Analysis of Big Data Privacy Risks and Countermeasures in Human-Computer Interaction Context

Lijing Jiang

{ JINGJEAN2004@outlook.com }

Undergraduate Student, Digital Media Technology Program, School of Computer Science, Chengdu University of Information Technology, Chengdu, Sichuan, China

Abstract. This article focuses on the large-scale information privacy security issues in the context of human-computer interaction and the corresponding management methods. It deeply analyzes the interaction and intrinsic connection between human-computer interaction and the risks of large-scale information privacy. It comprehensively summarizes the common privacy threat types in human-computer interaction scenarios, and provides targeted privacy risk prevention and control measures from both technical and management perspectives, establishing a privacy protection system that integrates technology and institutions. The research results show that current privacy protection research is trending towards a shift from the "notification - consent" model to the "communication - control" mechanism. Multi-channel interaction design and privacy reminder technology have become the focus of academic attention. This research has theoretical support and practical guidance value for improving the privacy protection mechanism in the human-computer interaction environment.

Keywords: Human-computer interaction; Big data privacy risks; Privacy protection framework; Multimodal interaction design; Privacy feedback technology.

1 Introduction

With the rapid advancement of digitalization, human-computer interaction technology has been widely integrated into every corner of daily life, from smart home systems to mobile applications. The ubiquitous interaction scenarios have generated a vast amount of user information [1]. This information not only makes services more personalized but also brings obvious privacy security risks. Studies have shown that in the current big data environment, privacy leakage incidents occur frequently and on a large scale. The number of big data leakages has also persisted, exceeding 5, 000 major cases in 2022 alone and encompassing many important areas, including healthcare and finances [2]. More so, in the 2021 report of App Personal Information Usage Trend Analysis [3], it was highlighted that out of the almost 10, 000 applications, 56.3% of applications were suspected of having problems of illegally gathering and using personal information with an average of 0.8 illegal risks per app.

ICIAAI 2026, May 22-24, Singapore, Singapore

DOI 10.4108/eai.22-5-2026.2365093

In an intelligent recommendation system, there is a phenomenon that is often referred to as the privacy contradiction, i.e., the desire to share personal information with other people and the actual act. Such a conflict within makes risk prevention more complicated. Single-dimensional solutions to problems are done by most existing research with little incorporation of technical, user cognitions and management norms. The mechanism of the privacy risk generation is very complicated, incorporating the problems of over-data collection and inadequate protection level on the storage, lack of proper user cognition and flawed management systems among other non-technical elements.

Depending on the data lifecycle, the risks of information security can be found in all phases of information acquisition, transmission, storage, application, and destruction. This will need us to ensure an elastic risk assessment and management mechanism that will be adjustable. This holistic perspective is still noticeably absent in current scholarly literature, and it is hardly possible to address the complex and ever-evolving threats to privacy in an appropriate manner. Hence, the development of a holistic privacy protection model that takes into account both technical factors, cognitive factors and institutional factors is very critical and urgent.

The research about big data privacy risks is based on several theoretical levels in the human-computer interaction environment. It is suggested in literature [4, 5], that the privacy computing theory suggests a trade-off between privacy threats and the possible rewards of the user. This contributes to understanding the role of people having concerns, and as well as offering theoretical justification in the influence of design interventions to change the perception and choices made by users on risk.

On the technical side, privacy protection mechanisms like differential privacy protection and fully homomorphic encryption have been an important theoretical basis for research. Concerning management, the privacy design concept proposes the idea of looking at privacy protection as the initial stage of system creation. These various theories act in concert with one another in forming a multi-level theoretical framework of researching the privacy dangers of big data in the human-computer interaction space.

