g., younger users prioritizing efficiency versus elderly users

Guo, X.
Research on Privacy and Security Protection in Multi-App Human-Computer Interaction Based on User Experience.
DOI: 10.5220/0014290700004718

In *Proceedings of the 2nd International Conference on Engineering Management, Information Technology and Intelligence (EMITI 2025)*, pages 10-16
ISBN: 978-989-758-792-4

emphasizing transparency) makes it difficult for universal privacy policies to fit all, but the complexity of privacy policies increases users' cognitive burden (Wang et al., 2021) (McDonald & Cranor, 2008). Existing achievements demonstrate that a single technical or design perspective is difficult to address systemic contradictions, and there is an urgent need to construct an integrated framework that conforms to user needs, technical guarantees, and platform collaboration.

This paper aims to propose a user-centered multi-platform privacy protection framework, achieving a coordinated optimization of security and experience by dynamically balancing privacy strength and functional requirements. Firstly, it analyzes the core challenges in multi-App interaction. Then, based on the Privacy by Design (PbD) principle, it integrates hierarchical encryption, federated learning, and dynamic permission control technologies to design a lightweight protection scheme (Cavoukian, 2009).

2 CHALLENGES IN MULTI-APP INTERACTION SCENARIOS

Under the multi-platform human-computer interaction environment, data sharing and functional synergy among different applications (APPs) for users have brought considerable convenience; however, they also given rise to a series of privacy protection issues.

Firstly, data sharing among different Apps relies on third-party interfaces, but the differences in technical standards and encryption protocols between platforms lead to the risk of data leakage. For instance, when users authorize login to JD.com through WeChat, their data must be transmitted between platforms. If there are vulnerabilities in the third-party interface, the data may be maliciously intercepted or misused (Cavoukian, 2009). A notable example is the 2018 Facebook-Cambridge Analytica incident that required a third-party application to illegally obtain data of 87 million users through the social graph, exposing the systematic pitfalls of cross-platform data flow (Tencent, 2022).

Secondly, in a multi-App environment, users need to configure privacy permissions for different apps individually, leading to increased operational complexity. For example, navigation Apps request "always allow" location access, whereas social platforms only request them "when in use". However, users have difficulty understanding the difference in permissions and potential risks (Isaac & Frenkel, 2018). Research shows that over 60% of users accept all requests by default due to permission prompt fatigue (Lin et al., 2022). More seriously, malicious Apps can also infer user information through permission combinations.

Finally, there exist significant differences in users' cognition of privacy risks, making it challenging to adapt consent protection strategies. Young users pay more attention to functional convenience and tend to open social data to obtain personalized recommendations; while elderly users have higher requirements for privacy transparency and are reluctant to share data due to concerns about risks. In addition, users often overlook key terms due to overly complex privacy policies, which exacerbates the risk of privacy leakage (Schaub et al., 2019).

3 USER-CENTERED PRIVACY

Privacy by Design (PbD), proposed by Anne Cavoukian, is a systematic methodology that emphasizes embedding privacy protection into the design stage of products, systems, and services rather than addressing it as an afterthought (Cavoukian, 2009). Its core lies in achieving privacy protection throughout the entire life cycle through seven principles, as illustrated in Figure 1: First, Proactive not Reactive, such as Blue Orange Digital's use of machine learning to proactively identify risks; second, Privacy as Default, minimizing data collection by default and requiring user authorization; third, Privacy Embedded, integrating privacy technologies(e.g., encryption, anonymization) into the system architecture; fourth, Full Functionality, balancing privacy with other functional requirements; fifth, End-to-End Security, ensuring the security of data collection, storage, processing, and destruction throughout the entire process; sixth, Visibility and Transparency, clearly informing users of data usage and open supervision; seventh, Respect for User Privacy, granting users control over their privacy. These principles, are centered on user rights and interests, requiring enterprises to deeply understand user needs and transform privacy protection into an intrinsic feature of the product rather than an additional function, thereby achieving a sustainable balance between technological innovation and privacy compliance.

