WEP Warwick Evans Publishing

International Journal of Computer Science and Information Technology

ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 4, Number 3, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v4n3.42
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Research on Social Network Secunity Issues and Countermeasures Based on Big Data

Yue Xu

Salesforce Service Cloud, Redmond, 98052, USA
yxu.joyce@gmail.com

ABSTRACT

In the current era of rapid advances in information technology, personal secrets and data protection in the social field are facing unprecedented challenges. The phenomena of privacy breaches, online fraud, data tampering, and social automation robots on social platforms pose a serious threat to users and platforms. This article delves into the core security risks faced by social networks in the era of big data, and proposes corresponding solutions from the perspectives of technology, privacy protection, and social collaboration, such as data encryption technology, multiple authentication mechanisms, abnormal behavior monitoring, and the construction of a network security education system. Through the dual means of technology and management, social platforms are expected to significantly enhance data security protection and reduce potential security risks.

KEYWORDS

Big data; Social networks; Privacy protection; Network security; Data encryption

1. INTRODUCTION

In today's rapidly expanding social media landscape, users are increasingly posting personal information on these platforms, which exacerbates the risk of information security. In an era where massive amounts of data are constantly accumulated and analyzed, social networking platforms have accumulated a huge amount of information related to user privacy, identity authentication, and interpersonal communication, which has become a coveted target for criminals. The phenomenon of user data leakage, information tampering, and online fraud is constantly emerging, which not only damages users' trust, but also poses a threat to social harmony and stability. In view of this, the use of technological measures, strengthening platform responsibility, and promoting social governance to ensure the security of social network user data and personal privacy have become issues that must be addressed and solved. This article will conduct an in-depth analysis of the security challenges and response strategies faced by social networks in the context of big data technology.

2. OVERVIEW OF BIG DATA AND SOCIAL NETWORKS

2.1. Basic Concepts of Big Data

Big data refers to a vast group of information collected using various data collection methods and high-tech means. It exhibits extremely large, diverse types, rapid flow, and accuracy, and is usually summarized as the 4V attributes (data volume, data type, data flow rate, data authenticity). In the world of massive data, the scale of data is enormous and constantly expanding, including not only conventional ordered data but also numerous unordered data such as images, film and television

materials, textual information, etc. These sources of information are extremely diverse, covering many fields such as social platforms, sensor networks, IoT technology, mobile communication tools, and more.

In addition, when dealing with big data, big data technology focuses on real-time acquisition, in-depth mining, and timely response of data, which greatly accelerates the speed of data processing and makes capturing and analyzing data dynamics faster. In terms of data reliability, the field of big data emphasizes the accuracy and credibility of information to ensure the correctness of analysis results. In the field of social media, the application of big data mainly manifests in user behavior pattern analysis, emotion detection, personalized promotion, etc., providing data support and strategic reference for social networking sites. However, the large volume and complex types of data have also posed significant challenges to privacy protection and data security. Ensuring the secure management and reasonable utilization of this information has become a core research topic.

2.2. Definition and Development of Social Networks

Social media refers to an online community built by users using network technology to communicate, exchange, and share information. This platform promotes the rapid transmission and expansion of information by forming interactive links between users. Common social media sites include Facebook, Twitter, Weibo, WeChat, etc., which focus on user generated content and promote global information exchange and connectivity. The core functions of these social media platforms include information dissemination, interactive comments, private messaging, and community discussions, profoundly transforming the way people receive information and engage in social interaction.

The evolution of social media can be divided into several different periods. In the initial stages, social platforms like MySpace and Friendster primarily allowed users to create personal pages and make friends. With the continuous improvement of network technology, social media has gradually become more diverse and diversified, achieving a transformation from fixed to mobile, from single to intelligent. At present, advanced social networking platforms are no longer limited to text and image communication, but also include diverse functions such as video live streaming, short video publishing, and instant interaction. Moreover, social media is gradually penetrating into daily life and commercial activities, such as online shopping, information dissemination, and public opinion supervision, and has become a very important medium for information exchange.

2.3. Integration of Big Data and Social Networks

In the digital age, the interweaving of big data and social networks has become a significant trend. Social networks continuously generate a large amount of user information, covering various unstructured and structured data such as text, images, videos, and geographic locations. With the help of big data technology, these complex and ever-changing data can be quickly collected, properly stored, deeply analyzed, and accurately interpreted, thus demonstrating immeasurable practical value in various fields such as commercial applications, academic research, and security protection.