2 Analysis of the Correlation between Human-Computer Interaction and Big Data Privacy Risks

In the current technological environment, the issue of personal information security has become a major challenge in the digital age. With the widespread popularity of smart terminals and the Internet of Things, massive amounts of data generated by users during daily interactions are constantly being collected and analyzed. Although this brings convenience for personalized services, it also poses serious risks of privacy leakage. Research [5] indicates that in common interaction scenarios such as smart homes, mobile applications, and social platforms, sensitive data such as users' activity trajectories, location information, and physiological characteristics are facing multiple threats including illegal acquisition, abuse, and unauthorized dissemination. The privacy protection theory [6] states that information transmission during the interaction process is covert and diverse. The traditional informed consent mechanism is difficult to fully protect users' privacy rights. The promotion of multimodal interaction technology has further increased the difficulty of privacy protection. The collection of information such as voice, images, and biometric features often exceeds the

expectations of users. Existing survey data show (as shown in Figure 1) that nearly 50% of smart device users have no clear understanding of the specific content of their data being collected. This information asymmetry weakens users' ability to independently control privacy, leading to a typical privacy paradox. From a technical perspective, although data encryption, anonymization, and access control protection measures have made certain progress, they still face urgent technical problems such as slow response and excessive resource consumption.

The studies indicate that the use, storage, and collection of personal information present leakage opportunities, which is now the central source of privacy threats. According to Qiao Rui, (2021), the current one-way model signal approval should be turned into a two-way interactive model communication - control and the added value of user active involvement in the privacy protection model is very important [1]. An example of multimodal human-computer interface design experiment was conducted by Bian Kun et al. in 2022 [2] and proved that the transparency of the interaction process is strongly connected to the sensitivity of the privacy of the users. In the article He Zhiwu allows an empirical survey of users of smart homes, which was published in 2021 [4] and summed up the reasons for privacy worries in three dimensions: technical attributes, context of use, and personal variations. More research carried out by Cao Yanging in 2022 helped to explain the discrepancy between the perceived risk of privacy and the protective behavior through which users address privacy risks [5], and found that there has been a wide disconnect between predicted risk aspects and real protective behavior. In 2021, Hao Le concentrated on customized recommendation systems [7] and examined the psychological perception of the choice of the user regarding the disclosure of personal information. On this basis, I have generalized the relationship between human-computer interaction and the risk of big data privacy as indicated in Table 1. All these research findings point to the fact that privacy threats in the human-computer interaction context can be described as multi-dimensional and dynamically evolving, and context-related, and a multi-layered option necessitating the overall correction of the situation on three levels: the technical approach, the managerial framework, and the user practices.

Table 1. Human-Computer Interaction and Big Data Privacy Risk Correlation Table

Related dimension	Risk generation mechanism
Interaction as the data collection entry point	The human-computer interaction interface serves as the direct contact point for data collection. The naturalness and seamless nature of interaction reduce the user's mental barriers, leading to unconscious or excessive data disclosure.
The interaction interface affects risk perception	The transparency, controllability, and feedback mechanism of the interaction interface directly influence users' perception and judgment of risks. Ambiguous or missing privacy information presentation results in "information asymmetry".
The dynamic nature of interaction increases risk complexity	Human-computer interaction is a continuous and dynamic process, and data risks also change in real time. Traditional static authorization cannot cover the entire lifecycle of interaction, resulting in risks arising during context transitions.
Interaction mode shapes user behavior (privacy paradox)[8]	Convenient and personalized interaction design creates a strong immediate experience benefit, causing users to tend to underestimate long-term privacy risks in their behavior, thereby practicing the "privacy paradox".

Advances in the technology field, particularly in multimodal interaction technology, have brought about more complex privacy protection challenges. The collection and application of biometric information such as voice and face have become prominent issues. Research shows [4] that the integration of multi-modal data in smart home devices may lead to a "data accumulation effect", increasing the threat to users' privacy exponentially. From the perspective of user behavior, the privacy contradiction phenomenon has attracted widespread attention from the academic community. Although users show strong concerns about privacy, they often actively share personal information when using it. The latest discovery is that personalized recommendation systems employ a "gradual information guidance" strategy, significantly reducing users' privacy vigilance. In terms of management mechanisms, academic discussions are shifting from the traditional "notification - permission" framework to a dynamic "communication - regulation" model, emphasizing the timely implementation of privacy protection during the interaction process.

