

ML-BASED ANALYTICAL STUDY ON THE LEVEL OF SECURITY OF USER DATA ON SOCIAL MEDIA WEBSITE

Syed Muqadir Hussain Shah¹, Khalid Hamid², Muhammad Danish Rasheed³,
Muhammad Ashraf Nazir⁴, Muhammad Waseem Iqbal⁵, Fareeha Zafar⁶,
Muhammad Ibrar⁷, Muaaz Akhter⁸

¹Department of Computer Science, University of Engineering and Technology Lahore, Lahore, 54000, Pakistan

²Department of Computer Science and Information Technology, Superior University Lahore, Lahore, 54000, Pakistan

³Department of Information Technology, Berkeley City College, USA

⁴Department of Computer Science, Government College University Lahore, Lahore, 54000, Pakistan

⁵Department of Information Technology, Superior University Lahore, Lahore, 54000, Pakistan

⁶Department of Computer Science, Government College University Lahore, Lahore, 54000, Pakistan

⁷Department of Computer and Mathematical Sciences, New Mexico Highlands University, Las Vegas, NM

⁸Department of Computer Science, Arid Agriculture University, Rawalpindi, Pakistan

¹muqadirhussainshah@gmail.com, ²khalid6140@gmail.com, ³mdanishrasheed.77@gmail.com,

⁴ashnaz.gcu.edu@gmail.com, ⁵waseem.iqbal@superior.edu.pk, ⁶Dr.F.zafar@gcu.edu.pk,

⁷Mibrar@live.nmhu.edu, ⁸muaaz.aradianz123@gmail.com

Corresponding Author: *

Khalid Hamid

DOI: <https://doi.org/10.5281/zenodo.17614882>

Received	Accepted	Published
11 September 2025	21 October 2025	04 November 2025

ABSTRACT

The fast development of social media sites has transformed the way people interact and share information, yet it has also created massive concerns regarding the safety of user data. As social media users share personal data daily (in billions), social media companies have the responsibility of ensuring this information is not hacked, accessed by unauthorized individuals, or used in different ways. This paper looks at the present condition of the security of user data on the largest social media sites, the efficiency of the security measures that can be applied, the most frequently observed types of vulnerabilities, and the contribution of user behavior to data compromise. The study examines the extent to which social media platforms enhance the safety of sensitive information through a general assessment of security measures, case studies of data breaches, and user surveys and indicates aspects where social media could be deficient in security. Another aspect that the research covers is the trade-off in the safeguarding of data and the functionality of the platform, whether the existing regulations and self-enforced security standards are adequate. The results provide an indication that although certain progress has been made, the challenges of ensuring strong data protection still exist. The paper ends with a conclusion based on some recommendations on how to improve data security on social media, such as enhanced user awareness, enhanced encryption, and stricter regulatory control measures.

Keywords: User data, security level, behavior, awareness, control measures, social media.

INTRODUCTION

Due to the emergence of social media, billions of users now post their personal details, preferences and activities they engage in on a daily basis online. These systems have become part of the communication, entertainment, and commerce systems and have created more connectivity than ever before. Nonetheless, this widespread exposure to personal information is a major concern for privacy and security. The social media sites gather, retain, and in most cases sell user information to third parties to advertise and provide personalized information to them. This has unfortunately enhanced more vulnerabilities and the user data has been exposed to cyberattacks, unauthorized access and data breaches [1][2].

There are several case studies in the news involving high-profile events like the Cambridge Analytica scandal and the data breaches on platforms like Facebook, which have put the safety of user information into the limelight [3]. These violations not only jeopardize the privacy of the users but also the confidence of social media sites. Although companies have put efforts in order to enhance security and adhere to the data protection laws, there is a question whether their measures are effective overall. The problem of users being threatened persists because hackers are using more advanced techniques to gain access to personal data, and users can easily share sensitive information through their online activities without noticing [4][5].

This research will focus on reviewing the state of security of user information on social media in the present day. The research aims to measure the effectiveness of social media companies in the protection of user information, as well as the additional efforts that are required to guarantee the privacy of data in a more connected digital environment by studying the currently practiced security procedures, possible threats, and awareness of the users [6][7]. The results of this study should be used to advance the current debate on the issue of data protection and educate users and developers of platforms on the severe consequences of the lack of personal information protection on the Internet [8].

