Scipioneers Journal of Science and Technology (SJST)
|| Website: www.scipioneers.com || Email: research@scipioneers.com || ISSN: 3108-3412 (Online)

The Challenges of Protecting User Data on Social Media and Other Digital Platforms

1st Dr. Farooqui Abdul Samad Gulam Rasool
Radhai Mahavidyalaya, Aurangabad, Maharashtra, India
abdulsamadfarooqui@gmail.com

Abstract:

Social media and digital platforms collect extensive user information, often without adequate transparency or user awareness. While these platforms enable communication and personalized services, they also pose risks such as data breaches, algorithmic profiling, and unauthorized third-party access. This paper examines the key challenges in protecting user data using a descriptive, secondary-data-based methodology. Findings indicate weaknesses in governance, cybersecurity, regulatory enforcement, and user practices. Recommendations highlight the need for strengthened governance, ethical AI, user education, and improved global data protection mechanisms.

Keywords: Social media, Privacy, Data protection, GDPR.

I. INTRODUCTION

Social media and digital platforms are now integral to daily life, with over 4.9 billion active users contributing personal data including demographic details, behavioural patterns, and geolocation information [1]. The economic structure of such platforms relies heavily on data monetization through targeted advertising and predictive analytics, resulting in extensive data harvesting practices [2]. However, the rapid development of data-driven ecosystems has created substantial concerns regarding privacy, surveillance, and data misuse. Many users remain unaware of how much data platforms collect or how their information is shared with advertisers and third-party entities. Incidents such as the Cambridge Analytica scandal have demonstrated the large-scale consequences of weak data governance and insufficient oversight mechanisms [6]. The rise of artificial intelligence (AI) and machine learning (ML) has further exacerbated privacy concerns. These technologies infer sensitive characteristics such as political beliefs, health status, and personality traits—even when such details are not explicitly provided—raising ethical issues related to discrimination and manipulation [7]. Governments have introduced legal frameworks such as the General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act to improve privacy protections. However, enforcement remains inconsistent due to cross-border data flows and jurisdictional conflicts [3]. Given these issues, a systematic analysis is required to understand the multifaceted challenges of protecting user data on digital platforms.

II. LITERATURE REVIEW

Studies emphasize that social media platforms are architected for large-scale data collection, including metadata such as device identifiers, session duration, and browsing behaviour [4]. Morris [5] highlights that privacy policies are often excessively long and complex, limiting user comprehension and resulting in uninformed consent. Research on data breaches indicates that platforms remain prime targets for cyberattacks due to high-value datasets and inadequate cybersecurity practices, including weak encryption and insecure APIs [8]. Case studies of major breaches demonstrate recurring vulnerabilities in platform infrastructure and insufficient monitoring.

Another critical area involves third-party data sharing. Johnson and Lee [2] note that advertising networks and external developers frequently access user data via APIs, often without clear disclosure to users. This opaque ecosystem creates significant accountability gaps. AI and ML technologies pose additional risks. Zhou et al. [4] report that algorithms can infer sensitive personal information from seemingly harmless signals, while Chen [7] demonstrates how predictive models contribute to privacy erosion.

Regulatory research indicates that even strong frameworks like GDPR face enforcement challenges due to global operations of digital firms [9]. Kumar [3] asserts that regulatory fragmentation allows platforms to exploit loopholes, reducing the effectiveness of privacy laws. Overall, existing research identifies technological complexity, poor transparency, weak governance, and fragmented regulation as core contributors to user data vulnerabilities.

III. METHODOLOGY

The study employs a descriptive and analytical methodology based on secondary data sources**,** including journal articles, regulatory documents, cybersecurity analyses, and platform policy reviews. Thematic analysis is used to categorize recurring issues such as data breaches, consent problems, algorithmic profiling, and regulatory gaps.

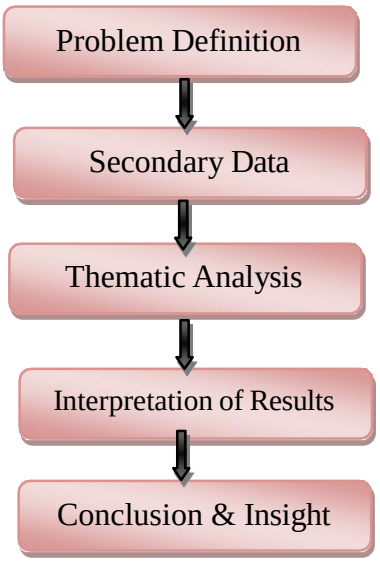

Fig. 1 Methodology Flow Diagram

Protecting user data on social media and digital platforms is a critical concern in today's online world. These platforms collect large amounts of personal information such as location, preferences, and communication details, which increases the risk of misuse and privacy violations. Many companies use this data for advertising and business purposes without clearly informing users. At the same time, users often do not fully understand privacy settings or the consequences of sharing personal details online. Cyberattacks, data breaches, and unauthorized access by third-party applications make the situation even more challenging. Furthermore, laws and regulations designed to protect user privacy are often outdated and unable to keep up with fast-developing technology. As a result, social media companies have more power and control over data than the users who own it. To ensure better protection, there is a strong need for stricter data privacy laws, improved cybersecurity measures, transparent data-handling practices, and increased user awareness. Working together, governments, platforms, and users can create a safer digital environment where personal data remains secure.