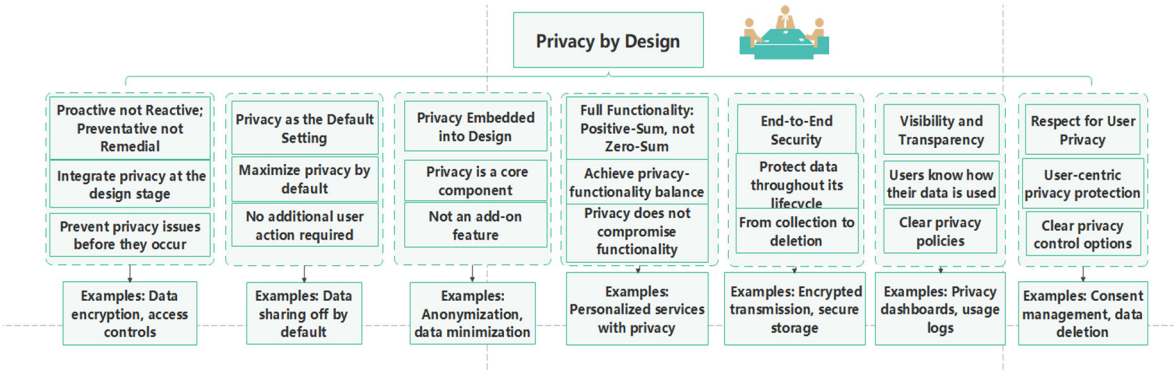

Figure 1：Pbd principle(Photo credit : Original).

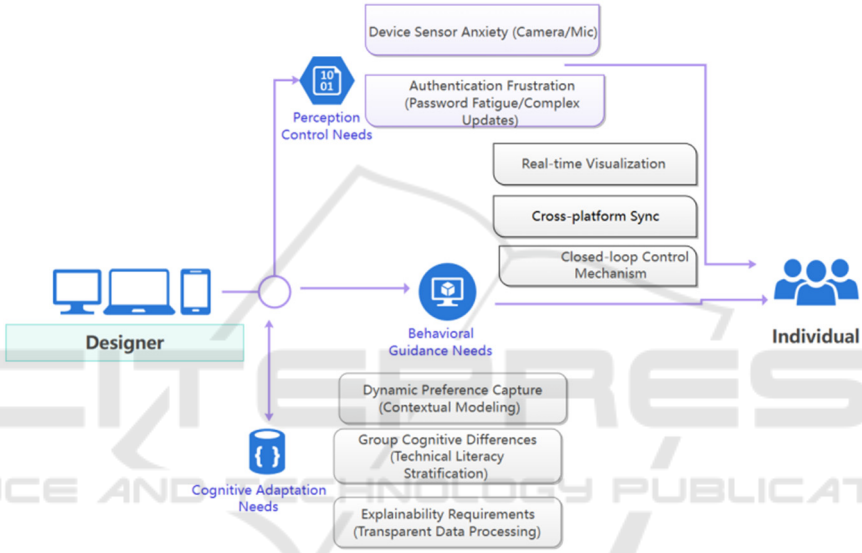

Figure 2：Core User Privacy Needs(Photo credit : Original).

As illustrated in Figure 2, user demand-driven privacy protection design focuses on three core dimensions: perceptual control, cognitive adaptation, and behavioral guidance. Relevant studies have indicated that in the smart home scenario, users have security concerns regarding continuous monitoring by sensors such as cameras and microphones, and the potential flaws in the identity authentication mechanism have led to frustration among 78% of users(Chalhoub et al., 2021) (Rosenberg et al., 2021). The group differences in privacy awareness directly affect the effectiveness of protection strategies, and dynamic modeling techniques need to be employed to capture individual privacy preferences (Zhang et al., 2023).

The personalized control system should establish a "presetting - adjustment - feedback" closed-loop mechanism. An augmented reality (AR)-based permission visualization interface has shown to enhance operational transparency by 43%, enabling users to intuitively perceive the data flow (Watanabe et al., 2022). Meanwhile, the cross-platform privacy policy synchronization technology supported by federated learning can reduce the risk of information overload by 37% while ensuring the continuity of multi-device services (Lee & Kim, 2023).

4 TECHNOLOGIES FOR PRIVACY PROTECTION

To cope with the privacy protection challenges in the multi-platform environment, numerous scholars having been exploring privacy protection technologies to strike a dynamic equilibrium between data security and functional efficacy.

Data encryption serves as the cornerstone for

safeguarding user privacy. In the interaction of multiple apps, user data typically needs to be transferred among different applications. If it is not encrypted the data might be intercepted or tampered with by malicious third parties. Through the adoption of encryption techniques (e.g., SSL/TLS protocol), the security of data during transmission can be guaranteed. Furthermore, anonymization of user data is also an effective means. Anonymization technologies eliminate or replace personal identification information within the data (such as names, ID numbers, etc.), ensuring that even if the data is leaked, it cannot be directly associated with specific users.