3 Types of Big Data Privacy Risks in Human-Computer Interaction Environments

In intelligent devices are widely spread, under the background of various interactive, personal privacy information is facing the unprecedented security challenges, show a complex and various characteristics of large data privacy risks from a technical perspective to explore, Privacy concerns mainly includes data acquisition phase of the excessive collection, storage, link security holes, the leak of risk in the process of transmission and data using the depth of mining. Specifically, terminal devices may collect data without the user's awareness, the security protection of cloud storage is insufficient, the encryption level of information transmission is not high enough, and the algorithm analysis results in overly precise user profiles. In the smart home environment, audio collection devices, video surveillance sensors, etc., may continuously record users' behaviors, and mobile applications often excessively request sensitive data such as location information and contact lists. These potential threats not only endanger personal privacy but may also lead to serious consequences such as identity theft and targeted fraud. Given the diversity of privacy risks, it is urgent to adopt systematic response strategies from multiple dimensions such as technical standards, operation management, and legal guarantees, to address the new privacy threats in human-computer interaction scenarios.

In the human-computer interaction environment, the privacy risks of massive information present multiple characteristics. According to the existing research results,these risks can be mainly classified into four stages： information collection,storage,processing,and application. Each stage has its own specific risk forms, as shown in Table 2.

Table 2. Privacy Risk Stage and Manifestations

Risk stage	Risk type	Specific manifestations
Collection	Excessive collection and covert collection	In the human-computer interaction environment, smart home systems use various sensors to quietly collect users' behavioral information; at the same time, mobile applications frequently request sensitive access permissions such as geographical location and contact list.
Storage	The vulnerability of a single point in centralized storage	Centralized data storage is prone to becoming the target of malicious attacks and poses a risk of extensive information leakage. For instance, in the relevant research of the "M Company Automobile Maintenance Data Platform Project", the exposed security vulnerabilities fully illustrate this point.
Handle	Algorithm black box and secondary utilization	In human-computer interaction environments, artificial intelligence systems (such as personalized recommendation engines) often process information in an undisclosed manner, and the original data may be used for subsequent research beyond the initial permission scope.
Use	Unauthorized sharing and commercialization	Without the users' knowledge, their personal data is transferred to third-party institutions or used for commercial analysis. The situation where government departments "do not sufficiently identify sensitive personal information" during the process of data disclosure falls under such risks.

4 The Design Strategy of Big Data Privacy Permissions from the Perspective of Human-Computer Interaction

Human-computer interaction has become a crucial link in the transmission of a large amount of information. The traditional privacy protection mechanisms are undergoing a profound transformation from static compliance to dynamic perception. Relying solely on "passive defense" methods such as technical encryption or administrative regulations is no longer sufficient to effectively address the privacy threats that arise immediately during the interaction process. The main battlefield of privacy protection has shifted to the interface where users communicate with the system itself. This requires solutions to break through the traditional binary opposition of "technology" and "management" and construct a comprehensive strategy centered on human-computer interaction design. The fundamental purpose is to establish "perceptive protection", that is, on the basis of ensuring information security, through meticulous interaction design, to transform the privacy management rights into a positive experience that users can feel, operate easily, and receive feedback. This transformation reflects a mode upgrade from "notification - authorization" to "dialogue - regulation", with a focus on specific scenarios such as smart home and personalized services. By leveraging design, it aims to eliminate the "contradiction gap" between privacy risk awareness and protection measures. Therefore, this section focuses on systematically constructing a privacy permission design framework system based on HCI theory and oriented towards practical applications, converting technical means such as differential privacy and decentralized learning, as well as governance principles such as privacy embedding, into interactive elements that users can understand and control, thereby establishing a long-term stable balance between data value mining and privacy rights protection.

The interaction between the human and the computer has turned out to be an important part of the communication of a big portion of information. The old forms of privacy protection are in the lean of radically re-evaluating their stagnant compliance forms of protection to dynamic perceptions. It is no longer adequate to adopt only the so-called passive defense means like technical encryption or administrative policies that can help to cope with the privacy threats that will emerge in the process of interaction immediately. The interface between users and the system has become the primary stage of privacy protection. It demands solutions to overcome the traditional binary rivalry of the concepts of technology and management and create a holistic approach to form a new strategy based on the design of human-computer interaction. The basic objective is to create "perceptive protection" in other words, on a premise of assuring information protection through careful interaction design to transform the rights of privacy management into a positive experience that the user will feel, operate conveniently and get responses. That change can be seen as a mode upgrade between the notification - authorization to dialogue - regulation with a specific scenario orientation to smart home and personalized services. It can use design to remove the gap between the awareness and protection mechanisms in relation to privacy risks. Thus, the present section is dedicated to building a privacy permission design structure system with respect to the HCI theory and oriented towards practice correspondingly, transforming technical processes, like differential privacy and decentralized learning, and the principles of the governance structures, like privacy embedding, into elements of interaction that the user can learn and manage, which will allow creating a stable long-term equilibrium between data value mining and protection of the privacy rights.

