

Research on Privacy Protection and Security Technology of New Media Big Data Platforms

Ying Liu

Xiamen Institute of Software Technology, Xiamen, Fujian, China

Abstract: With the rapid development of new media technology and the widespread popularity of big data applications, new media big data platforms are facing serious privacy leakage and security risks while providing personalized services and enhancing user experience. This paper discusses in depth the challenges and coping strategies faced by new media big data platforms in the field of privacy protection and security, as well as the future development trend. The following conclusions are drawn: (1) New media big data platforms face serious privacy leakage and security risks while providing personalized services and enhancing user experience. (2) New media big data platforms face multiple technical challenges in the area of privacy protection and security, including the balance between performance and efficiency, the balance between privacy and security, the challenge of cross-platform data protection, and the rapidity of technology updates. (3) With the continuous improvement of relevant laws and regulations and the policy environment, new media big data platforms need to pay close attention to policy developments to ensure the legitimate collection, use and protection of user data. (4) The privacy protection and security technology of new media big data platforms will show the development trend of technological innovation and integration, standardization and normalization, user participation and transparency, as well as cooperation and sharing.

Keywords: New Media; Big Data; Privacy Protection and Security Technologies.

1. Introduction

With the rapid development of information technology, new media big data platforms have become an indispensable part of modern society. By collecting, storing, processing and analyzing massive amounts of data, these platforms provide users with a variety of services such as personalized content recommendation, accurate advertising, social media interaction and so on [1]. From news information, short video sharing to online shopping and social networking, new media big data platforms permeate every aspect of people's lives, greatly enriching people's digital life experience and promoting the rapid development of related industries. However, the rapid development of new media big data platforms also brings unprecedented privacy and security challenges. As platforms need to collect a large amount of user data to provide personalized services, these data often contain sensitive information such as users' personal preferences, behavioral trajectories, and social relationships. Once these data are inappropriately used or leaked, it will cause serious infringement on users' personal privacy and may even trigger broader social security issues [2]. Therefore, how to make full use of big data resources to improve service quality under the premise of safeguarding user privacy and data security has become an important issue that new media big data platforms must face. Studying the privacy protection and security technology of new media big data platforms is not only crucial to safeguarding users' rights and interests and enhancing the credibility of the platforms, but also of great significance to promoting the digital security and sustainable development of the whole society.

In the academic field, the research on privacy protection and security technology of new media big data platforms has attracted widespread attention [3]. Scholars at home and abroad have explored this issue in depth from multiple perspectives, including but not limited to data encryption techniques [4], access control mechanisms [5], privacy

protection frameworks [6], security audits and compliance assessments [7], and other aspects. These studies provide a rich theoretical foundation and practical experience for this paper. However, with the continuous progress of technology and the rapid development of new media platforms, there are still some shortcomings in the existing research, such as the convergence of privacy protection and security technology applications, and the challenges of cross-platform data protection [8]. Therefore, this paper aims to further explore the privacy protection and security technologies of new media big data platforms on the basis of existing research, with a view to providing new ideas and insights for research and practice in related fields.

2. Overview of New Media Big Data Platform

2.1. Definition and Characteristics

New media big data platform refers to a comprehensive service platform that collects, stores, processes, analyzes and applies massive new media data by using modern information technology, especially big data, cloud computing, artificial intelligence and other advanced technologies. These platforms not only cover traditional media forms such as news, radio and television, but also extensively involve emerging media forms such as social media, short videos, live broadcasting and online shopping. The main features of new media big data platforms include:

(1) Massive data: the new media platform generates a huge amount of data every day, covering multiple dimensions such as user behavior, content creation, and social interaction.

(2) Diversity: data comes from a variety of channels and terminals, including mobile devices, PCs, IoT devices, etc., and data types are also rich and diverse, such as text, images, video, audio, etc.

(3) Real-time: new media data is highly time-sensitive, and the platform needs to collect, analyze and apply the data in

real time to quickly respond to market changes and user needs.