Hierarchical permission management serves as a critical technical approach for achieving a balance between functionality and privacy protection. In scenarios involving interactions among multiple apps, many applications require a significant number of permissions to provide personalized services. However, this often leads to excessive exposure of user privacy. By implementing hierarchical permission management, permissions can be classified into "essential permissions" and "enhancement permissions". Essential permissions are the minimum set of permissions required for an application to function properly, whereas enhancement permissions are utilized to improve or extend the app's capabilities. During user authorization, the system should provide clear explanations regarding the specific purposes and potential risks associated with each permission. For example, a navigation app might designate *"continuous location access"* as an optional permission for route optimization, but only require *"location access only during use"* as an essential permission when the navigation feature is actively being used (Isaac & Frenkel, 2018). This approach not only meets functional requirements but also ensures maximum protection of user privacy.

The sandbox mechanism, as operating system-level privacy-preserving technologies, implements data and resource isolation between applications to prevent malicious Apps from exfiltrating user information. In multi-App interaction environments, sandboxing restricts direct inter-application data access, ensuring that each application can only access its own data and resources within the boundaries of its authorized permissions. For instance, the sandbox mechanism in the iOS system rigorously controls application access to the user's file system, contact list, and other sensitive information (McDonald & Cranor, 2008). Even if an app undergoes a malicious attack, the sandbox mechanism successfully blocks attackers from accessing data belonging to other apps through the compromised app. This technology play a crucial role, particularly in multi-app interaction settings, as it significantly reduces the likelihood of data leakage at its source.

5 RELATED STRATEGIES

The privacy governance framework should be designed with a focus on the continuously changing needs of users. This involves creating a comprehensive, closed-loop regulatory system that encompasses the user level, and platform level. By doing so, the framework can facilitate the co-evolution of precise privacy control and seamless user experience.

5.1 User Requirements: User-Centered Design

Developing strategies to enhance privacy security requires looking at user needs, behaviors, and psychology to ensure that privacy protection measures are effective without compromising the user experience. A study of the relationship between Dutch students' perceptions of privacy risks and the privacy protection strategies they adopted shows that while individuals often express concerns about privacy, these concerns alone are not enough to motivate them to adopt stronger privacy protection practices (Van den Broek et al., 2020). This suggests that the core of privacy protection lies in improving users' privacy awareness. Studies indicate that users frequently lack of a thorough understanding of privacy risks, leading them to ignore potential threats when making privacy-related decisions. To solve this issue and increase users' awareness of privacy risks and protection measures, clear and easy-to-understand privacy policies and data usage instructions should be provided. Schaub et al.'s showed that by designing clear and concise privacy tips, users can be effectively helped to understand privacy risks and make more informed decisions (Lin et al., 2022). Furthermore, using simple language and visualization tools (e.g., icons, charts) to explain the privacy policies, offering real-time notifications at critical operational moments (e.g., when data is collected) to help users understand the data usage, and providing privacy protection tutorials or guidance when users encounter difficulties can assist users in mastering privacy settings. Implement privacy-enhancing technologies (PETs) to avoid affecting the user's operational fluency. Provide visual feedback

(e.g., "Your data has been encrypted") to strengthen users' sense of security. Ensure consistency in privacy protection measures across various platforms and devices, and offer a unified privacy settings interface to simplify cross-platform management for users. Lastly, through user feedback systems and privacy transparency reports, the platform can enhance the user's sense of participation and trust, encouraging them to actively participate in privacy protection efforts (Egelman & Peer, 2015).

5.2 Data Security: The Integration of Technical Means and Transparency

Data security is the foundation of privacy protection. By integrating technical methods with transparent design, it is possible to ensure data protection while improving user experience. First, data encryption and anonymization play a key role in safeguarding user privacy. During cross-application data transmission, encryption techniques are utilized to secure data and prevent malicious third parties from intercepting or altering it. At the same time, user data is anonymized to prevent direct exposure of user identities. For example, in health-related applications, anonymized health data can be shared with research institutions, which protects privacy and supports scientific research (Egelman & Peer, 2015). Second, permission hierarchy management is an important technique to balance functional requirements and privacy protection. The permissions are graded according to the functional requirements, for example, the permissions are divided into "necessary permissions" and "optional permissions", and detailed instructions are provided when the user authorizes. This approach meets functional requirements while maximizing privacy protection (Isaac & Frenkel, 2018). When a user authorizes a feature, potential risks are communicated through straightforward and concise alerts to help users make informed decisions (Lin et al., 2022). For instance, when the user authorizes access to the address book, the system could notify users, "This permission may be used to share contact details. Please proceed with caution."