On social networks, the application of big data mainly focuses on key areas such as analyzing user behavior patterns, exploring interpersonal communication networks, evaluating emotional tendencies, and achieving customized content promotion. Through the study of user communication and interaction, published information, and social network structure, major platforms can gain a detailed understanding of users' preferences, interpersonal interaction status, and shopping habits. This refined data processing not only promotes the birth of targeted marketing strategies, but also provides solid support for targeted advertising and personalized content push, greatly enhancing commercial value.

3. MAIN SECURITY ISSUES IN SOCIAL NETWORKS

3.1. Privacy Leakage

Personal privacy faces a significant risk of leakage in the social networking environment, and this issue is particularly pronounced. Users frequently disclose their information on social media, accumulating a massive amount of personal information on social networks, covering many aspects such as identity authentication, geographic location, preference habits, and interpersonal communication. If this information is accessed by unauthorized individuals or maliciously exploited, the consequences of privacy breaches are unimaginable. Criminals use online fraud, illegal data collection, and system vulnerabilities to steal users' sensitive information, and then engage in illegal activities such as impersonation and fraud. At the same time, the privacy protection measures of social networks are not sound enough, and the privacy settings are cumbersome and difficult to understand, which makes it difficult for users to accurately control the dissemination boundaries of their information, further expanding the hidden dangers of privacy leakage. Recently, a series of data breaches have aroused widespread public attention to social network privacy and security, and have driven continuous improvement of relevant laws, regulations, and technologies.

3.2. Network Fraud and Malicious Attacks

In the field of social media, online fraud and harmful attacks are frequent security risks, usually carried out through social manipulation techniques, harmful programs, and online deception. Criminals use the trust relationships established between users on social media platforms to lure them into clicking on harmful links, installing malicious software, or leaking personal information such as bank account information, login passwords, etc. These fraudulent activities manifest in various forms such as identity forgery, false winning information, phishing websites, etc. Their core purpose is to steal users' personal information or directly carry out property fraud. Harmful attacks, on the other hand, silently invade users' devices, steal data, disrupt normal system operations, and sometimes use social platforms as a springboard to attack other users by spreading malicious code, building zombie networks, and other methods. With the continuous growth of social media user base and data, the methods of online fraud and harmful attacks are also upgrading, which poses a great challenge to the security protection of users and social platforms.

3.3. Data Tampering and Information Manipulation

In the field of social media, illegal tampering of data and manipulation of information seriously damage users' trust and trust in the platform. Criminals use illegal means such as fabricating user profiles, modifying posted information, controlling comments and likes, etc., to undermine the authenticity of information. This behavior not only misleads the majority of users, but may also become a tool for spreading rumors, manipulating public opinions, and even interfering in political elections and economic development. Information manipulation is often carried out through the creation of false news, the establishment of fake accounts, and the organization of large-scale cyber warfare operations, with the aim of deliberately guiding public opinion or launching attacks against specific targets. These behaviors can quickly spread and have far-reaching social impacts through the dissemination effect of social media.

3.4. Social Robots and Fake Accounts

On social platforms, automated programs (i.e. social bots) and artificial identities (i.e. fake accounts) pose significant security threats. These programs and accounts are often used to disseminate false information on a large scale, manipulate public opinion, and initiate harmful online activities. Through pre-set programs, social robots can mimic human user activities such as liking, sharing, and

commenting, generating a large amount of interaction in a short period of time, quickly increasing the visibility of specific content, and shaping public opinion. These automated tools are not only used for unethical marketing strategies, but also frequently appear in political propaganda, provoking social conflicts, or confronting competitors. Fake accounts, on the other hand, spread rumors, engage in online fraud, or steal user information by disguising themselves as real users. When these accounts act collectively, they can also act as the "navy" of the internet, playing a decisive role in public opinion struggles, creating false hype or manipulating public opinions. The widespread use of social bots and fake accounts seriously undermines the integrity and trust of social networks, and also poses great challenges to the secure operation of platforms. Effective measures are urgently needed to address this issue.