(4) Personalization: based on big data analysis and artificial intelligence technology, the new media platform is able to provide users with personalized content recommendations and services.

2.2. Technical Architecture

The technical architecture of a new media big data platform usually includes a data collection layer, a data storage layer, a data processing and analysis layer, and an application layer.

(1) Data Collection Layer

It is responsible for collecting data from various channels and terminals, including user behavior data, content data, and social relationship data. Collection methods include API interfaces, crawler technology, and user-initiated submission.

(2) Data storage layer

Store massive data, usually using distributed storage, cloud storage and other technologies to ensure data reliability and scalability.

(3) Data processing and analysis layer

Cleaning, integrating, mining and analyzing the collected data to extract valuable information and insights. This layer usually involves big data processing frameworks (e.g., Hadoop, Spark), machine learning algorithms, and data mining techniques.

(4) Application Layer

Based on the results of processing and analysis, it provides users with application services such as personalized content recommendation, precise placement of advertisements, and construction of user profiles.

2.3. Data Types and Characteristics

The data types of the new media big data platform are rich and varied, mainly including: 1) User behavior data, which records the user's operation behavior on the platform, such as browsing, clicking, sharing, commenting, etc., reflecting the user's interests and preferences. 2) Content data, including news, articles, pictures, videos and other media content, is the core resource of the platform. 3) Social relationship data, such as followers, fans, friends and other relationship data between users, reflecting users' social network and influence. 4) Location data, user location information obtained based on GPS, Wi-Fi and other positioning technologies, which can be used to provide location-based services and advertisements. 5) Transaction data, data generated by users' transaction behaviors such as purchase and payment on the platform, reflecting users' consumption habits and economic status. These data types have different characteristics, such as timeliness, privacy, value density, etc., which put forward different requirements on the platform's data processing and analyzing capabilities.

2.4. Platform Operation Mode

1) Ad push, based on user profiles and interest preferences, personalized ad content is pushed to users to increase the click rate and conversion rate of ads. 2) Content recommendation, using machine learning algorithms to analyze user behavior and content, and recommend content of interest for users to improve user experience and platform activity. 3) User profile construction, through the integration and analysis of user data, to build user profiles, providing accurate user insights and decision-making support for the platform. 4) Data value-added services, open data resources to third-party

partners, provide data analysis and consulting services, and realize the commercial value of data.

3. Privacy Protection and Data Security Issues in the New Media Era

With the popularization of social media, mobile applications and smart devices, people's personal information is more and more likely to be leaked. Personal privacy protection and data security in the era of new media face the following major issues.

3.1. Data Collection and Sharing

In the era of new media, the collection of personal information has become more convenient and widespread. Social media platforms, e-commerce websites and mobile applications collect users' personal information, including but not limited to names, ages, genders, geographic locations, purchasing records and so on. Such personal information may be used for commercial purposes such as ad push, market research, etc., and may even be utilized by unscrupulous elements for illegal activities such as fraud and theft.

In addition, the sharing of personal information is also a problem. Many apps and websites will cooperate with third parties to sell users' personal information to advertisers or other organizations. This sharing of information may lead to the misuse of users' personal privacy or even leakage to unrelated people or organizations.

3.2. False Information and Internet Fraud

In the new media era, disinformation and online fraud have also become a serious problem. Through platforms such as social media, microblogs and WeChat, people can easily publish and disseminate information. However, this also gives the wrongdoers the opportunity to create and spread false information. False information may mislead the public and cause social instability and economic losses.

In addition, Internet fraud is also a privacy protection issue. Through the Internet, unscrupulous elements can easily obtain other people's personal information to carry out fraudulent activities. For example, through phishing websites, fake bank websites and other means, lawbreakers can obtain users' bank account numbers, passwords and other sensitive information, thus stealing their property.