5.3 Platform Collaboration: Cross-Platform Privacy Coordination

As the central entity responsible for collecting and processing data, the platform must take on the primary role in ensuring privacy protection. In a multi-platform environment, user data may circulate between various platforms, necessitating a collaborative mechanism across platforms to safeguard privacy and security. Data minimization and transparency serve as the foundational principles for privacy protection within platforms. Platforms should only gather the minimal amount of data required to fulfill specific functions (Van den Broek et al., 2020). At the same time, platforms should explain to users in simple and easy-to-understand language the specific ways of data collection and use (Lin et al.,2022). Furthermore, cross-platform privacy cooperation is a critical strategy for addressing inconsistencies in privacy settings across multiple platforms. For example, Google implements a unified account management system that allows users to manage the privacy settings of all Google services through a single interface (Google, 2022). Standard protocols like OAuth 2.0 or OpenID Connect can be employed for cross-platform authentication, offering single sign-on (SSO) functionality to reduce the inconvenience of repeated logins. Additionally, a dedicated permission management interface should be developed to help users view and modify cross-platform data permissions, ensuring consistency in user identities and data permissions. A cross-platform privacy protection alliance should be established to coordinate privacy measures among platforms, develop standards for cross-platform privacy protection and best practices, and hold regular meetings to share privacy protection technologies and experiences. In addition, platforms need to conduct routine privacy audits to ensure that their policies and measures align with the latest legal and regulatory requirements. For example, For instance, Facebook periodically releases transparency reports to disclose the handling of data requests and privacy protection measures (Meta, 2023). In practical applications, Apple's privacy label feature mandates developers to specify the types of data collected by an application and their purposes, aiding users in understanding privacy risks and making informed decisions (Apple, 2021).

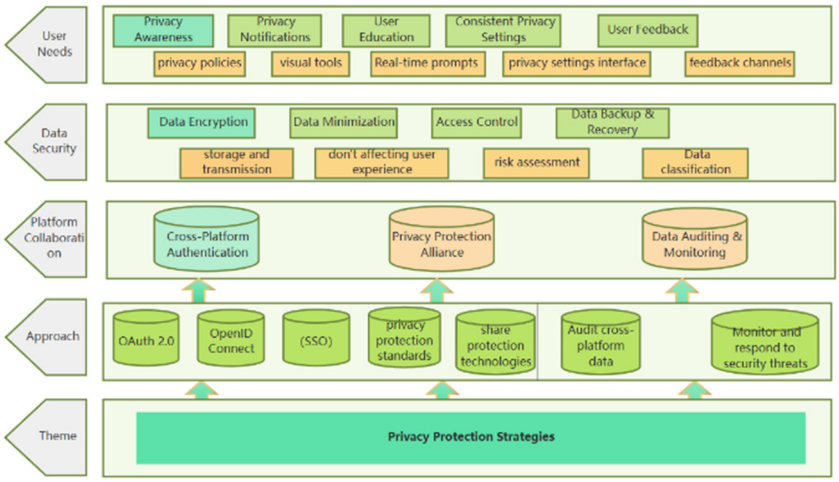

Figure 3：Privacy Protection strategies(Photo credit : Original).

6 FUTURE RESEARCH DIRECTIONS AND PROSPECTS

As human-computer interaction expands across multiple platforms, incorporating intelligent agents, XR environments, and automated compliance systems, privacy protection faces new challenges, such as cross-modal data integration and the blurred distinction between virtual and real domains. Although existing research has made progress in traditional scenarios, it lacks adaptability to the rapidly evolving technological landscape. There is a pressing need to investigate novel strategies that harmonize technological innovation, legal frameworks, and user-centric experiences.

To address the risks associated with cross-platform interactions of AI agents, a compact authentication mechanism leveraging zero-knowledge proof has been devised. Through the construction of decentralized identity mapping, this approach ensures comprehensive traceability of intelligent agents' operational activities. It supports the functionality of AI services like ChatGPT while safeguarding against unauthorized use of user information.