Literature Review

In 2022, the image-sharing social media app Instagram saw over 500 million downloads, while a newer platform, BeReal, garnered nearly 100 million downloads (Ceci, 2023). For users of these platforms, this wealth of data reveals our daily routines (behaviors), tracks our online preferences (psychographics), captures our browsing and shopping patterns (webographics), and observes our social connections with family and friends (demographics) [9][10]. Additionally, this extensive data can be integrated into data lakes for analysis, user profiling, and sold to interested third parties. Due to the lack of sufficient self-regulation, legislation has been enacted in most countries, requiring informed consent for collecting online data. However, many users are faced with lengthy explanations and often do not read the policies before giving their consent [11][12]. Warren and Brandeis explored the unauthorized use of personal images and advocated for the "right of the individual to be let alone." Later research focused on the misuse of customer data within technology, highlighting concerns about secondary data usage, where individuals were deprived of agency and autonomy over how and where their data was collected [13][14]. Although gathering data from third parties was legally permissible, it was seen as crossing a privacy boundary, as neither "implied nor explicit consent" was given [15][16].

Digital foot printing refers to the process of gathering data based on an individual's trackable digital activities and online presence [17][18]. Digital footprints are the key tool for monitoring online activities, communications, and actions that result from frequent internet use [19]. According to data from 2021, there were approximately 1,637,973,022 cyberattacks targeting Indonesia. These included 122,435,215 malware activities, 16,939 website incidents, 2,885 incident reports from the public, and 1,872 security information gaps [20]. The report also highlighted that, in addition to being a target of cyber-attacks, Indonesia was one of the largest sources of such attacks [21]. Site hacking involves attempts by attackers to gain unauthorized access to a website, either by exploiting valid accounts or

vulnerabilities within the site. Once access is obtained, attackers can engage in malicious activities [22]. Common objectives of site hacking include altering the site's appearance (defacement), extracting data from the victim's server, and encrypting the site to disrupt its functionality [23].

On social media, some private data is shared by users either unknowingly or voluntarily. In some cases, private information, beyond what users intentionally share, is extracted by offering incentives. Through Location-Based Social Network Services (LBSNS) such as FireEagle, Google Latitude, and nearby, it is possible to identify a person's location, as well as the locations of their friends [24]. From the privacy analytics perspective, certain factors determine the benefits and risks that influence a user's decision to disclose personal information [25]. It also suggests that individuals are sometimes willing to compromise some level of privacy if the perceived risk is acceptable. By using Social Networking Sites, people expose themselves to various risks, which often result in breaches of their privacy [26]. This study is all about checking out how people use social media and what they know about acting right online they surveyed 250 folks using a questionnaire online to find out about their social media habits and what they understand about digital ethics the survey looked at things like demographics what people know about online ethics and how they view ethics on the social media platforms they use most people knew about the laws and rules for online behavior but some were unsure or did not know much when it came to how people see digital ethics most had a positive

view but few had a negative take on it cool to see how people think about being good digital citizens [27].

This is study about how to make social media safer by using big data its like they are trying to find ways to make sure social media is more secure they looked at what other people have already said about how to keep social media safe they came up with some ideas for government to handle security on social media some places don't have very good rules for keeping social media secure the study gives suggestions on how to deal with safety issues on social media they mentioned that more work is needed to come up with better safety plans for Indonesia [28].

This is study about to comparing data security and privacy on instagram and twitter they analyzed 25 journal articles from trusted sources to determine which platform excels in safeguarding user information instagram outperformed twitter in some security aspects yet both face vulnerabilities like phishing attacks the study emphasizes individual vigilance and employing security measures such as two factor authentication for enhanced protection it underscores the need for continuous efforts to enhance data security on social media platforms for the benefit of all users [29].

Methodology

The proposed study will assess the extent of safety of user information in social media sites through both qualitative and quantitative research. The approach will interview its users, experts, and conduct a technical study of the data protection frameworks utilized by the social media [30].

