Journal of Computer Science and Artificial Intelligence
ISSN: 3078-8242 (Print), ISSN: 3078-2309 (Online) | Vol. 2, No. 2, 2025

Application of Data Privacy Protection Technology in Social Media Platforms

Dishu Yang

Khoury College of Computer Sciences, Northeastern University, San Jose, CA 95113, United States

Abstract: The widespread use of social media platforms has made data privacy protection issues increasingly prominent. This article aims to analyze the application of data privacy protection technologies in social media, and provide a detailed review of different types of privacy protection technologies and their characteristics. It clearly points out the challenges that social media platforms face in privacy protection, including risks of personal data leakage, difficulties in complying with regulations, and insufficient user awareness of privacy protection. By strengthening the application of technologies such as data encryption and privacy computing, improving the privacy policies of social media, and enhancing users' awareness of privacy protection, an effective set of technical and administrative measures has been developed to enhance the platform's data confidentiality capabilities and the level of protection for user privacy.

Keywords: Data privacy protection; Social media platforms; Privacy computing; Encryption technology; User Privacy.

1. Introduction

While social media platforms provide convenient services, the issue of data confidentiality has become increasingly prominent. With the rapid advancement of information technology, the possibility of personal data leakage continues to rise, making the maintenance of privacy rights particularly crucial and becoming a focal point of social public opinion. Data privacy protection technology, as a key measure to maintain information confidentiality, includes various technical solutions such as encryption technology, de-identification, and privacy computing. Although these technologies have been widely deployed, they still face multiple challenges in the daily management of social networks, such as technological adaptability, cost-effectiveness, and legal compliance. Therefore, in-depth analysis of privacy protection technologies and their application research in social networks are crucial for strengthening platform data security, while also increasing user trust in the platform and further promoting the healthy development of the social networking industry.

2. Types and Characteristics of Data Privacy Protection Technologies

With the rapid development of social media platforms, protecting user data privacy has become an important issue. In response to this issue, numerous privacy protection technologies have emerged, each with its own characteristics and widely deployed in the field of data security on social media. For example, data encryption technology encodes information in a special way to ensure that only authorized users can interpret and access the data. This technology is widely used to protect users' conversation content, sensitive information, and login passwords. The significant advantage of encryption methods is that they can effectively resist unauthorized access, but at the same time, they also face a balance between encryption strength and processing efficiency. Anonymization technology eliminates or obfuscates user identities, making it impossible for data to be directly traced to specific individuals. This method is widely used in user behavior analysis and can effectively maintain privacy, but it may cause data distortion, which in turn affects the accuracy of the analysis results. Data anonymization technology reduces the risk of data leakage by modifying, replacing, or masking sensitive data. Social media platforms typically use this technology to anonymize sensitive information such as users' phone numbers and addresses. Although desensitization techniques help maintain data availability, they may affect data integrity.

Differential privacy technology adds noise to data, making it difficult for individual privacy information to be recognized by external attackers even if the data is leaked. This technology has been widely applied in the field of big data sharing and analysis, which not only maintains personal privacy but also ensures the effectiveness of data in statistical analysis. And blockchain technology, with its characteristics of distributed storage, data immutability, and transparency, enhances information security and user control over data. In the field of social media, the application of blockchain technology helps to track data access history and ensure data security, although its high cost and high technological barriers limit its widespread application. Homomorphic encryption technology is a method that can directly process encrypted data without performing decryption operations. It has great potential in the field of data mining because it can process data while protecting user privacy. However, due to its high computational difficulty, its application is still subject to certain limitations.

3. Data Privacy Protection Issues Faced by Social Media Platforms

3.1. Risk of Personal Privacy Information Leakage

Social media platforms, as the core area of interpersonal communication and information dissemination, carry the private data of numerous users. On these platforms, users' private information such as profile information, conversation content, geographic location, and personal preferences continue to accumulate and may be shared and mined. Although these platforms have implemented various security

policies to safeguard user privacy, technical flaws, employee information leaks, and collaborations with external partners still expose user data to threats of unauthorized access and improper use.