4. COUNTERMEASURES FOR SOCIAL NETWORK SECURITY ISSUES

4.1. Strengthen Privacy Protection Mechanisms

In the era of big data, personal privacy protection in social networks has encountered unprecedented challenges. In order to resist the threat of privacy breaches, major platforms urgently need to adopt a series of technologies and management strategies to strengthen the defense line of user data security. As a key means of privacy protection, data encryption technology mainly encrypts sensitive user information to ensure that even if data is stolen during transmission or storage, it cannot be illegally interpreted. Common encryption methods include symmetric encryption and asymmetric encryption. In symmetric encryption, the encryption and decryption processes use the same key. The formula is:

$$C = E(K, P)$$

Among them, C is ciphertext, is plaintext, P is encryption key, and E is encryption algorithm. In this way, user data is protected during transmission.

Multi factor authentication constitutes an important defense line for information security. This mechanism requires users to present other verification credentials during the login process, such as a verification code received on their mobile phone or personal biometric information, in addition to basic password input. This design can effectively prevent illegal elements from easily infiltrating the account even in the event of password theft, greatly enhancing the protection level of the account. The anonymization technology of data avoids the exposure of personal identity by confusing or interfering with user data. This method blurs or adds interference signals to sensitive user information such as birth date or geographic location, making it impossible to accurately infer the user's true information even if the data is illegally accessed. This technology is widely used in big data fields such as data analysis and advertising positioning to maintain user privacy. In addition, users are granted greater authority to determine the visibility of their personal information. The platform should adopt high standard privacy protection measures by default, while allowing users to adjust the disclosure of information according to their preferences. With the help of these technological means and management strategies, the platform can effectively enhance the level of privacy protection, reduce the possibility of data leakage and abuse, and thus more effectively defend users' privacy rights.

4.2. Establishing a Network Security Education System

Building a solid defense line for social network security, the network security education system plays a key role in helping users enhance their awareness of network security and proficiently apply basic protection skills. In the big data environment, users urgently need to master the methods of personal information protection, the ability to identify network risks, and strategies to cope with these challenges. Establish educational objectives and content. Network security education needs to cover

a wide range of knowledge areas, with core content including password policies, privacy maintenance, identification of phishing, application of multi factor authentication, and advanced technologies such as data encryption. Its core purpose is to enhance users' security literacy, enabling them to identify and effectively respond to cyber threats, and ensuring the integrity of personal information. The specific content of the network security education system is detailed in Table 1.

Table 1. Content of Network Security Education System

Educational content	Educational Objectives	Implementation method
Password management	Enhance password strength and security	Online courses
The use of multi factor authentication	Ensure multi-layered protection for the account	Practical training
Identify phishing attacks	Raise users' awareness of malicious emails and links	Simulated attack drill
Optimization of privacy settings	Enhance users' awareness of privacy control	Case study teaching
Data encryption and anonymization	Enhance awareness of data protection and privacy	Technical Workshop

User learning effectiveness and security awareness enhancement can be evaluated through methods such as network assessment and simulated attack testing. When measuring password strength, the entropy formula is a commonly used tool that helps evaluate the security of passwords. The formula is:

$$H = L \times \log_2 N$$

Among them:

H Entropy value for password (security)

L The length of the password

N The size of the password character set (such as using letters, numbers, symbols, etc.)

Regular training and teaching activities can guide users to gradually master methods to enhance password security, learn to create more complex passwords, and use advanced technologies such as multi factor authentication to defend their account security. With the help of a comprehensive network security knowledge transmission system, users' awareness of protection will be significantly improved, thereby more effectively defending their privacy and data from infringement, and calmly facing various security challenges on social platforms.

4.3. Enhancement of technical means

In the context of big data, the security challenges of social networks are gradually becoming more diverse, and improving technological means has become the core strategy to combat security risks. In order to ensure the stability and security of user information and the platform, strong protective measures need to be deployed in various technical dimensions, including threat detection, dynamic supervision, system vulnerability repair, and the application of artificial intelligence and machine learning technologies. Dynamic threat detection identifies the possibility of network attacks and malicious behavior through data analysis and behavior tracking. The system can detect and mark abnormal activities and issue timely warnings by analyzing user login locations, devices used, access times, and other information. The key technical formula behind it is:

$$At = \frac{\sum_{i=1}^{n} (Xi - \mu)}{\sigma}$$

Among them:

A_t Representing abnormal behavior detection values,

X_i For observation values,

μ As an average value,

σ For standard deviation.