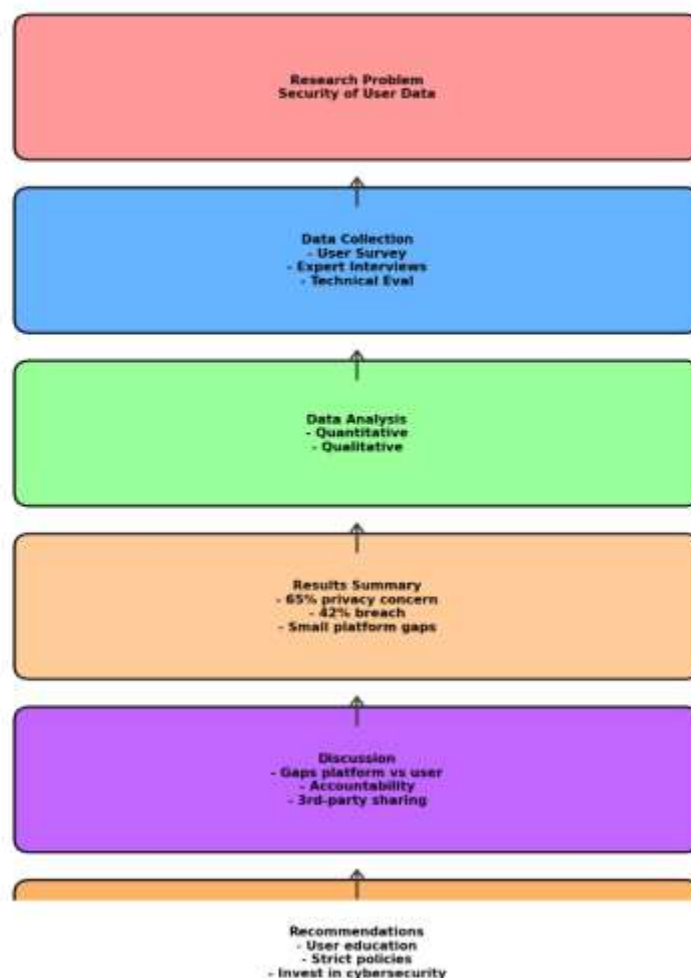


Figure 1: Research Methodology
Research Design

The study is a mixed-method study, as it combines a user survey, interviews with experts, and technical analysis to evaluate the level of data safety in a holistic manner. This is a multi-dimensional treatment that guarantees that subjective user experiences and objective technical findings are factored in [31].

Data Collection

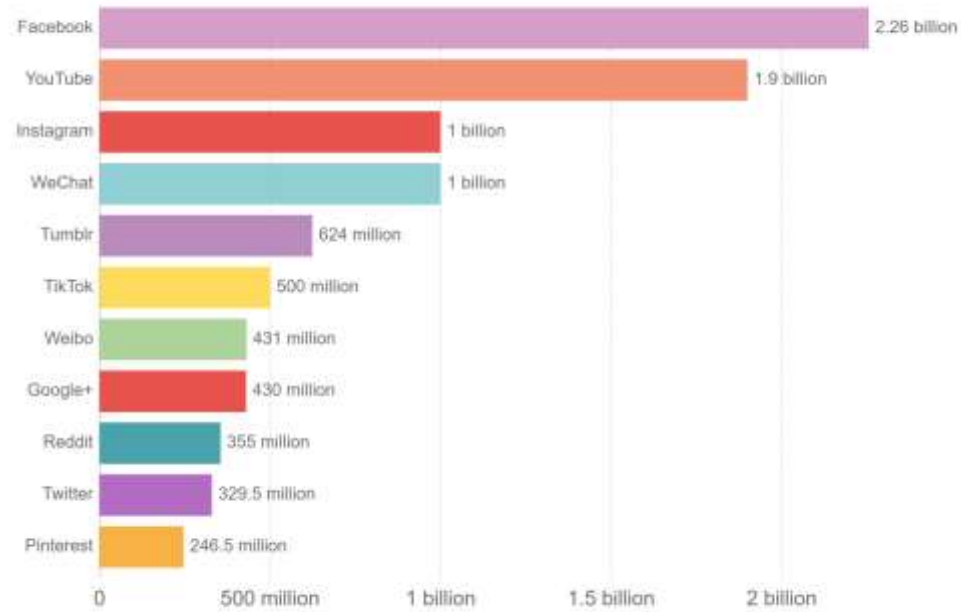
Surveys

According to different surveys, data is collected related to this topic and through this data, it can be analyzed that the percentage of users on these sites is increasing rapidly and their data security is a big threat and challenge [32]. The following chart shows the no of users on different social media sites [33].

Number of people using social media platforms, 2018

Estimates correspond to monthly active users (MAUs). Facebook, for example, measures MAUs as users that have logged in during the past 30 days. See source for more details.

Our World
in Data



Source: Statista and TNW (2019)

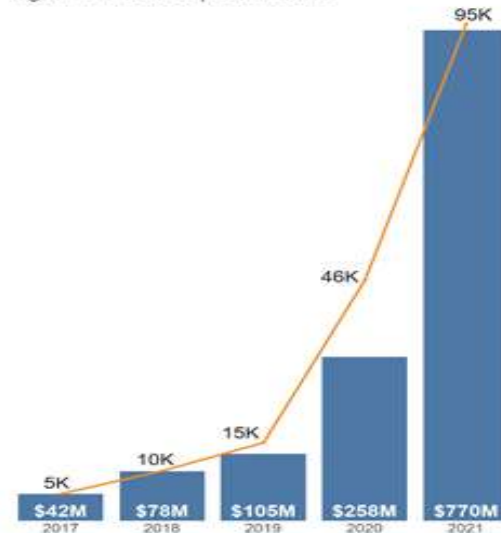
CC BY

Figure 2: Social Media Usage [34][35][36]

The following chart shows the number of frauds and how they have increased over the years.