Social networking applications may be affected by factors such as hacker attacks, database exposure, or improper security settings, resulting in the leakage of many users' private information. Meanwhile, these applications may collaborate with external advertising publishers, data analysis agencies, etc. to share or sell user data, which undoubtedly increases the potential risk of personal privacy breaches. To present this issue more intuitively, Table 1 below lists the common pathways of personal privacy breaches and their impacts:

Table 1. Common Ways of Personal Privacy Leakage and Their Impact

Ways of privacy leakage	Describe	Possible impacts
Hacker attack	Hackers steal user data by attacking the databases or servers of social media platforms.	User information is stolen, accounts may be abused, and users' finances and identities are at risk.
Data sharing and sales	The platform shares or sells user data with third-party companies (advertisers, data analytics companies, etc.).	User data is used for advertising push, behavior tracking, etc., which violates user privacy and affects user experience.
Internal leakage	Unauthorized access, use, or disclosure of user data by internal personnel on the platform.	User information leakage may lead to identity theft or malicious exploitation.
Technical vulnerabilities	The platform's system or application has security vulnerabilities that can be easily exploited by malicious software or attackers.	The data has been tampered with or leaked, affecting the platform's reputation and user trust.

3.2. Legal Compliance and Privacy Protection

Faced with the increasingly prominent issue of data privacy, countries have formulated relevant legal provisions to enforce strict personal privacy protection standards for social networking platforms in data management and storage. The General Data Protection Regulation (GDPR) introduced by the European Union can be regarded as a model, which stipulates that platforms must obtain explicit authorization from users when collecting and using user information, and guarantees users the right to request the deletion of their data. Meanwhile, the California Consumer Privacy Act (CCPA) passed by the state of California in the United States also requires platforms to enhance users' privacy choices. Even though most social networking platforms have recognized the necessity of complying with regulations, compliance work remains challenging in the face of diverse privacy laws and regulations around the world. For cross-border operating platforms, it is undoubtedly a challenge to comply with different privacy protection regulations in various legal systems. Moreover, some platforms lack transparency in data collection and distribution, often leading to legal disputes and trust crises.

3.3. Lack of User Privacy Protection Awareness

Despite the increasing attention to personal data confidentiality, a large number of social media users still lack sufficient understanding of privacy and security. Many people share their information on social media without thinking, without realizing the risk of abuse or the possibility of leakage. Especially for the youth group, they often disclose various types of information on social media for convenience or pursuit of fun, but lack sufficient attention to the potential privacy leakage issues that may arise from this. The following Table 2 can visually demonstrate the specific manifestations and consequences of insufficient awareness of user privacy protection:

Table 2. Symptoms and consequences of insufficient awareness of user privacy protection

The manifestation of lack of privacy awareness	Describe	Possible consequences
Excessive sharing of personal information	Users frequently share sensitive information on social media, such as address, phone number, financial status, etc.	The risk of personal information leakage increases, and there may be issues such as fraud and harassment.
Ignore privacy settings	The user did not adjust the privacy settings of the social media platform in a timely manner, resulting in default disclosure of personal information or excessive sharing scope.	User data is prone to abuse, increasing the risk of platform information leakage.
Lack of vigilance towards third-party applications	The user did not prudently authorize third-party applications to access their social media account data.	Third parties may abuse data for advertising push, data sales, etc., infringing on user privacy.
Low risk awareness	Users have insufficient awareness of the potential risks of privacy breaches and neglect preventive measures.	Insufficient awareness of the consequences of privacy breaches may lead to issues such as property damage or identity theft.

3.4. Applicability and Cost Issues of Privacy Protection Technologies

In practical applications, although there are various privacy protection technologies, platforms have to weigh their applicability and deployment costs. For social networking platforms with a large number of users, when choosing privacy protection technologies, it is not only necessary to focus on the protective capabilities of the technology, but also to consider its operability and economy in expanding its scale. For example, although data encryption technology can strongly defend data security, the encryption and decryption processes require high computing resources, which may have a negative impact on the platform's operational efficiency and user experience. In addition, although techniques such as differential privacy and homomorphic encryption can provide stronger privacy protection, due to their computational complexity and high cost, corresponding trade-offs must be made when applying them. Meanwhile, deploying privacy protection technologies also means bearing significant development and maintenance costs. Social networking platforms must invest funds and human resources to carry out technological innovation, ensure compliance, and manage data, which is particularly challenging for small and medium-sized platforms.

