IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 17, April 2026
Impact Factor: 8.2

Data Privacy Challenges in Social Media

Agnes John, Fatou A Bah, Devesh Tiwari
Sharda University, Greater Noida

Abstract: *The escalation of social media has changed communication, sharing of the information and online interaction worldwide. Although these platforms offer a lot of benefits, also creates significant risks to user's privacy in data. Users in social media mostly share their personal information like phone contacts, location, photos and opinions, in many instances without fully understanding how collecting, storing and using the data. This study shows the major privacy of data challenges accompanied with social media, which includes unauthorized of data access, identity theft and third-party data sharing. It also analyses, the factors enhancing to privacy violation like lack of inadequate enforcement. The research paper examines technological and legal measures existence to protect user data and emphasis their challenges. In conclusion, recommendations are given to enhance protection of privacy through stronger regulations, improved platform security, and increasing in user education.*

Keywords: Data privacy, social media , Data breach, user awareness, Cybersecurity

I. INTRODUCTION

Social media is now an integral component life, enhancing billions of people to communicate, collaborate and share information abruptly. Platforms like Facebook, Instagram, twitter, Snapchat and Tiktok allow users to share their personal information to the globe. Nevertheless, the accelerated development of these platforms has prolonged serious concerns regarding privacy of data and security. Research reveals that users often reveal critical findings amount of personal data without comprehending the associated privacy risks. [1] identified that sensitive information are shared by many users, underrating the potential fallout of such disclosures. Correspondingly, [6] highlighted that norms privacy differs among users, frequently leading to inconsistent privacy protection behaviors. A further significant challenge is privacy settings complexity. [2] documented that configuration privacy complication frequently results in information unintended data exposure. In addition, applications of third party have been pinpointed as a major source of leaking information, in response to many request excessive permissions apart from their functional requirements [3]. Location-based services also pose significant threats. Chow et al. T41 demonstrated that geotagged posts can reveal sensitive patterns such as home and workplace locations. In addition to the advanced data mining techniques can infer private attributes from publicly available data, increasing the risk of profiling and surveillance [5]. The rise of machine learning technologies has further complicated privacy protection. While privacy-preserving mechanisms such as differential privacy aim to reduce data leakage, they may impact system performance and accuracy [8]. Moreover, identity theft and fake profiles continue to facilitate unauthorized data harvesting and online fraud [10] Although data protection regulations such as GDPR have strengthened user rights, enforcement challenges remain [9]. As a result, social media users continue to face vulnerabilities despite the availability of technical and legal safeguards. Therefore, understanding the existing literature on data privacy challenges is essential to identify gaps and develop stronger protection mechanisms. This study builds upon previous research to analyze the key privacy threats in social media and propose practical solutions to enhance user data protection.

DOI: 10.48175/IJARSCT-34218

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 17, April 2026
Impact Factor: 8.2

II. LITERATURE REVIEW TABLE

S/N	Title of the paper	Name of Author	Techniques used	Tools used	Key findings
[1]	Privacy risks in social networking sites	Gross et al	Statistical analysis, survey methods	SPSS mining tools	Users disclose large amount of personal data unaware of risks.
[2]	Understanding privacy settings	Madejski et al	User behavior analysis	Facebook API, Analytics tools	Complex settings lead to accidental data exposure
[3]	Third-party applications and privacy leakage	Besmer et al	Permission analysis	App auditing tools	Apps collect excessive personal information
[4]	Location privacy in social media	Chow et al	Location obfuscation algorithms	GIS tools, simulation software	Location sharing can reveal home or work patterns
[5]	Data mining andprivacy threats	Aggarwal et al	Data mining profiling algorithms	WEKA Hadoop	Mining techniques can infer sensitive attributes
[6]	Privacy concerns in online social networks	Boyd et al	Qualitative analysis	Survey platforms	Privacy norms vary across demographics
[7]	Cyberbullying and personal data exposure	Patchin et al	Content analysis	Text analysis tools	Public posts enable harassment and misuse
[8]	Machine learning for privacy protection	Shokri et al	Differential privacy, ml models	Python tensor flow	Privacy preserving ml reduces leakage but impacts accuracy
[9]	GDPR Impact on social media privacy	Voigt et al	Legal analysis	Policy analysis tools	Regulations strengthen user rights
					but enforcement
[10]	Anomaly detection algorithms	Brown et al	Anomaly detection algorithms	Network analysis tools	Fake accounts data harvesting and scams