This formula is used to measure the unusual index of behavior, and once the index exceeds the preset limit, the system will activate the warning mechanism. With the help of automated auxiliary tools, the platform can quickly repair security risks upon discovery. The built-in vulnerability detector in the system periodically checks the code and system to search for potential security vulnerabilities; Once a vulnerability is detected, a patch or upgrade plan will be automatically created; Subsequently, automated tools will deploy these patches to plug security vulnerabilities. This process effectively reduces the time required to respond to security threats and avoids the risk of vulnerabilities being maliciously attacked.To avoid information leakage, the system can use data leakage protection mechanisms to monitor the real-time flow of critical information. This mechanism effectively detects and intercepts abnormal data transmission behavior by deeply analyzing user operating habits and data flow paths, preventing unauthorized sensitive information from leaking out.

4.4. Platform Responsibility and Social Cooperation

The online social space shoulders a core mission in safeguarding personal information security, and urgently needs to rely on technological power and public collaboration to maintain user secrets. Social media platforms need to establish clear and visible privacy guidelines to enable users to understand their data collection and usage methods, and strictly comply with legal provisions such as the General Data Protection Regulation to ensure the legality of data processing. In addition, the platform needs to regularly conduct security reviews to identify system vulnerabilities, ensure encryption and security management of data during flow and storage, and prevent data leakage or illegal intrusion. Social collaboration is equally crucial, and platforms need to maintain close contact with government departments, judicial institutions, and various enterprises, especially in sharing security risk information. Through cross domain collaboration, all parties can share attack intelligence and enhance overall protection effectiveness. The formula can be expressed as:

$$S = f(P_1, \ P_2, ...P_n)$$

Among them, S represents the sharing effect of security intelligence, P_1, P_2, ..., P_n and represents different cooperation platforms. This type of information sharing can effectively prevent the spread of attacks and improve security response speed.

The platform has an obligation to provide users with network security education, enhance their understanding of network security through sending security information, organizing network attack simulation training, and guiding them on how to create complex passwords, identify phishing scams, and privacy protection techniques. In addition, the platform needs to establish a responsibility traceability system, and in the event of a data breach, immediately announce and implement remedial strategies to maintain user trust. Only by fulfilling these responsibilities and promoting collaboration can social platforms effectively resist the ever-changing security challenges.

5. CONCLUSION

With the rapid development of social media, the security challenges in the era of big data are increasing day by day. Ensuring user information security not only requires the responsibility of platforms, but also requires cooperation from all sectors of society. By leveraging advanced

technologies such as encryption, anomaly monitoring, and intelligent analysis, information protection can be significantly enhanced. In addition, social platforms also need to take on social responsibility, improve privacy protection systems, and closely collaborate with government agencies, judicial departments, and peer enterprises to exchange security information, promote the development of cybersecurity education, and enhance public awareness of security prevention. Only with the joint efforts of all sectors of society can social media platforms ensure user privacy and data security in the context of big data, and promote the construction of a safe and reliable cyberspace.

REFERENCES

[1] Wang, Shengzhou, Shuxia Liu. "Research on Personal Credit Reporting Issues in the Social Network Big Data Environment." Credit Reporting 41.9 (2023): 23-28.

[2] Luo, Fuzuo, Zhifu Yuan, Zhiyun Lai, et al. "Simulation analysis of big data security terminal architecture based on edge caching." Computer Simulation 40.3 (2023): 494-498.

[3] Ye, Huiwen, Xianfeng Ye. "Research on Privacy Paradox and Information Protection in Social Networks in the Era of Big Data." Western Broadcasting and Television 44.2 (2023): 75-77.

[4] Zhang, Liu, Xiwei Wang, Zixuan Song, et al. "Construction of Social Network Public Opinion User Theme Map System from the Perspective of Information Ecology." Library and Information Research 16.2 (2023): 91-96.

[5] Wang, Xiaohui. "Social network security issues and solutions in the context of big data." Communication World 31.2 (2024): 64-66.

[6] Zhang, Weihong, Lin Huang, Shengyong Cao, et al. "Research on Social Network Security Issues and Countermeasures Based on Big Data." Mobile Information 45.2 (2023): 128-130.

[7] Guo, Guifei. "Research on Multi-modal Secure Content Search in Online Social Networks Based on Deep Reinforcement Learning." Network Security Technology and Applications 6 (2023): 41-42.