4. Application Strategy of Data Privacy Protection Technology on Social Media Platforms

4.1. Strengthen the application of data encryption and de-identification technology

Data encryption technology, as the foundation of privacy protection, plays an indispensable role in the privacy protection of social networks. By encrypting sensitive data, the possibility of data being illegally accessed can be effectively reduced. Social media platforms need to adopt symmetric encryption technology (such as AES) and asymmetric encryption technology (such as RSA) as a whole at their architecture level. The AES algorithm is often used for encryption in instant messaging due to its real-time processing efficiency, while RSA technology, with its public-private key encryption mechanism, is suitable for key exchange and user identity verification. Assuming user data D, the encrypted data is represented as:

$$E_k(D) = D \oplus K \tag{1}$$

Among them, E_k represents the encryption function, D is the raw data, and K is the key. Through this method, even if data transmission is intercepted, attackers cannot decrypt and restore it.

De-identification technology further reduces the risk of privacy breaches by removing, replacing, or blurring sensitive data. In social media, user identifiers (such as IDs or IP addresses) can be hashed to generate irreversible encrypted values. For example, using SHA-256 to generate a hash value for a user identifier:

$$H(x) = SHA-256(x) \tag{2}$$

This processing method not only ensures the privacy of user information, but also maintains its rightful value in data statistical analysis. In order to further improve processing efficiency, it is necessary to build a computing system with strong encryption and anonymous processing capabilities, thereby strengthening the security protection of data during storage and transmission.

4.2. Utilizing Privacy Computing to Enhance Data Privacy Protection Level

By utilizing privacy computing methods, social media data security has been innovatively safeguarded, especially in large-scale data analysis and sharing scenarios, where the application of differential privacy and federated learning technology is particularly prominent. Differential privacy technology effectively ensures the confidentiality of individual user information during the analysis process by introducing interference signals into the data. Assuming a data analysis task requires calculating the total number of user activities $Q(D)$, the result of privacy protection achieved by adding noise ε is:

$$Q'(D) = Q(D) + \varepsilon, \varepsilon \sim N(0, \sigma^2) \tag{3}$$

Among them, $N(0, \sigma^2)$ is a zero mean normal distribution. The intensity of noise (i.e. standard deviation σ) determines the balance between privacy protection level and data accuracy. A higher level of noise can better protect privacy, but it can reduce the accuracy of analysis results.

As an advanced distributed machine learning approach, federated learning has important applications in ensuring data privacy. This technology enables these devices to train the same model cooperatively without exchanging their original data by deploying algorithms on each terminal device. Assuming that n each device participates in training, the model on each device is updated to ΔW_i, and the global model is calculated through weighted averaging to obtain:

$$W = \sum_{i=1}^{n} \frac{n_i}{N} \Delta W_i \tag{4}$$

Among them, n_i is the sample size of device i and N is the total sample size. Federated learning achieves a dual balance between privacy protection and model performance, but its communication cost and model synchronization issues still need to be optimized.

4.3. Optimize privacy protection policies and management of social media platforms

In addition to applying technological means, the privacy and security policies and management models of social media websites also play a crucial role. With the continuous optimization of privacy protection regulations around the world, major platforms have to abide by the legal provisions of different countries, such as the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA) of California, USA. These

regulations explicitly stipulate that when collecting user information, the platform must clearly explain the purpose of using the information to the users and obtain their explicit permission.

