Research on Personal Big Data Privacy Protection and Security Risk Prevention

Zeng Yingqing

Guangzhou Huashang College, Guangzhou, 511399, China

Abstract: *With the rapid development of information technology, big data technology has become an important component of modern society. In this context, the collection and use of personal data is becoming increasingly common, involving people's daily lives, work, learning and other aspects. However, this data collection and use behavior has also brought problems of personal privacy disclosure and security risks, posing potential threats to people's lives. This article aims to explore issues related to personal big data privacy protection and security risk prevention to ensure personal privacy safety. This article conducts in-depth research on the current status and existing problems of personal big data privacy protection through a survey and analysis approach, and proposes corresponding solutions. It is hoped that this research can provide ideas for improving the level of personal big data privacy protection and ensuring personal privacy safety.*

Keywords: *big data hidden, security risk, technology strengthening*

1. Introduction

In the context of the rapid development of big data technology and the widespread collection and of personal data, research on personal big data privacy protection and security risk prevention has become a hot field. Scholars at home and abroad have conducted in-depth research from multiple perspectives such as laws and regulations, technology research and development, and user education, have achieved certain research results. However, there are still some problems in existing research, as lack of uniform laws and regulations, technical vulnerabilities and security risks, lack of user awareness and education, and difficult to measure data privacy infringement. This article explores the issues and solutions related to personal big data privacy protection and security risk prevention. The research aims to improve the level of personal big data privacy protection, ensure personal privacy and provide reference and inspiration for related research and practical applications. The study of personal big data privacy protection and security risk prevention is not only of great significance for the protection of individual rights, but also has an important role in promoting the development of enterprises, governments, and society.

2. Overview of the privacy protection and security risks of big data

In the era of big data, the collection and use of personal data involve many fields, such as healthcare, finance, education, and more. These data contain a large amount of personal privacy information, such names, addresses, phone numbers, email addresses, etc., which may cause adverse effects on once leaked or used improperly.

The goal of big data privacy protection is to ensure that personal privacy is not illegally collected, stored, used, and disclosed. Meanwhile, it is also necessary to ensure the availability and security of the data to prevent the data from being tampered with or damaged. Big data security risks refer to potential threats and losses caused by data leakage, destruction, or misuse. These risks not only pose a threat to personal privacy but also may cause serious economic losses and reputation damage to enterprises and governments.

To address these challenges, technologies and methods for big data privacy protection and security risk prevention continue to develop and evolve. Currently, common technologies include data anonymization processing, access control, etc. Meanwhile, it is also necessary to strengthen the protection of personal privacy from the aspects of laws and regulations, management policies, and increase public awareness and skills in privacy protection.

3. Problems and risks of data privacy security

3.1 The lack of uniform laws and regulations

The lack of unified laws and regulations is an important issue in personal big data privacy protection and security risk prevention. Firstly, the lack of unified laws and regulations may lead to vulnerabilities in data privacy protection. In real life, every day our personal information is used in various apps, and many companies and institutions collect a large amount of personal data, including personal information, health information, financial information, etc. However, due to the lack of unified laws and regulations to regulate the collection and use of these data, some companies and institutions may abuse these data or disclose them to unauthorized third parties.

Secondly, the lack of unified laws and regulations may also lead to security risks in data processing and utilization. Due to the lack of unified laws and regulations to regulate data processing and utilization, there are many security risks in companies and institutions when collecting, storing, and using data. For example, some hackers may take advantage of technical vulnerabilities to steal data or launch cyber attacks. In addition, some companies and institutions may also disclose data to competitors or malicious individuals, resulting in data leakage and abuse, causing personal losses to users[1] .

In fact, the lack of unified laws and regulations has led to multiple data breaches. For example, in 2018, Facebook suffered huge losses due to the leakage of personal information of 8 million users. This incident shows the threats and challenges posed by the lack of unified laws and regulations to personal data privacy protection and security risk prevention.