Reports about fraud originating on social media soared over five years

2021 total reported losses were about 18 times what they were in 2017, and the number of people who reported losing money in 2021 grew to 19 times higher than those reports in 2017.



Figures based on fraud reports directly to the FTC indicating a monetary loss and identifying social media as the method of contact.

Figure 3: Frauds on Social Media [34][35][36]

The following chart shows the fraud in terms of loss in millions of dollars over the years from 2017 to 2021 in Fig. 3.

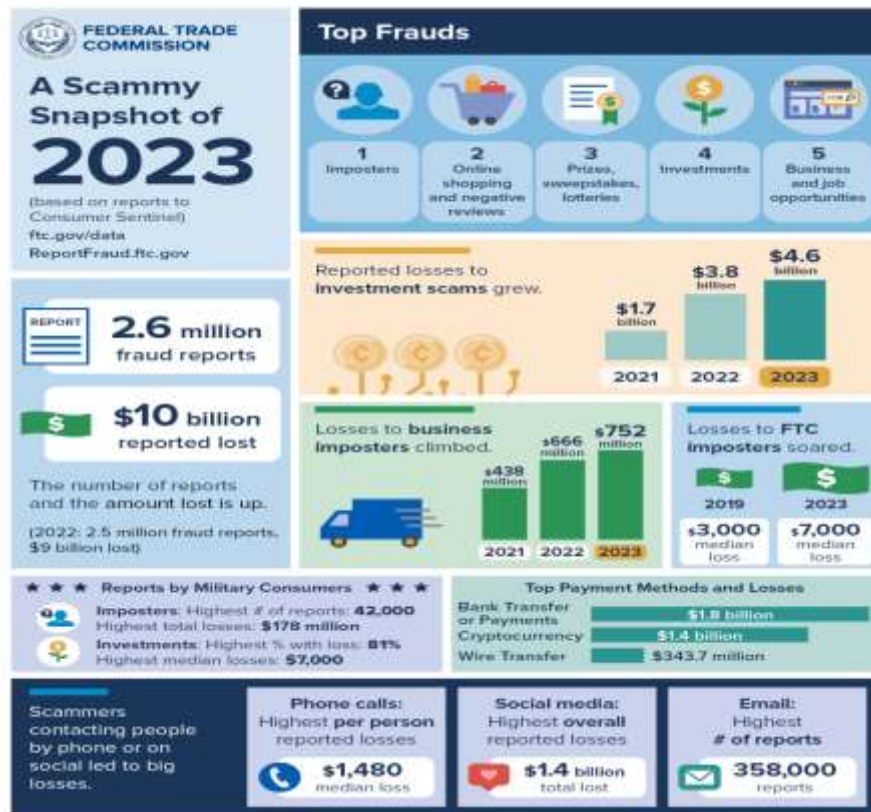


Figure 4: Latest Frauds Report on Social Media [36][37][38]

The following chart shows the fraud or scams of different types in terms of loss in millions of dollars and categories over the years from 2017 to 2021 in Figure 4.

Secondary Data Collection

As mentioned in the literature review above, multiple fraud cases have been reported over time and these cases have become bigger and bigger as the no of users on these sites has increased rapidly, while the level of security of data is lacking and the data of the users is becoming in insecure with time [39].

Results and Discussion

The study reveals critical insights into the level of security of user data on social media platforms, based on user perspectives, expert analysis, and technical evaluations.