In order to ensure the implementation and enforcement of privacy policies, major platforms need to regularly review and evaluate privacy and security measures in order to timely identify and address potential risks and deficiencies. Data lifecycle management occupies a core position in privacy protection, and platforms must implement strict supervision over various aspects such as data collection, storage, application, and clearance to ensure that data meets privacy protection standards at all stages. In the data storage stage, a hierarchical storage strategy can be implemented to separate sensitive information from general information and encrypt sensitive information. In addition, the platform can also adopt blockchain technology to enhance transparency and tracking capabilities for privacy and security. With the help of blockchain networks, user information usage and access history records are stored to ensure that every data access activity can be reviewed and confirmed for compliance. Thanks to the immutable nature of blockchain and decentralized storage mechanism, this system not only ensures privacy and security, but also enhances users' trust in data management processes.

In the process of implementing privacy protection policies, the system should not only prioritize compliance, but also fully respect users' rights to informed consent and choice. An open and transparent privacy policy enables users to clarify the platform's operations in data collection, application, and storage, thereby enhancing the platform's credibility. In addition, the system should also provide users with various privacy customization functions, allowing them to decide the degree of information disclosure according to their own wishes.

4.4. Enhancing User Privacy Protection Awareness and Behavioral Norms

As the main body of privacy protection, users' behavior patterns greatly affect the possibility of privacy information leakage. Therefore, social media platforms have a responsibility to raise users' awareness of privacy protection through education and proper guidance, and guide them on online behavior guidelines. These platforms should be designed with intuitive privacy tips and user interfaces, allowing users to clearly recognize potential privacy risks and adjust their privacy options in a timely manner.

In order to encourage users to improve their online privacy protection behavior, social media platforms can implement incentive mechanisms, such as providing points or exclusive benefits as encouragement for users who actively configure privacy settings. Meanwhile, the platform can also utilize data analysis techniques to gain insights into differences in user privacy protection behaviors, such as conducting statistical analysis on the proportion of privacy settings applied among different user groups. Assuming the total number of users on a certain platform is N, and the number of users who have enabled privacy protection settings is n, the popularity rate of privacy protection awareness can be expressed as R:

$$R = \frac{n}{N} \times 100\% \tag{5}$$

By continuously tracking and evaluating this data, the platform can improve user guidance materials and interface layouts for privacy features in a targeted manner. In terms of user education, specific examples are integrated for education, and the real consequences of privacy breaches are used to raise users' awareness of data security.

Conclusion: In the rapidly evolving era of social media, maintaining user data security has become particularly important, and privacy protection issues have become increasingly prominent. Through encryption technology, de-identification, privacy computing, and other means, the platform can effectively protect user data security and avoid privacy information leakage. However, the effectiveness of these technological means also depends on whether the platform's privacy policy and management system are sound. Optimizing privacy protection policies and enhancing users' awareness and behavioral norms of privacy protection are equally important. With the continuous innovation of technology and the improvement of laws and regulations, social media platforms will promote the reasonable sharing and utilization of data while ensuring that user privacy is not violated, and promote the healthy growth of the entire industry. By implementing comprehensive privacy protection measures, the platform can establish a solid trust relationship with users and jointly face various challenges in privacy protection.

References

[1] Salim S , Turnbull B , Moustafa N .Data analytics of social media 3.0: Privacy protection perspectives for integrating social media and Internet of Things (SM-IoT) systems[J].Ad hoc networks, 2022(Apr.):128.

[2] Stephen M C , Wendy R , Antoine C V .The dark side of digitalization and social media platform governance: a citizen engagement study[J].Internet Research: Electronic Networking Applications and Policy, 2023, 33(6):2172-2204.

[3] He Y , Ouyang W ,Shaolong LiLin WangJing ZhouWenwei SuShenzhang LiDonghui MeiYan ShiYanxu JinChenglin LiYonghui Ren.Cloud computing data privacy protection method based on blockchain[J].International journal of grid and utility computing, 2023, 14(5):480-492.

[4] Cheng Z , Ji X , You Y Q X .FLPP: A Federated-Learning-Based Scheme for Privacy Protection in Mobile Edge Computing[J].Entropy, 2023, 25(11).

[5] Yang Z C , Kuang H , Liu J X .Privacy protection model considering privacy-utility trade-off for data publishing of weighted social networks based on MST-clustering and sub-graph generalization[J].International Journal of Modeling, Simulation, and Scientific Computing, 2023, 14(04).