3.2 Technical vulnerabilities and security risks

At the technical level, current personal privacy and security issues mainly exist in three aspects: (1) database vulnerabilities; (2) phishing attacks; and (3) authentication and authorization.

(1) Database vulnerabilities refer to the risk that if hackers successfully attack a database, they may obtain sensitive personal information stored within it, such as names, addresses, phone numbers, email addresses, passwords, etc. This information can be used for identity theft, fraud, or other malicious activities. For example, if attackers gain access to the database of an e-commerce website, they may view users' personal information and purchase records, and then impersonate users to engage in transactions or steal users' funds. Additionally, attackers may also sell the obtained data to third parties for advertising marketing, political investigation, or other unethical business practices.

(2) Phishing attacks are a type of attack that uses fake websites or email messages to induce users to enter sensitive information. These attacks often pretend to be legitimate websites or services, using fake pages or links to persuade users to enter sensitive information such as usernames, passwords, credit card information, etc. If users inadvertently fall victim to these attacks, their personal information may be stolen or misused. Additionally, phishing attacks may also use email messages to Induce users to click on malicious links or download malicious attachments， which may then infect a user's computer or other devices.

(3) Authentication and authorization issues can result from technical vulnerabilities, such as insufficient user identity verification or improper authorization allocation. This may allow attackers to impersonate legitimate users or gain access to permissions that they should not have, thus accessing or modifying sensitive data[2] .

3.3 Lack of user awareness and education

In the information age, personal data is collected and used in large quantities, but users generally lack sufficient understanding and alertness about the processing methods and possible risks of these data. Specifically, users are not clear about how these data are collected, used, and shared, and are even less aware of how to protect their privacy. This phenomenon may result from various reasons, such as information asymmetry, education deficiency, etc.

In addition, users often encounter security risks when using internet services due to a lack of relevant knowledge and skills. These risks may come from various forms of cyber attacks such as malicious software and phishing websites. Users generally lack sufficient understanding of the prevention measures of these risks, which further aggravates the risk of personal privacy disclosure.

3.4 Difficult to measure data privacy violations

There is no unified standard for the definition and scope of data privacy in personal big data privacy protection and security risk prevention. Different countries have different definitions and protection scopes for data privacy. This makes it difficult to determine in practice which behaviors belong to infringement of personal data privacy, so effective measures cannot be taken for prevention.

Moreover, the consequences of data privacy infringement may not be apparent until a long time later. Due to the complexity of data and the widespread network dissemination, once user data is leaked, the losses and impact on users are often extreme. Some users may suffer significant losses, while others may be minimally affected[3] . This makes it difficult for individuals to determine whether their data privacy has been infringed and the extent and scope of the infringement, and even if they are able to determine that their privacy has been violated, they often choose not to pursue or take action because of the high cost or lack of support from relevant laws and regulations. This makes it difficult for individuals to take action when facing data privacy infringement.

4. Individual data privacy security solutions

4.1 Establish sound laws and regulations

Improving laws on personal data privacy protection clearly stipulates requirements and norms for the collection, use, storage, and sharing of personal data. In terms of data collection authorization, the collection of personal data must be explicitly authorized by the user, and can only be used within the scope of the authorization. When collecting personal data, any organization or individual must clearly inform the user of the purpose, scope, and manner of the collection and obtain user authorization beforehand. The authorization method can adopt Free choice method, and users should not be prohibited from using software if they do not agree to the authorization. If the user does not grant authorization, some functions of the software can be stopped.

In terms of data storage security, personal data storage must take security measures to prevent data leakage and unauthorized access. When storing personal data, any organization or individual must take necessary security measures, such as encryption and access control, to ensure the confidentiality and integrity of the data. Any organization or individual who violates personal data protection laws will be subject to corresponding legal responsibilities and penalties. Organizations or individuals who collect, use, store or share personal data without authorization may be punished by fines, revocation of business licenses, etc., and an inter-departmental coordination mechanism can be established. The protection of personal data privacy involves multiple departments such as public security, industry and commerce, communication management. The core of the coordination mechanism is to strengthen information sharing and joint law enforcement. By establishing an information sharing platform and database, each department can obtain relevant information and data in a timely manner to achieve information sharing and mutual communication. Each department strengthens joint law enforcement actions to jointly combat illegal activities involving personal data infringement and form an effective deterrent[4] .