To solve the risk to privacy, first, it is necessary to discuss the transparency and explainability of the user-centred permission management, which is one of the effective bases of personal privacy protection. The design idea must be aimed at changing the process of the information transmission that has not turned into a visible state tidy and understandable, as well as to simplify the difficult calculation and judgment process.

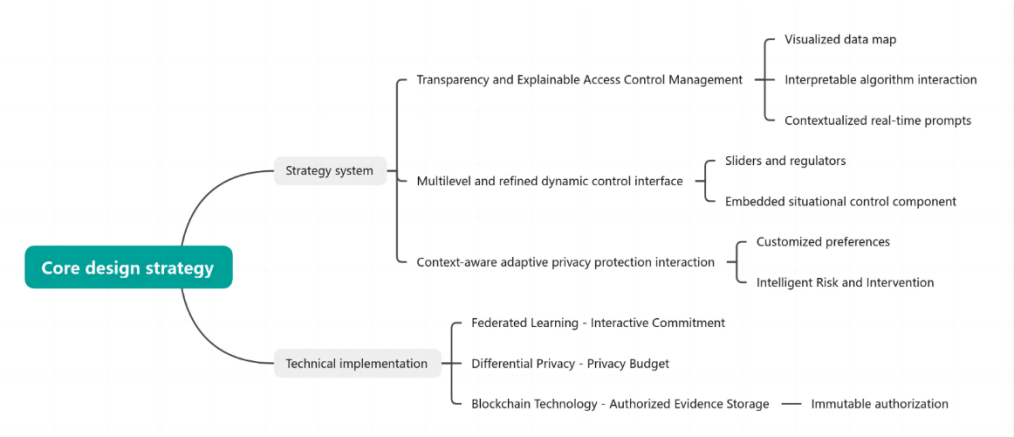

Fig. 1. Core Design Strategy (Picture credit: Original)

To begin with, the transparency and explainability of user - centered permission management are used to deal with data imbalance, an important basis for protecting personal privacy. The design concept should be centered on transforming the invisible information - transmission process into a visible and simple - to - understand state, and making complex calculations and judgments more clear - cut.

Another aspect is that there is a multi - level, well - honed dynamic control interface that gives users control rights. It shouldn't merely conclude at the "on/off" binary choice. Continuous, multi - dimensional, and context - related control granularity should be given to handle the complexity of big data applications. Presently, control levers and multi - dimensional adjustment devices are provided in the user interface. In certain scenarios, control components are added to integrate adjustment elements directly into the operation, so as to prevent them from being hidden deep in multiple - level menus. In addition, preset scenario rapid options and well - defined settings are offered to meet different needs. A number of scenario presets are developed to address the personalized needs of advanced users.

The end part is about adaptive privacy protection interaction that depends on context awareness. An ideal operating outcome should let the system have the skill to "uncover the user's intentions". While making sure of security, it has to minimize needless interference as far as possible. Thanks to this experience, the system is able to perceive the surrounding environment and make self - adjustments accordingly. There is a need for a situation - based flexible configuration policy, and users' potential learning and personalized preferences need to be shaped. And by using artificial intelligence algorithms, a "user privacy tendency model" is gradually established. For unusual and potentially threatening access behaviors such as frequent use of microphone devices by a certain software, various interaction methods are adopted promptly, such as sudden dialog boxes or continuous status bar reminders, to actively engage in a "conversation" with the user, explaining potential risks, asking for the user's opinion, and thereby transforming passive records into active defense.

5 Scenarios-oriented Technology - Management - HCI Integrated Protection Framework

In the human-computer interaction environment, the complexity of big data privacy risks makes a single-dimensional solution inadequate. Current research and practice mostly believe that building a multi-dimensional privacy protection system that integrates technology, management, and human-computer interaction design is an inevitable trend.