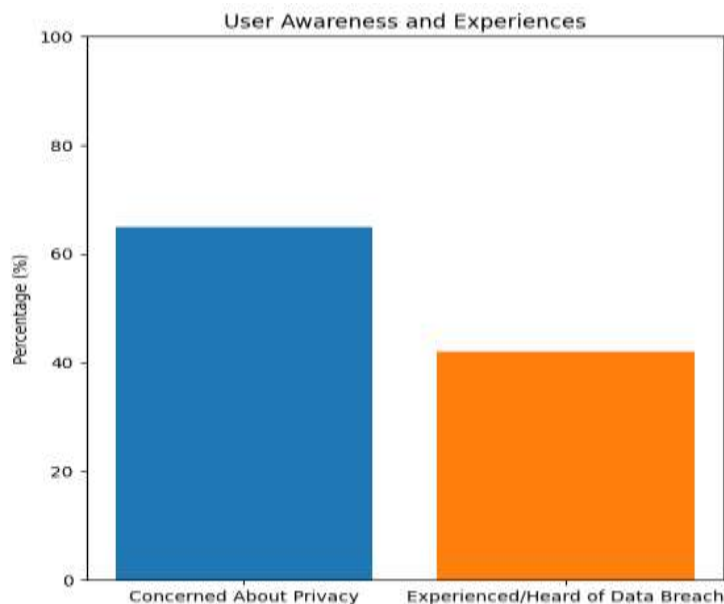


Figure 5: User Perception Regarding Privacy

Fig. 5 shows that more than 60% concerned about privacy and almost 40% just heard about a data breach but are not really concerned about it.

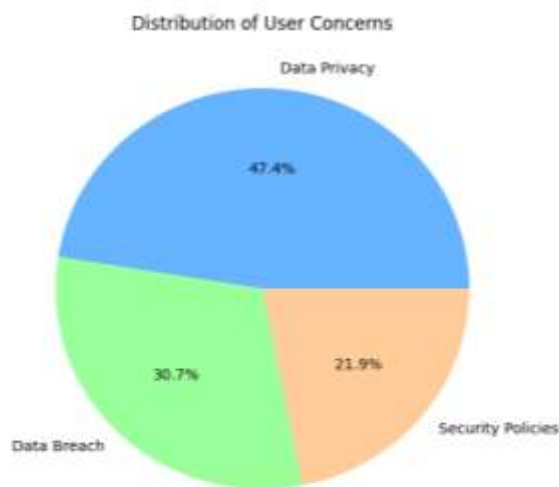


Figure 6: Users' Concerns Regarding Security, Privacy and their Breach

Fig. 6 shows user concerns in which data privacy of users has the highest priority, then data breach and at the end, security policies.

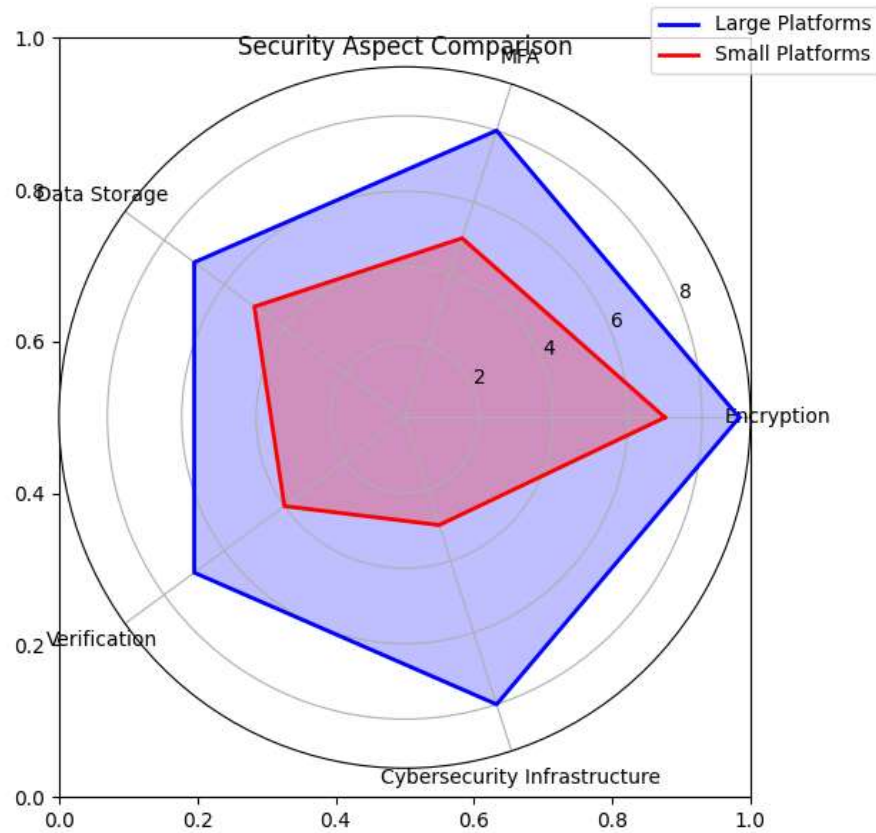


Figure 7: Comparison of Security Aspects

Fig. 7 represents the comparison of security aspects as cybersecurity infrastructure, verification, encryption, MFA and data storage in small platforms and large platforms.