4.2 Strengthen technology research and development and improve safety

System enhancement can be achieved through methods such as using virtual patches or database password bridging tools to address data vulnerabilities(Figure 1): deploying a database firewall product with virtual patch functionality in series before the database. Virtual patches can help the database prevent discovery of and penetration attacks against the database's vulnerabilities, and prevent attackers from launching direct attacks on the database using vulnerabilities. This can reduce the risk of personal privacy data leakage caused by database vulnerabilities. For the issue of weak passwords in databases, a database password bridging tool can be used to strengthen them with the help of third-party tools. For example, a third-party software with a database password bridging function can help solve the problem of weak passwords. Through this tool, weak passwords can be modified to strong passwords, thereby improving the security of the database and preventing personal privacy data leakage caused by password cracking.

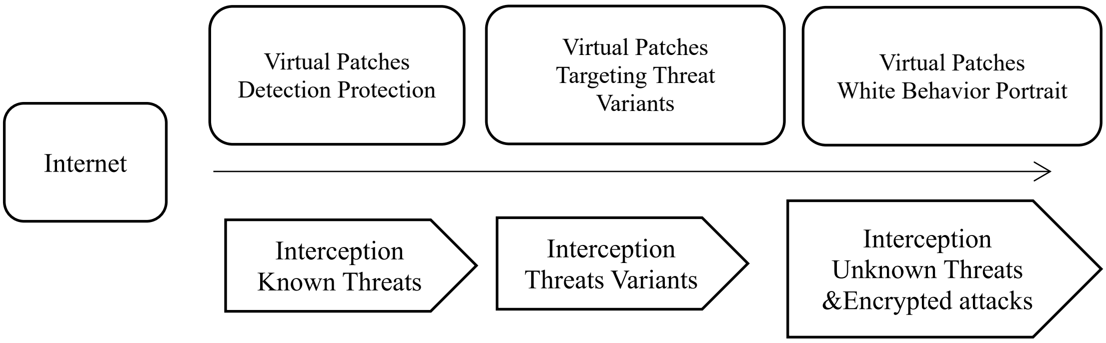
Internet
Virtual Patches Detection Protection
Virtual Patches Targeting Threat Variants
Virtual Patches White Behavior Portrait
Interception Known Threats
Interception Threats Variants
Interception Unknown Threats &Encrypted attacks

Figure 1. Virtual Patches

The following solutions can be applied to address authentication and authorization issues:

(1) Enable multi-factor authentication: Multi-factor authentication is a more secure method of identity verification that requires users to provide additional authentication methods beyond passwords, such as voiceprint verification, face recognition, etc. Disabling multi-factor authentication can leave the system vulnerable to attacks such as password guessing and brute-force attacks.

(2) Reasonable allocation of permissions: The system should allocate permissions based on the user's role and responsibilities. Administrators should assign permissions to users based on their job responsibilities to avoid assigning unnecessary permissions. Additionally, the scope of user operations should be restricted to avoid unauthorized operations and accessing sensitive data.

(3) Introduce advanced security tools to help manage and protect the system's security, such as using identity and access management tools to enhance system security and perform regular maintenance

4.3 Improve user awareness and self-protection ability

For enterprises, they should provide more transparent personal data usage and path, including how to collect data, how to use and share data, and be able to provide concise explanations and guide users to understand in the process of using apps, not limited to detailed service agreements and privacy policies. And, companies should establish privacy controls that allow users to manage their personal data autonomously. This can include providing features such as privacy Settings, data export and deletion. Through these features, users can better control their data and prevent data leakage and abuse. Third, the government can cooperate with enterprises to provide education and training to the society, such as the development of online small programs, including video tutorials, online lectures, etc., to popularize the knowledge and skills of big data privacy protection to users. These courses can include topics such as basic privacy principles, guidelines for secure operations, and identifying and avoiding cyber attacks. Posters, manuals and promotional videos can also be produced to convey the harm caused by big data privacy leaks to users, as well as tips for protecting personal privacy information. These materials should explain complex concepts in plain language and provide practical operational advice.