Background

Understanding data privacy in social media requires familiarity with several key concepts. Data privacy refers to the protection of personal information from unauthorized access or misuse. Personal data includes any information that can identify an individual, such as name, email address, location, or contact details. A data breach occurs when confidential information is accessed without authorization, often resulting in serious consequences for users. Encryption is a technique used to secure data by converting it into a coded format that cannot be easily understood without proper

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 17, April 2026 Impact Factor: 8.2

authorization. Anonymization involves removing identifiable information from datasets to protect user identity. Additionally, third-party access refers to external organizations gaining access to user data through applications or services, while tracking technologies such as cookies are used to monitor user behavior online.

Problem Statement

Even if more and more people are using social media, they still have to deal with major data privacy problems such illegal access to their data, sharing it with third parties, identity theft, data breaches, and using their personal information in ways that aren't allowed. A lot of people don't know about privacy settings and platform rules, which can lead to sensitive data being accidentally shared. Current privacy protection systems are often too complicated and not strong enough, which makes it hard for consumers to keep their information safe. Consequently, it is imperative to examine the principal privacy concerns in social media and ascertain viable strategies to enhance user data protection.

Research Objectives

Goals of the Research

- To find the biggest problems with data privacy on social media.
- To look at what causes privacy violations and data abuse.
- To look at how third-party apps affect user privacy.
- To see how well current privacy protection methods work.
- To recommend appropriate measures for enhancing privacy and security.

III. METHODOLOGIES

This research adopts a qualitative and analytical methodology to examine data privacy challenges in social media by utilizing previously published studies and documented evidence. The study primarily relies on secondary data sources, including research papers, journal articles, and case studies referenced in the literature. Foundational work on privacy risks in social networking sites highlights how users unknowingly expose personal information due to weak privacy awareness and platform design [1]. Similarly, studies focusing on user interaction with privacy settings demonstrate that complex configurations often lead to unintended data exposure [2]. A comparative analysis approach is used to evaluate different aspects of data privacy across social media platforms. Research on thirdparty applications reveals that permission-based access systems can lead to excessive data sharing and potential leakage of sensitive information [3]. In addition, location-based privacy risks are analyzed using studies that examine location obfuscation techniques and their limitations in protecting user identity [4]. These comparative insights help identify common vulnerabilities across platforms.

The methodology also incorporates data mining and profiling perspectives to understand how user data is collected and utilized. Prior research indicates that data mining techniques can extract detailed user behavior patterns, which raises concerns about profiling and misuse of personal information [5]. Furthermore, qualitative studies on social networks provide an understanding of user concerns and behavioral patterns related to privacy, emphasizing the role of human factors in data protection [6]. To strengthen the analysis, the study considers emerging threats such as cyberbullying and personal data exposure, which are often linked to inadequate privacy controls and public data sharing [7]. Advanced machine learning-based privacy risks are also examined, particularly focusing on inference attacks that can extract sensitive information from trained models [8]. These findings highlight the evolving nature of privacy threats in modern digital environments. Overall, this methodology integrates insights from multiple studies to provide a comprehensive understanding of data privacy challenges in social media. By combining comparative analysis, behavioral studies, technological evaluation, and regulatory perspectives, the research offers a well-rounded approach to examining privacy risks and identifying effective solutions.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 17, April 2026
Impact Factor: 8.2