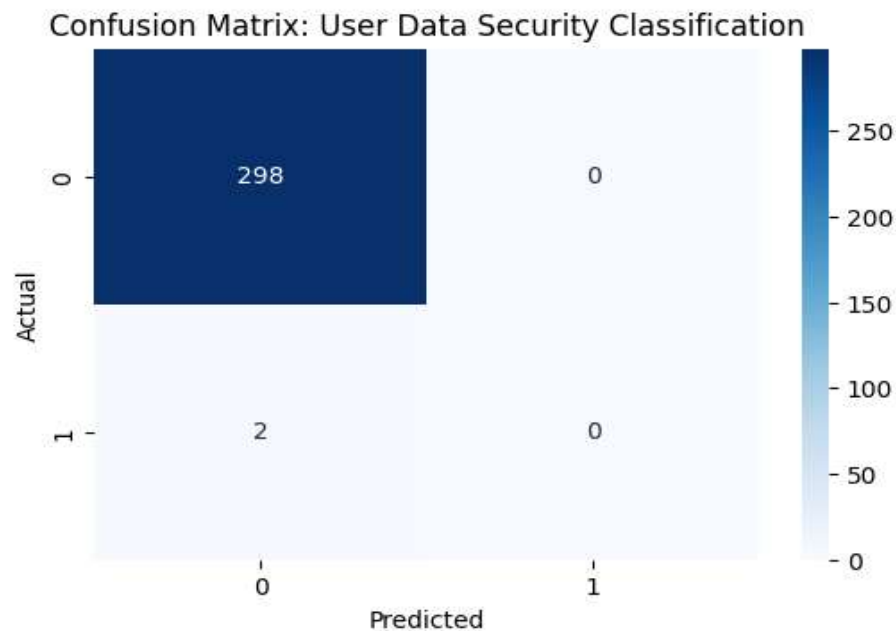


Figure 8: User Data Security Classification

Fig. 8 represents the user data security classification with predicted and actual levels of security.

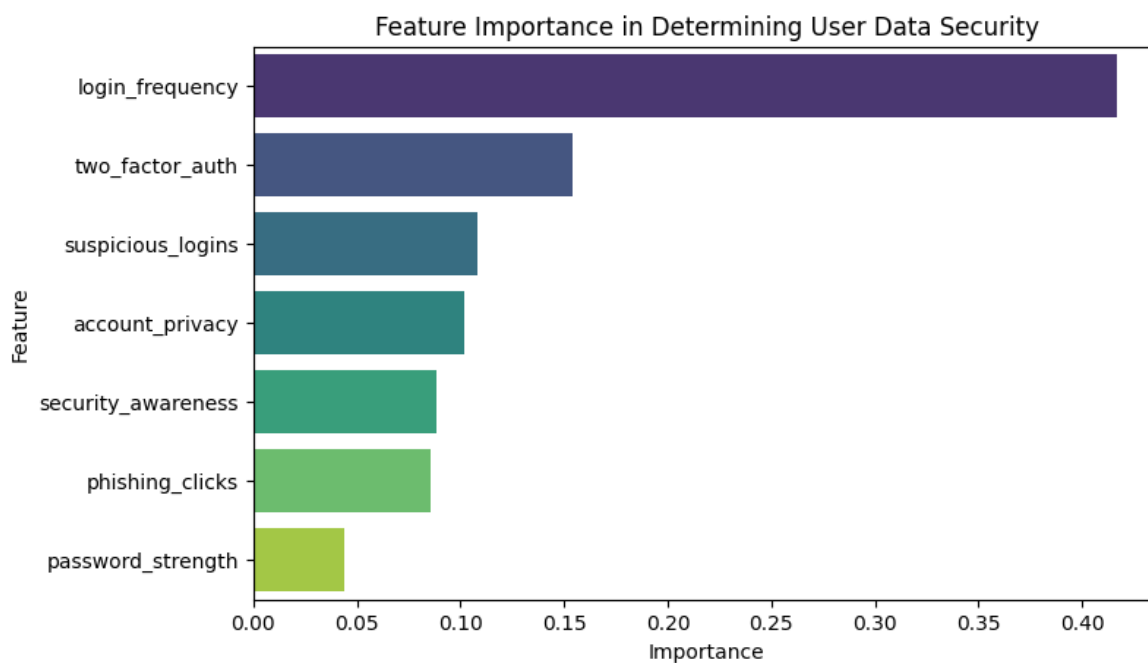


Figure 9: Features Important in Determining User-level Data Security

Fig. 9 represents and involved features that determine user-level data security, including password strength, phishing clicks, security awareness, account privacy, suspicious logins, two-factor authentication and login frequency, with their importance.