4.4 Improve the evaluation indicators and system of data privacy infringement

At the social level, the research and evaluation system of data privacy should be strengthened. It is necessary to clarify the definition and scope of data privacy, so as to judge which behaviors are infringements of personal data privacy, evaluate and grade the degree of privacy infringement, and provide corresponding constraints and penalties for each level of infringement. Establish the corresponding processing mechanism. Accept individual complaints and take appropriate action to investigate and deal with them. In addition, the corresponding claim mechanism can be established to help the individual who has been violated and help the victim file a claim with the involved unit.

Encourage industry self-discipline and self-restraint, in addition to the government's supervision, the industry should also strengthen self-discipline and self-restraint. The awareness and level of data privacy protection in the entire industry can be improved through the formulation of industry norms and the establishment of data privacy protection standards and best practices in the industry.

The government and enterprises can cooperate to establish data privacy protection evaluation indicators and systems. To solve the problem that data privacy infringement is difficult to measure, a set of evaluation indicators and system can be established to evaluate and measure the effect of personal data privacy protection.

The assessment process includes the following steps: collection of personal data, storage and processing of personal data, data breach events, security audits and privacy impact assessments. These steps cover the entire process from the collection and processing of personal data to its storage and transmission, helping to provide a comprehensive assessment of an organization's risk of data privacy violations. In order to better evaluate the data privacy violation, it is necessary to choose the appropriate assessment tool. These tools can include data security audit software, privacy risk assessment tools, etc. With these tools, data can be collected and analyzed automatically, improving evaluation efficiency and accuracy. The evaluation system is not a one-off effort, but needs to be evaluated and updated on a regular basis[5] . This can be done in combination with changes in national laws and regulations and changes in the organization's business. At the same time, it is also necessary to make corresponding adjustments and improvements according to the new evaluation results and findings, and constantly improve the accuracy and effectiveness of the evaluation system.This can help the government, enterprises and users better understand the protection of personal data privacy, and timely identify and solve potential security risks and problems.

5. Conclusion and discussion

This paper makes an in-depth study of data privacy protection and security risk prevention for individuals, summarizes the existing problems and risks of data privacy security for individuals, and puts forward corresponding solutions. By establishing sound laws and regulations, strengthening technology research and development and improving security, improving user awareness and self-protection ability, and improving the evaluation indicators and systems of data privacy violations, individuals' data privacy protection and security risk prevention can be effectively strengthened.

In the process of research, we found that the protection of personal data privacy and security risk prevention is a complex and important field, involving many aspects such as laws and regulations, technology, and user awareness. Therefore, future research should start from many aspects to further deepen the understanding and research on the privacy protection and security risk prevention of individual data, so as to better protect the privacy and security of users.

References

[1] Xu Mengyao. Research on privacy flow and Personal Information Protection in Big Data [J]. Journal of Southeast University (Philosophy and Social Sciences Edition), 2022,24(S1):pp.46-49.

[2] Wang Weijie.. Common Problems and Countermeasures of data security risk Assessment [J]. Security Science and Technology,2023,(06):pp.11-14. (in Chinese)

[3] WU Z G.. Progress of privacy protection technology for big data applications [J]. Telecom Network Technology, 2016,(02):pp.7-10. (in Chinese)

[4] Dou Y. Research on the countermeasures of data open sharing and personal privacy protection--Hierarchical data and algorithm accountability [J]. Modern Information, 2021, 41(07):pp.146-153.

[5] Wang Yang. Research on privacy protection of Network users under big Data environment [J]. Network Security Technology and Application, 2022 (10):pp.56-59. (in Chinese)