Design a dynamic blurring mechanism that combines light field sensing with edge computing. Utilize Neural Radiance Fields (NeRF) technology to detect sensitive information, such as facial features and identification details, in real-time within mixed-reality environments. Additionally, creates a spatial overlap early-detection framework. When the spatial mapping between the virtual interface and the physical environment exceeds the safety threshold, graded fuzzy processing is automatically triggered (Steed et al., 2022).

Construct a configurable legal clause generator to allow privacy policies to adapt dynamically based on regional laws(e.g., GDPR, CCPA). Leverage natural language processing techniques to interpret legal documents and produce standardized data collection formats that ensure compliance across multiple platforms, thereby resolving the issue of regulatory delays in cross-platform services.

7 CONCLUSIONS

This paper, starting from the perspective of user experience and incorporating the principles of Privacy by Design (PbD), comprehensively examines the balancing mechanism between privacy protection and functionality in multi-application interactions. By analyzing user behaviors and conducting technical validations, a three-dimensional collaborative approach involving "users, technology, and platforms" is proposed. In the future, it is viable to investigate the lightweight implementation of intelligent agent identity verification and real-time responses to privacy risks within XR environments. This would promote the evolution of privacy protection from passive adherence to active intelligence. The study provides theoretical and practical support for the construction of a secure and trustworthy multi-platform interaction ecology, while also offering substantial reference value for enhancing the privacy protection technology framework and industry standards.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509‑514.

Apple. (2021). App privacy details on the app store. Cupertino: Apple Inc.

Bitkom Research. (2023). Mobile app usage and privacy concerns: 2023 survey report. Berlin: Bitkom Association.

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Ontario: Information and Privacy Commissioner of Ontario.

China Academy of Information and Communications Technology. (2020). China privacy risk index report (2018‑2019). Beijing: Posts & Telecom Press.

Chalhoub, G., Kraemer, M. J., Nthala, N., et al. (2021). "It did not give me an option to decline": A longitudinal analysis of the user experience of security and privacy in smart home products. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 1‑16.

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). Proceedings of the CHI Conference, 2873‑2882.

Google. (2022). Unified privacy management in multi-device ecosystems. Mountain View: Google LLC.

Isaac, M., & Frenkel, S. (2018, March 19). Facebook and Cambridge Analytica: What you need to know. The New York Times.

Lee, H., & Kim, S. (2023). Visual analytics for real-time privacy monitoring. IEEE Transactions on Visualization and Computer Graphics, 29(5), 2158‑2168.

Lin, J., et al. (2022). Why users ignore permissions: A longitudinal study of mobile app privacy decisions. Proceedings of the USENIX Security Symposium, 345‑362.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. I/S: A Journal of Law and Policy for the Information Society, 4(3), 543‑568.

Meta. (2023). Quarterly privacy transparency report: Q3 2023. Menlo Park: Meta Inc.

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Rosenberg, D., et al. (2021). Context-aware privacy frameworks for IoT ecosystems. IEEE Transactions on Dependable and Secure Computing, 19(4), 2456‑2470.

Schaub, F., et al. (2019). Designing effective privacy notices: A longitudinal analysis. Proceedings of the CHI Conference on Human Factors in Computing Systems, 1‑13.

Smith, J., & Brown, T. (2021). Social media analytics and privacy trade-offs in multi-platform ecosystems. IEEE Transactions on Human-Machine Systems, 51(4), 321‑330.

Steed, A., Frljak, M., et al. (2022). Privacy preservation in augmented reality environments: A perceptual study. ACM Transactions on Interactive Intelligent Systems, 12(4), Article 32.

Tencent. (2022). WeChat Open Platform Security Whitepaper. Shenzhen: Tencent Security.

Van den Broek, M., et al. (2020). Privacy concerns and protection behaviors in Dutch students. Computers in Human Behavior, 108, 106342.

Watanabe, K., et al. (2022). Cognitive load theory for elderly-friendly privacy interface design. International Journal of Human-Computer Studies, 164, 102876.

Wang, L., et al. (2021). Age and cultural differences in privacy preferences: Implications for personalized systems. Computers in Human Behavior, 120, 106742.

Zhang, X., & Liu, H. (2020). Designing transparent privacy controls for multi-platform applications. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 1‑12.

Zhang, Y., et al. (2023). User-centric privacy-function tradeoff modeling in IoT systems. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 7(2), Article 67.