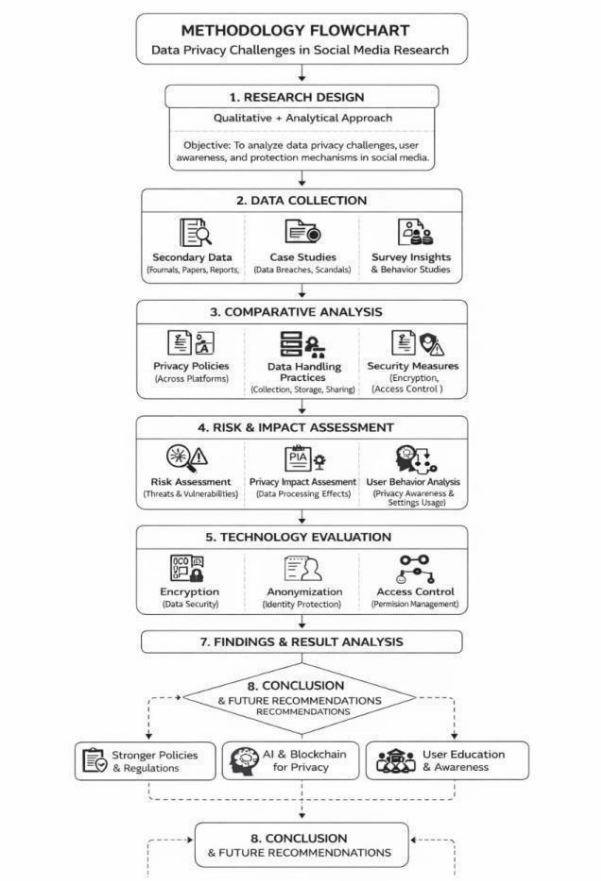

Figure1: Methodology flowchart on data privacy challenges in social media

Problem Statement

Even if more and more people are using social media, they still have to deal with major data privacy problems such illegal access to their data, sharing it with third parties, identity theft, data breaches, and using their personal information in ways that aren't allowed. A lot of people don't know about privacy settings and platform rules, which can lead to sensitive data being accidentally shared. Current privacy protection systems are often too complicated and not strong enough, which makes it hard for consumers to keep their information safe. Consequently, it is imperative to examine the principal privacy concerns in social media and ascertain viable strategies to enhance user data protection.

IV. RESULT ANALYSIS

A thorough examination of data privacy issues on social media sites uncovers several important issues with user knowledge, platform security, third-party access, and technological limits. One of the most important things to note is that users don't know much about privacy rules and settings. A lot of people agree to platform permissions, cookies, and terms of service without fully knowing what they mean. This conduct immediately makes it easier for anyone to see personal information including phone numbers, email addresses, whereabouts, browser history, and private messages.

Another important finding of this study is that third-party apps and advertising are heavily involved in collecting data. To make targeted marketing better, social media sites routinely exchange information about how users use their sites

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 17, April 2026 Impact Factor: 8.2

with marketers, recommendation engines, and outside businesses. But this makes it more likely that people may use data without permission and use personal information for business purposes. The results show that third-party integrations are still one of the weakest links in protecting privacy.

The study also found that the privacy settings on social media sites are often hard to understand and set up correctly for regular users. Because of how complicated it is, a lot of people keep their accounts in public mode by default, which means that their postings, personal information, friend lists, and location information are all open to the public. This unintentional exposure greatly increases the danger of cyber crimes including stalking, identity theft, phishing, and impersonation assaults.

Another thing that the analysis found is that cyberattacks and data breaches on social media sites are on the rise. Attackers often employ weak passwords, reused credentials, unsecured APIs, and software bugs to get to user data. Even if security measures like encryption, secure login systems, and two-factor authentication lower certain risks, they are still not adequate to stop all privacy intrusions.

The paper also talks about how machine learning and data mining might be used to threaten privacy. Advanced algorithms may look at public postings, likes, comments, and browsing patterns to figure out sensitive personal information like hobbies, political views, habits, and even where you live. These technologies can help make things more personal, but they also bring up big moral and privacy issues.

The investigation shows that human factors and technology shortcomings pose virtually the same level of privacy hazards when looked viewed side by side. Not knowing about risks, sharing things carelessly, and not managing passwords well are just as harmful as software bugs and insufficient platform security.

