UDC 004

CONTROLLING DATA SECURITY IN SOCIAL NETWORKS

I. Tagangylyjov, A. Klychev

Oguz Han Engineering and Technology University of Turkmenistan, Ashgabat, Turkmenistan.

Abstract. In the digital era, social media platforms have become essential tools for communication, business, and social interaction. With over 4.5 billion active users globally, the security of personal data shared on these platforms has become a critical concern. This article explores the various aspects of data security in social media networks, focusing on the types of data involved, the potential risks and threats, and the technologies used to protect user information. It discusses the importance of encryption, blockchain, artificial intelligence, and biometric systems in safeguarding users' personal data. Additionally, the article examines the legal frameworks,

such as the General Data Protection Regulation (GDPR). and the ethical considerations necessary for maintaining privacy and security on these platforms. As the use of social media continues to grow, the integration of advanced technologies and the enforcement of strict privacy regulations are essential for ensuring the protection of users' data and privacy.
Keywords: Data Security; Social Media; Privacy Protection; Encryption: Blockchain Technology; Artificial Intelligence; Biometric Systems; Cybersecurity; GDPR: Data Privacy Regulations.

Introduction

Social media is now not only a platform for communication, but also a major means for business, public and social interactions. In 2025, more than 4.5 billion people use social media to share information, communicate, post and perform other actions. In such conditions, ensuring data security on social media becomes extremely important. Protecting users' personal data and their security requires the use of modern technologies and solutions aimed at protecting them.

Main Part

There are several issues and threats related to the security of social media data. To address these issues, it is important to have a deeper understanding of the types of data and their privacy. Social media data is not only the personal data of users, but also information that can affect public and economic interests.

Data in social networks can be of different types, each of which has its own security measures:

– Personal data: Name, surname, email, phone number, location and other personal data of users. This data indicates the identity of the user, and its protection is one of the most important tasks.

– Geolocation data: Information about the user's location or movements. Geolocation data shows where users are located. Incorrect use of this data may result in loss of privacy of personal data.

– Actions and behavior: Actions, posts, comments, reactions to photos and their social activity. This data can be useful both for the user and for society, but it requires protection from unwanted interference.

– Interaction data: Messages and conversations between users, as well as their posts and comments on platforms. This data is important because it reveals the interactions between users.

Social media data is open to various threats and users face risks related to their identity:

– Fake data and data sharing: Misuse or false use of data can result in people's personal data being misrepresented. For example, creating fake social media accounts to collect information can result in loss of privacy.

– Data theft (cyber attacks): Cyber attacks are one of the most common ways to steal personal data from social media users. In such attacks, the stolen data can be used to gain unauthorized access to user accounts.

– Loss of identity: In social media, a person's identity may be at risk. Users may lose their identity or privacy due to the dissemination of their personal data or wrong actions.

Various technologies and approaches are used to ensure data security in social networks. New technologies strengthen security measures and help protect user data.

Encryption is one of the most important technologies for protecting data on social networks. This method makes data accessible only to authorized users, protecting it from unauthorized use.

– Asymmetric encryption: Two keys (public and private) are used. The private key is stored only by the user, and encrypted data can only be decrypted using the public key.

– Symmetric encryption: One key is used, and the encrypted data is decrypted with the same key. It is a convenient and fast method for protecting data.

Blockchain provides decentralized storage of data in social networks. This technology prevents data from being changed or deleted, giving the user the ability to maintain control over their data.

– Decentralized data storage: IN In a blockchain, data is not stored in one place, but is distributed across several nodes, which reduces the risk of its loss or modification.

Artificial intelligence (AI) and machine learning help analyze user actions on social networks and identify suspicious activities.

– User Behavior Analysis: AI algorithms can detect abnormal user activity and warn of potential threats.

– Threat Prevention: AI technologies can alert you to potential risks in advance and help prevent them.

Biometrics plays an important role in enhancing social network security and user identification. It allows you to grant access to an account only to those users who have passed biometric verification.

– Facial recognition: Biometrics allows you to identify users by their face, limiting account access to authorized individuals only.

– Biometric systems based on fingerprints or other characteristics: Biometrics can be used to improve the security of user accounts.

Legislation and public norms play an important role in ensuring data security on social networks. Different countries adopt laws that help protect user privacy.

The mai laws is General Data Protection Regulation (GDPR). Europe has adopted the GDPR, which gives users full control over their personal data. This law requires social networks to take steps to ensure data security.

In order to ensure data security on social networks, it is important not only to use technology, but also to adhere to ethical standards and social principles. Adopting ethical standards and social norms helps to protect the privacy of users' data.

– Privacy and Public Responsibility: All social media users should have the right to protect their personal information and data, and the ability to control access to it.

Data Security in Social Networks:

– Social networks gather and share various types of data (personal information, posts, photos, geolocation data). This section would explain how this data should be kept confidential and who is responsible for securing it.

– Modern technologies to ensure data security on social networks, such as encryption (end-to-end encryption), and necessary tools to secure communication.

Emerging Solutions:

– Current security methods for keeping users' data private on social networks (masking, data encryption) and their integration with user preferences.

– The importance of new solutions like blockchain technology for ensuring data security on social networks.

Cyberattacks on Social Networks:

– Cyberattacks on social networks and their consequences (external attacks, the use of suspicious programs or phishing attacks).

– How data on social networks and the internet can be compromised, and what security measures need to be implemented to protect it.

Economic, Ethical, and Legal Aspects:

– The economic impact of data security on social networks: How this data creates value in the economy and the need for measures to ensure data quality and security.

– Ethical and legal issues: The protection of personal data in a legal and ethical way, and the importance of regulations that strengthen users privacy rights on social networks.

Intercommunication Systems and Specific Features:

– How communication systems can be improved to manage data security on social networks.

– Expanding the impact of privacy measures and cybersecurity regulations on user experiences in social networks and data security.

Diversity of Data Monitoring Systems:

– Different monitoring methods used to manage data security on social networks, including data analysis, algorithms, and advertisement security.

– Expanding the role of privacy measures in social networks that help users control the privacy level of their interactions.

Future Solutions:

– New solutions for data security in social networks (intelligent algorithms, multi-factor authentication).

– Ensuring the implementation of privacy regulations for various social services, forums, and websites to secure data.

Conclusion

To ensure data security in social networks, it is necessary to use various technologies, laws, ethical standards and public measures. A comprehensive approach using new technologies and solutions allows to protect the identity and data of users in social networks.

References

1. Cavoukian, A., & Dixon, D. (2018). "Privacy by Design: A Counterpoint to the Security-Privacy Debate." International Journal of Information Management, 38(1). 15-21.

2. Zhang, L., & Zhang, Y. (2020). "Data Security and Privacy in Social Media." Journal of Cybersecurity. 16(3). 45-63.

3. Liu, L., & Li, B. (2019). "Privacy Preservation in Social Networks: Techniques and Challenges." Journal of Information Security and Applications, 50. 125-136.

Information about the authors

Tagangylyjov I., Lecturer, Oguz Han Engineering and Technology University of Turkmenistan, i.tagangylyjow@gmail.com, i.tagangylyjov@etut.edu.tm.

Klychev A., Senior lecturer, Oguz Han Engineering and Technology University of Turkmenistan, annamyrat.gylyjov@etut.edu.tm.