3.3. Data Leakage and Hacking

In the new media era, a large amount of personal and corporate data is stored in the cloud or on servers. These data may contain sensitive information such as users' personal letters home business secrets. However, due to technical loopholes, mismanagement and other reasons, these data may be hacked or pooled exposed

Hacking refers to the act of unauthorized individuals or organizations to invade other people's computer systems through the network to obtain or destroy data. Hacking may lead to problems such as leakage of personal privacy, leakage of business secrets, etc., which bring huge losses to individuals and enterprises.

3.4. Data Misuse and Commercial Espionage

In the new media era, data is widely used in commercial activities. By analyzing users' data, enterprises can understand users' needs and behavioral habits so as to provide

better products and services. However, some enterprises may misuse users' data for commercial espionage or other improper purposes.

Commercial espionage refers to the acquisition of trade secrets or other sensitive information of competitors by an enterprise through unlawful means for commercial gain. This activity may lead to the leakage of an enterprise's trade secrets, which may bring about huge losses to the enterprise.

4. Sorting out Key Technology Methods for Big Data Security and Privacy Protection

Starting from the life cycle model of big data, strengthening and accelerating the research on security technologies at different stages will become one of the key issues facing big data in the future. With the increase in the amount of online data, in the process of using the data, it may cause the leakage of sensitive information that individuals have no intention to disclose, resulting in data insecurity, therefore, the privacy protection technology of data is proposed. Privacy protection technology can effectively ensure the confidentiality of data and solve the problem of leaking personal private information or sensitive information in the process of data release and analysis. At present, the commonly used privacy protection techniques contain privacy protection techniques based on data anonymization, privacy protection techniques based on data distortion, privacy protection techniques based on data encryption and desensitization techniques.

4.1. Anonymization Privacy Protection Technology

Data anonymization technology is a method of realizing privacy protection, which realizes data anonymization by hiding user-related information in the data to achieve the purpose of protecting data security. This technology has become a hot research topic in the field of information security since it was proposed.

In order to prevent the linking of user's privacy in order to resist the attack on user's private information through links and to ensure the release of data with user's privacy and security, various privacy-protecting anonymization models have appeared successively, which are: k-anonymity model, l-diversity model, t-proximity model, and so on. Among them, the k-anonymity model.

Among them, the k-anonymity model, in order to avoid user data being attacked by links, requires that each record in the data be indistinguishable from at least k-1 other records, so as to effectively reduce the risk of information leakage of the released data. In the process of technical realization, two problems need to be solved: first, how to improve data availability and reduce the loss of data and information while protecting data. The second is to reduce the risk of leakage of sensitive information.

4.2. Differential Privacy Protection Technology

When a user makes a data query, the data owner provides accurate information to complete the query, which is very easy to cause information leakage, and the attacker may then impersonate the user to make another query, and invert the user's privacy information from the query result. In order to solve the above problems, privacy protection is achieved by transforming the original data or adding noise to the statistical results, i.e., differential privacy protection technique.

Differential privacy protection is a privacy protection technology based on data distortion, the realization of this technology needs to solve 2 problems: one is to determine whether the algorithm meets the differential privacy, in order to ensure the security of the data; the other is because by adding noise to the original dataset, after the perturbation process, it is possible to reduce the impact of noise on some key data. Noise mechanisms for differential privacy protection are mainly categorized into exponential, Gaussian and Laplace mechanisms. It is widely used in relational databases, recommender systems, and trajectory information privacy protection. Through this technology can not only protect the privacy information of the trajectory data of mobile objects, but also ensure the availability of the data.

4.3. Data Encryption

Data encryption is a basic technology for privacy protection, which ensures the security and integrity of personal privacy data through encryption algorithms and key strategies, commonly used homomorphic encryption, attribute encryption and so on. In the distributed environment of cloud platform, there are various encryption techniques to hide sensitive information, such as secure multi-party computation, distributed anonymization, distributed association rule mining and distributed clustering.

4.4. Desensitization Technology

Data desensitization technology is the use of desensitization rules to privatize and deform operations on sensitive information to achieve the purpose of protecting the security of private data. Because, the data after desensitization is of the same type as the original data, the desensitization technology can ensure the availability of the data more effectively. Data attackers obtain personal information, analyze and correlate it to obtain more private information, and desensitization technology can effectively reduce the visibility and correlation of information. The organic combination of this technology and the security technology of cloud platform can protect the data security more effectively.