Based on the results and survey, the study proposed a framework—

Proposed Layered-Framework



Figure 10: Layered Framework as Proposed Model

Fig. 8 represents the proposed layered framework with the exact flow that how to secure the user data with different security levels involved.

User Awareness and Perceptions.

One of the most important concerns of the users (65 percent) was the privacy of data, but they admitted that they knew little about the security policies of the specified platforms. About 42 percent of the respondents had suffered a data breach or unauthorized use of data or heard about it.

Expert Insights

Analysts pointed out encryption, multi-factor authentication (MFA) and periodic updates to security measures as the most important actions that platforms take to keep the user data safe. Nonetheless, some fundamental weaknesses were also noted by them, including lax data-sharing policies with third parties and vulnerability to phishing.

Technical Analysis

Platforms showed strong encryption in their data transmission, but differed considerably in the

policy of data storage and retention. Some platforms had loopholes in the system used to verify users and their accounts could easily be accessed by unauthorized users. It was also noted that the smaller platforms were usually under-equipped in cybersecurity infrastructure and were therefore easy targets for attackers.

Discussion

The results highlight a lack of correlation between the sturdy actions alleged by platforms and user experiences of data security. Although bigger platforms invest in cutting-edge security solutions, the issues are still present in the fields of user education, open data-sharing policies, and immediate breach messages.

Accountability and Responsibility of the User and Platform

1. The use of MFA is among the basic security measures that a lot of users never practice, which leads to the vulnerability of data.
2. At the same time, platforms should focus on the introduction of user-friendly interfaces to promote the use of security options.

Third-Party Data Sharing

Another theme that reappeared continuously was the inability to have user control over the shared data with third parties. More transparent and visible policies will be the key to restoring the confidence of the users.

Smaller Platforms and Resources Limitations

Smaller social media should invest in the foundational protection of cybersecurity and follow best practices in the industry to secure the data of users.

Recommendations

- Increase user education awareness to increase awareness of security features and best practices.
- Implement more stringent data-sharing policies with third parties.
- Promote the investment in security improvements, especially on minor platforms, to establish a safer online space.

The discussion illustrates the complexity of the data security of social media, which requires

concerted efforts of users, platforms, and regulatory authorities to close the gaps identified.

Conclusion

The research identifies the issues and difficulties of guaranteeing the safety of user data on social media. As much as technological innovation has allowed platforms to adopt the advanced security procedures in the form of encryption, multi-factor authentication and periodic updates, there are still sizable loopholes. These comprise the weaknesses in the third-party data sharing, lack of user awareness, and lesser security measures on smaller platforms. Although it is the duty of users to safeguard their data by following the best security practices, platforms should assume more responsibility by offering clear policies, convenient tools, and proactive actions to ensure the protection of user data. Regulators also play a very important role in setting and implementing a standard of data privacy/security in the industry. To solve the mentioned problems, it will be necessary to make a joint effort between social media sites, users, and policymakers to create a secure, trusted, and privacy-aware digital environment. Since social media sites can eliminate the gaps in existing practices and policies, they will be able to increase user confidence and guarantee stronger protection of personal information in the world, which is becoming more connected.

References

- [1] L. Ceci, "Most Downloaded Social Media Apps Worldwide 2022," Statista, 2023. [Online]. Available: <https://www.statista.com/statistics/1284900/top-social-media-apps-worldwide-by-downloads/>
- [2] B. Nguyen, F. Jaber, and L. Simkin, "A systematic review of the dark side of CRM: The need for a new research agenda," *Journal of Strategic Marketing*, vol. 30, no. 1, pp. 93–111, 2022, doi: 10.1080/0965254X.2019.1642939.
- [3] B. Custers, S. van der Hof, and B. Schermer, "Privacy expectations of social media users: The role of informed consent in privacy policies," *Policy & Internet*, vol. 6, no. 3,