In this system, technology is seen as the core competence, management as the institutional assurance, and human - computer interaction design as the important connection that links users and turns the effectiveness of the former two into actual protection results. This approach is not simply an additive approach; it looks for organic cooperation. The technical mechanism makes fine interaction control workable. The management system gives guidance on the ethical limits and compliance of interaction design. Great human - computer interaction design can strengthen users' acceptance and compliance with technological and management measures, creating a self - sustaining cycle. The purpose of this framework is to offer a flexible top - level architecture for a range of application scenarios. It makes sure that while

mining the value of data, privacy protection can be systematically planned, carried out integrally and felt across the whole flow.

Figure 2 shows that this integrated protection framework comprises three core levels that interlock with each other and interact constantly.

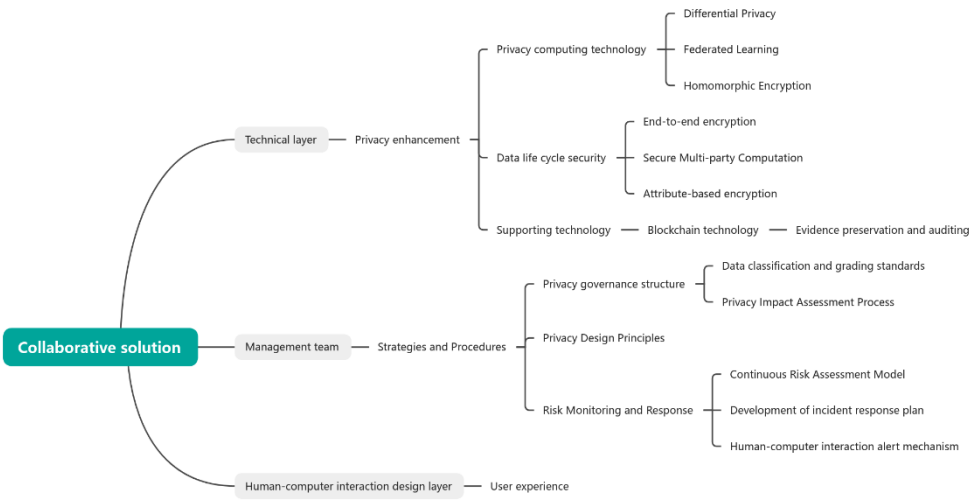

Fig. 2. Collaborative solution (Picture credit: Original)

First, on the technical level, it is in charge of supplying privacy - improving abilities that can be embedded for interaction purposes. Its crucial task is to present a set of "privacy capability components" that the upper layer can call. It contains the application of a variety of privacy - safeguarding computing methods in the information processing period. Right now, a great deal of the proposed methods consist of homomorphic encryption technology - a way to encrypt data and then encrypt it again [9], federated learning algorithm (solving the problem of data being on islands) [10], and distributed differential privacy algorithm [11]. Throughout the whole data lifecycle, different security measures, for example, full-fledged encryption, multi - party secure computing, and attribute - based encryption methods, have been set up to construct a strong defense mechanism. Due to the assistance of technologies like blockchain, for example evidence storage and audit traceability, a secure isolation zone for sensitive computing in the trusted execution environment is created. With the help of particle swarm optimization technology, a blockchain federated learning method based on particle swarm optimization (PSO) and Paillier encryption algorithm is built and abbreviated as FedPPB [12].

The second part is the management layer, responsible for developing strategies and processes to carry out the design. It ensures that technology application and interaction design follow a set of governing rules. It creates positions for information protection experts and sets up information classification and categorization criteria. It defines privacy assessment procedures and incorporates the concept of "factoring privacy into default and design" in the whole

product - development process. It clearly pinpoints which interaction points should offer privacy control options and deeply reflects on how to present them, ensuring user privacy is fully protected. It also creates a risk assessment and handling mechanism, formulates a long - term crisis assessment model and emergency response plan, and in so doing, enhances overall security.

The end part is the HCI design layer, in charge of carrying out user - controlled experience transformation. It changes technical capabilities and management requirements into user - friendly, effective, and reliable user experiences. It constructs standardized privacy interaction design models, for example, the "authorization and permission dialog window model", "personal information control panel model", and "data transmission visualization model", to make sure of consistent experiences across different platforms and situations, decreasing the learning difficulty for users. For the design of interfaces, it uses psychological theories, for example the default option effect and loss aversion tendency, to guide decision - making and ensure the privacy and security of the application. Nevertheless, it must also ensure the user's right to autonomous selection and the transparency of information. Creating a quick and well - defined feedback system is the most important step, so users receive immediate and intuitive confirmation upon changing privacy settings. Simultaneously, while strictly following privacy protection norms, it acquires user interaction data to measure the actual effectiveness of the design plan. The analysis results are fed back to refine management policies and technical parameters, and a "scheme formulation - implementation operation - effect evaluation - continuous improvement" cycle is established. This mechanism is capable of constantly improving privacy protection means and increasing user experience.