5. Challenges and Future Trends

5.1. Technical Challenges

New media big data platforms face multiple technical challenges in the field of privacy protection and security, which not only stem from the massive volume and diversity of data, but also are closely related to the limitations of technological development itself.

(1) Balance between performance and efficiency

How to maintain high efficiency in data processing and analysis while protecting privacy and ensuring security is a major challenge for new media big data platforms. Privacy protection technologies such as encryption and desensitization tend to increase the complexity and computational cost of data processing, so how to safeguard privacy without affecting the performance and response speed of the platform is an important direction for technology development.

(2) Balance between privacy and security

Privacy protection and security protection are two aspects that complement each other, but there are often conflicts in actual operation. How to effectively prevent external attacks and data leakage while safeguarding user privacy is a key issue that needs to be addressed by new media big data

platforms.

(3) Challenges of cross-platform data protection

With the diversified development of new media platforms, user data is often dispersed across multiple platforms. How to realize cross-platform data protection and ensure the security and privacy of data during transmission, storage and processing is a major challenge for new media big data platforms.

(4) Rapid technical update

The technology update speed of new media big data platform is very fast, and new privacy protection and security technologies keep emerging. How to keep up with the technology development trend and apply new technologies to the platform in a timely manner is the key to maintain the competitiveness of the platform.

5.2. Legal and Policy Environment

With the rapid development of new media big data platforms, the relevant laws, regulations and policy environments are also improving. However, changes in the legal and policy environment have put forward new requirements for privacy protection and security of new media big data platforms.

(1) Regulation of cross-border flow of data

With the acceleration of globalization, cross-border flow of data has become an important feature of new media big data platforms. However, there are differences in the regulatory requirements for cross-border flow of data in different countries and regions, and how to ensure the legality and security of cross-border flow of data is a concern for new media big data platforms.

(2) Legal framework for the protection of users' rights and interests

As users' awareness of privacy increases, the protection of users' rights and interests by relevant laws and regulations is also being strengthened. New media big data platforms need to comply with relevant laws and regulations to ensure the legal collection, use and protection of user data and avoid legal risks.

(3) Policy guidance and supervision

Government policies have an important impact on the development of new media big data platforms. Policy guidance can promote technological innovation and industrial upgrading, while regulation can standardize market order and protect user rights and interests. New media big data platforms need to pay close attention to policy dynamics and actively respond to policy requirements.

5.3. Future Trends

In the face of technological challenges and changes in the legal and policy environment, the privacy protection and security technology of new media big data platforms will show the following trends. Technological innovation and integration, with the continuous development of artificial intelligence, blockchain and other emerging technologies, the new media big data platform will continue to explore the application of new technologies in the field of privacy protection and security. For example, the use of artificial intelligence technology to improve the efficiency and accuracy of data processing, and the use of blockchain technology to achieve data traceability and tamper-proof; standardization and normalization, in order to cope with the legal requirements of cross-border flow of data and the protection of users' rights and interests, new media big data

platforms will actively promote the standardization and normalization of privacy protection and security technologies. Through the development of unified technical standards and specifications, the platform's data security and privacy protection level will be improved; user participation and transparency, as users' privacy awareness increases, the new media big data platform will pay more attention to user participation and transparency. By providing user-friendly privacy settings and transparent data processing processes, users' trust and satisfaction with the platform will be enhanced; Cooperation and Sharing, in the face of complex and changing privacy protection and security challenges, new media big data platforms will strengthen cooperation and sharing with other platforms, government agencies and scientific research institutions. By sharing technology and experience, we will jointly address the challenges in the field of privacy protection and security.