IV. DISCUSSION AND RESULTS

The thematic analysis identified seven major categories of challenges that critically influence user data protection on social media and digital platforms. These results show that the vulnerabilities arise from a combination of platform policies, technological weaknesses, user practices, and legal inefficiencies.

Firstly, weak governance and consent structures make it difficult for users to provide informed consent. Privacy policies often contain overly complex or ambiguous wording, which limits transparency and leads to automatic acceptance without genuine understanding of data implications [10].

The rise in data breaches reflects shortcomings in cybersecurity protocols across platforms. Many systems continue to rely on outdated encryption, insecure APIs, and inadequate monitoring mechanisms, enabling frequent and large-scale cyberattacks [11].

Additionally, opaque third-party sharing practices create further risks. Platforms share data with advertisers and external service providers in ways that often remain hidden from users, reducing their ability to control how their data is used beyond initial collection. Algorithmic profiling intensifies privacy concerns by inferring sensitive personal traits such as emotions, political preferences, and behavioural tendencies. This information may be exploited for manipulative advertising, political targeting, and potentially discriminatory outcomes [12].

Even where legal structures are in place, regulatory and enforcement gaps persist. Cross-border data flows and fragmented jurisdictional authority weaken implementation of privacy rights and restrict enforcement capabilities across regions [13].

Lastly, user behaviour continues to pose a significant security challenge. Oversharing of personal information, weak password practices, and a general lack of digital literacy make users more susceptible to privacy violations and cybercrime.

V. CONCLUSION

This study reveals that safeguarding user data on social media and digital platforms is an evolving challenge shaped by complex technological systems, opaque data-processing practices, and inconsistent regulatory environments. Despite the introduction of strong privacy laws such as GDPR, enforcement remains inconsistent and fragmented across borders. Major privacy risks on digital platforms arise from weak data governance, frequent security breaches, opaque third-party sharing, and increasing algorithmic profiling. Addressing these challenges requires transparent data practices, stronger cybersecurity, unified global regulations, ethical AI standards, and improved user awareness to ensure a safer and more privacy-focused digital environment. Comprehensive reforms across technical, legal, and social dimensions are essential to building trust and protecting user data in digital ecosystems.

VI. REFERENCES

[1] A. Smith, “Digital privacy in the age of social media,” *Journal of Cyber Policy*, vol. 5, no. 2, pp. 45–57, 2022.

[2] L. Johnson and H. Lee, “User data exploitation on major digital platforms,” *International Review of Information Security*, vol. 12, no. 3, pp. 112–128, 2021.

[3] P. Kumar, “Global data protection laws and compliance challenges,” *Data Governance Review*, vol. 4, no. 1, pp. 20–34, 2023.

[4] W. Zhou, S. Khan, and R. Li, “Profiling and privacy risks in AI-driven platforms,” *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2890–2904, 2020.

[5] R. Morris, “Consent fatigue and privacy policy complexity,” *Digital Ethics Quarterly*, vol. 6, no. 1, pp. 77–89, 2021.

[6] M. Green and S. Patel, “Social media scandals and policy reform,” *Media Law Review*, vol. 9, no. 2, pp. 98–113, 2022.
[7] L. Chen, “Algorithmic risks and predictive privacy violations,” *AI & Society*, vol. 38, pp. 601–612, 2023.
[8] J. Almeida, K. Faria, and D. Santos, “Cyber vulnerabilities in online platforms,” *Cybersecurity Journal*, vol. 11, pp. 51–65, 2020.
[9] K. Rao and A. Singh, “Cross-border data protection challenges,” *Int. J. Law Technol.*, vol. 14, no. 4, pp. 233–248, 2021.
[10] E. Blythe and K. Wright, “Privacy policies and user comprehension: A systematic review,” *Journal of Cyber Policy*, vol. 7, no. 1, pp. 45–61, 2022.
[11] IBM Security, “Cost of data breach report,” *IBM Research Publication*, 2024.
[12] S. Zuboff, *The Age of Surveillance Capitalism*. New York, NY, USA: PublicAffairs, 2019.
[13] European Commission, “GDPR enforcement and compliance gaps,” *EU Data Protection Report*, 2023.