6 Conclusion

This paper unravels the complicated and mutually defining interaction between human and computer interaction and privacy threat, offers a collection of strategies in privacy permission design in the focus of human and computer interaction is interaction based on communication and control, and an elaborate architecture plan top-level. It develops three-dimensional integrated collaborative security model that incorporates technology, administration and HCI. This gives a methodological guideline for solving privacy protection issues in a systematic way.

Though such organization is attempted in this article and much has been made deep, nevertheless it has the following weaknesses. The study predominantly uses the academic sources of Knowledge Infrastructure of China (CNKI) and the range of the literature is slightly constrained. In addition, the research methods also have some limitations. Being a piece of literature review and theoretical constructions, the strategies and frameworks suggested in this article are primarily based on the literature analysis and logical reasoning. Nevertheless, they do not have a real user testing and prototype evaluation. Such a limitation of research methods can have an impact on the validity and viability of the research findings.

According to the discoveries and weaknesses of this article, a new study can be carried out to examine multi-modal data sampling techniques, such as eye-tracking, physiological sensors, and analysis of interaction records, and combine interdisciplinary techniques to create a multi-faceted system of research methods. Recast the privacy concept, go into new depths of

exploring new concepts of privacy like psychology, intent and emotion, as well as develop new interactive protection systems. Last but not least, encourage the integrated creation of scenario applications and shared norms, and carry out thorough research involving the particular requirements in particular domains like the finance sector, healthcare area and the educational area, so that the outcomes of the research are more relevant to the practical application.

References

[1] Qiao, R.: From "Information-Consent" to "Communication-Control": An interactive privacy protection mechanism based on human-computer dialogue. China Publishing. pp. 40–43 (2025)

[2] Bian, K., Han, D., Li, S., et al.: Research progress in multimodal human-computer interaction design. Mechanical Design. pp. 199–204 (2024)

[3] Qi An Xin: 2021 app personal information usage trend analysis report. Big Data Expo. (2021-05-27) (2022-12-29). https://www.donews.com/news/detail/4/3152878.html.

[4] He, Z., Zhang, M.: Peeking into privacy: A multidimensional analysis of influencing factors on privacy concerns of smart home users. Journal of Huazhong University of Science and Technology (Social Sciences Edition). pp. 117–129 (2025)

[5] Cao, Y., Ke, Q., Yang, H.: Research on user privacy risk perception and protection behavior in smart home use scenarios. Library and Information Knowledge. pp. 70–82 (2025)

[6] Liu, B., Lei, X., Dong, J.: Research on the influence of privacy protection technology features on user privacy protection behavior willingness. Journal of Information Science. pp. 214–229 (2024)

[7] Hao, L.: Research on the influencing factors of privacy information disclosure in AI human-computer interaction personalized recommendation. Information Theory and Practice. pp. 69–80 (2024)

[8] Miao, F.: Privacy boundary: Characteristics, causes and resolution of user privacy paradox in human-computer interaction. Journal of Kunming University of Science and Technology (Social Science Edition). pp. 49–56 (2023)

[9] Wang, B., Zheng, B., Chen, Y.: HEAFed: Efficient asynchronous federated learning algorithm for homomorphic encryption. Computer Applications Research. pp. 1–11 (2026)

[10] Wang, J.: Design and implementation of privacy-preserving big data analysis platform based on federated learning. Information Technology and Informatization. pp. 55–58 (2025)

[11] Kong, J., Zhou, H., Zhong, D.: Research on federated learning method for distributed differential privacy. Journal of Xi'an University of Technology. pp. 927–935 (2025)

[12] Shen, F., Liu, Z., Liang, Q., et al.: FedPPB: A federated learning method for blockchain based on PSO and Paillier encryption algorithms. Computer Research and Development. pp. 1–27 (2026).