6. Conclusion and Recommendations

6.1. Conclusion

Through the in-depth study of privacy protection and security technology of new media big data platform, this paper draws the following main conclusions:

(1) The importance of privacy protection and security technology. While providing users with personalized services and enhancing user experience, new media big data platforms also face serious privacy leakage and security risks. Therefore, it is of great significance to strengthen the research and application of privacy protection and security technologies to safeguard users' rights and interests, enhance platform credibility and promote the healthy development of the industry.

(2) Technical Challenges and Response Strategies. New media big data platforms face multiple technical challenges in the field of privacy protection and security, including the balance between performance and efficiency, the balance between privacy and security, the challenge of cross-platform data protection, and the rapidity of technical updates. In response to these challenges, the platform needs to continuously explore the application of new technologies in the field of privacy protection and security, and at the same time strengthen technical research and development and talent cultivation to improve the security and privacy protection level of the platform.

(3) Impact of legal and policy environment. With the continuous improvement of relevant laws, regulations and policy environment, new media big data platforms need to pay close attention to policy dynamics to ensure the legitimate collection, use and protection of user data. At the same time, the platform also needs to strengthen compliance construction and legal risk management to avoid the impact of legal risks on platform operations and user rights and interests.

(4) Future Development Trends. The privacy protection and security technology of new media big data platforms will show trends of technological innovation and integration, standardization and normalization, user participation and transparency, and cooperation and sharing. These trends will push the platform to continuously improve the level of security and privacy protection and provide users with more secure, trustworthy and personalized services.

6.2. Recommendations

Based on the above conclusions, this paper puts forward

the following recommendations to promote the continuous development of new media big data platforms in the field of privacy protection and security:

(1) Strengthen technology research and development and talent cultivation. New media big data platforms should increase R&D investment in the field of privacy protection and security technology and explore the application of new technologies in the platform. At the same time, it should strengthen talent cultivation and team building to improve the platform's technical strength and innovation ability.

(2) Improve privacy protection and security policies. The platform should formulate a perfect privacy protection and security policy to clarify the principles of collection, use and protection of user data. At the same time, it should strengthen policy publicity and user education to raise users' awareness of and attention to privacy protection and security.

(3) Strengthen compliance building and legal risk management. The new media big data platform should pay close attention to changes in relevant laws and regulations and the policy environment, and strengthen compliance construction and legal risk management. By establishing a sound compliance mechanism and legal risk prevention system, it ensures the legitimacy and safety of platform operation.

(4) Promote technological innovation and standardization. The platform shall actively promote technological innovation and standardization, and strengthen cooperation and exchanges with other platforms, government agencies and scientific research institutions. By formulating unified technical standards and specifications, it will improve the data security and privacy protection level of the platform and promote the healthy development of the industry.

Conflicts of Interest

The authors declare that they have no conflict of interest.

References

- [1] Mo Ya-Xian. Research on privacy protection of social media in China[D]. East China University of Politics and Law, 2021.
- [2] ZHAO Chen. Privacy protection dilemma of social media in the new media era--Taking WeChat as an example[J]. New Media Research,2017,3(22):5-6.
- [3] Chen Xuebao,He Xiaosong. Research on key technologies for big data security and privacy protection[J]. Software,2023,44(10): 50-52+73.
- [4] Yan Chunlan. Research on network data security and privacy protection technology of radio and television stations in the era of integrated media[J]. Radio and television network, 2023, 30(06): 63-65. DOI:10. 16045/j. cnki. catvtec.2023.06.010.
- [5] Wang N, Ma Yiming, Zhao Juan. Research on big data security and privacy protection technology[J]. China High-Tech, 2022, (21): 52-54.
- [6] Liu Zechao. Introduction to data security and privacy protection technology[J]. Radio Engineering, 2022,52 (08): 1300-1301.
- [7] Du Pu. Research on data security and privacy protection technology of 5G communication network under mobile edge computing environment[J]. Yangtze River Information and Communication, 2022,35(10):211-214.
- [8] Bianna. Research on Typical Risks and Safeguard Mechanisms of Big Data Information Security[J]. Popular Standardization, 2022, (19):110-112.