The overall analysis of the results shows that problems with data privacy on social media are caused by a mix of user behavior, weaknesses in the platform's architecture, third-party access, and new cyber dangers. The results clearly suggest the need for easier privacy controls, stronger authentication, AI-based threat detection, and programs that teach users all the time.

Proposed Solutions

To lower the dangers to data privacy on social media, a number of steps may be taken. Privacy settings on social media sites should be made easier to understand and use so that users can quickly choose who may see their personal information. To stop people from getting into accounts they shouldn't, multi-factor authentication should be used more. Data storage and transmission must use strong encryption mechanisms. Third-party apps should only be able to access the data they need. Governments should also make privacy laws stricter and punish people who misuse data more harshly. There should also be initiatives to teach individuals about safe social media use and privacy dangers.

V. FUTURE SCOPE

Future research in the field of data privacy can focus on developing advanced technologies such as artificial intelligence-based privacy protection systems that can automatically detect and prevent data misuse. There is also a need for stronger global data protection regulations that can be uniformly enforced across different countries. Simplifying privacy settings on social media platforms can help users better control their data. Additionally, emerging technologies such as blockchain offer promising solutions for secure data management. Increasing user awareness through educational programs and campaigns will also play a crucial role in addressing privacy challenges in the future. Furthermore, future work can explore the integration of privacy-by-design principles into social media platforms, ensuring that data protection is built into systems from the initial stages of development. Research can also focus on improving transparency through clearer and more user-friendly privacy policies. The development of advanced authentication methods, such as biometric and multi-factor authentication, can further strengthen account security. In addition, continuous monitoring systems and real-time threat detection mechanisms can help in identifying and preventing privacy breaches more effectively.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 17, April 2026
Impact Factor: 8.2

VI. CONCLUSION

In conclusion, data privacy on social media is still a big problem since people share too much information, the privacy settings are too complicated, third parties may get to your information, and cyber risks are on the rise. The research indicates that privacy issues arise from both technology and human elements. Encryption, authentication, and legal rules are some of the existing security measures that offer some protection, although they are not perfect. To make social media safer, we need tighter privacy rules, easier-to-use restrictions, and more people who know how to use them. Future improvements in AI-based privacy protection and privacy-by-design technologies can make data security even stronger.

REFERENCES

[1]. Gross, R., and Acquisti, A., "Privacy Risks in Social Networking Sites," Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, 2005

[2]. Madejski, M., Johnson, M., and Bellovin, S. M., "Understanding Privacy Settings in Facebook," IEEE International Conference on Social Computing, 2012.

[3]. Besmer, A., Watson, J., and Lipford, H. R., "The Impact of Social Navigation on Privacy Policy Configuration," Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2010.

[4]. Chow, R., Golle, P., and Jakobsson, M., "Controlling Data in the Cloud: Privacy in Social Media," Proceedings of the ACM Workshop on Cloud Computing Security, 2009.

[5]. Aggarwal, C. C., "Data Mining and Privacy," Springer, 2015.

[6]. Boyd, D., and Ellison, N. B., "Social Network Sites: Definition, History, and Scholarship," Journal of Computer-Mediated Communication, vol. 13, no. 1, pp. 210–230, 2007.

[7]. Patchin, J. W., and Hinduja, S., "Cyberbullying and Online Harassment: Reconceptualizing the Victimization of Adolescents," Computers in Human Behavior, vol. 24, no. 6, pp. 2773– 2787, 2008.

[8]. Shokri, R., Stronati, M., Song, C., and Shmatikov, V., "Membership Inference Attacks Against Machine Learning Models," IEEE Symposium on Security and Privacy, 2017.

[9]. Voigt, P., and Von demBussche, A., The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer, 2017.

[10]. Brown, B., "Identity Theft and Fake Profiles in Social Media," Journal of Cybersecurity Studies, vol. 5, no. 2, pp. 45–60, 2019.