- pp. 268–295, 2014, doi: 10.1002/1944-2866.POI366.
- [4] J. A. Obar and A. Oeldorf-Hirsch, “The biggest lie on the internet: Ignoring the privacy policies and terms of service,” 2020.
- [5] J. A. Obar and A. Oeldorf-Hirsch, “The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services,” *Information, Communication & Society*, vol. 23, no. 1, pp. 128–147, 2020, doi: 10.1080/1369118X.2018.1486870.
- [6] S. D. Warren and L. D. Brandeis, “The right to privacy,” *Harvard Law Review*, vol. 4, no. 5, pp. 193–220, 1890, doi: 10.2307/1321160.
- [7] M. J. Culnan, ““How did they get my name?: An exploratory investigation of consumer attitudes toward secondary information use,” *MIS Quarterly*, vol. 17, no. 3, pp. 341–361, 1993, doi: 10.2307/249775.
- [8] M. Micheli, C. Lutz, and M. Büchi, “Digital footprints: An emerging dimension of digital inequality,” *Journal of Information, Communication and Ethics in Society*, vol. 16, no. 3, pp. 242–251, 2018, doi: 10.1108/JICES-02-2018-0014.
- [9] M. P. Priya, M. K. Devi, S. U. Kamali, S. Akshayaa, and P. R. Amutha, “Personality prediction using digital footprints to analyze kids’ activities,” in *Proc. 2020 Int. Conf. Power, Energy, Control and Transmission Systems (ICPECTS)*, 2020, pp. 1–3, doi: 10.1109/ICPECTS49113.2020.9337056.
- [10] Badan Siber dan Sandi Negara, *Laporan Tahunan Monitoring Keamanan Siber 2*, pp. 54–55, 2022. [Online]. Available: <https://cloud.bssn.go.id/s/Lyw8E4LxwNiJoNw>
- [11] A. M. Delshadi, O. Ullah, Y. Khan, M. W. Iqbal, H. A. B. Muhammad, K. Hamid, F. Abbas, and M. Ibrar, “Empowerment of Artificial Intelligence (AI) in preventing and detecting ransomware: an analytical review,” *Spectrum of Engineering Sciences*, vol. 3, no. 9, pp. 36–48, Sept. 2025.
- [12] J. Keshavelal, M. Fahad, I. F. Nawaz, M. U. Qayyum, K. Hamid, Z. Nazir, M. Ibrar, and H. A. B. Muhammad, “Embedding Artificial Intelligence in Games NPC and effects on emotional health,” *Spectrum of Engineering Sciences*, vol. 3, no. 8, pp. 1032–1042, Aug. 2025..
- [13] A. M. Delshadi, M. M. Aziz, M. U. Qayyum, M. W. Iqbal, K. Hamid, F. Abbas, H. Liaqat, and M. Ibrar, “AI-based fake login attempt detection system using behavioral analytics,” *Spectrum of Engineering Sciences*, vol. 3, no. 8, pp. 1043–1056, Aug. 2025.
- [14] Y. Usman, A. Khan, K. Hamid, M. W. Iqbal, and M. Ibrar, “Visually Impaired People Empowered by Deploying CNN-Based System on Low- Power Wearable Platforms,” *Journal of Computing & Biomedical Informatics*, vol. 09, Aug. 2025.
- [15] H. Ali, D. Younas, K. Hamid, M. Noor, and M. Ibrar, “Human-Centered Comparable to Technology-Driven Approaches in Reducing the Bullwhip Effect: A Cross-Industry Study,” *Annual Methodological Archive Research Review*, vol. 3, no. 8, pp. 209–248, Aug. 2025
- [16] I. Ahmad, M. Amin, K. Hamid, S. Rizwan, and S. Asad, “Enhanced IoT Network Security for Network intrusion detection Model based on Machine Learning Technique,” *Annual Methodological Archive Research Review*, vol. 3, pp. 188–212, Aug. 2025, doi: 10.63075/0vcg0093.
- [17] I. F. Nawaz et al., “AI and Digital Distraction: Impact of Smart Technologies on Time and Health Management,” *Annual Methodological Archive Research Review*, vol. 3, no. 6, pp. 129–149, 2025.
- [18] K. Hamid et al., “Empowering Robust Security Measures in Node. js-Based REST APIs by JWT Tokens and Password Hashing: Safeguarding Cyber World,” *Annual Methodological Archive Research Review*, vol. 3, no. 5, pp. 379–393, 2025.
- [19] M. Danish et al., “Security of Next-Generation Networks: A Hybrid Approach Using ML-Algorithm and Game Theory with SDWSN,” *Annual Methodological Archive Research Review*, vol. 3, no. 4, pp. 18–36, Apr. 2025, doi: 10.63075/wdpwrr31.

- [20] M. W. Iqbal, K. Hamid, M. Ibrar, and A. Delshadi, "Meta-analysis and investigation of usability attributes for evaluating operating systems," *Migration Letters*, vol. 21, no. 5, pp. 1363–1380, 2024.
- [21] N. A. Malik et al., "Behavior and Characteristics of Ransomware-A Survey," in *2024 2nd International Conference on Cyber Resilience (ICCR)*, IEEE, 2024, pp. 01–05. Accessed: Oct. 15, 2025. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/10532983/>
- [22] K. Khaliq, N. Z. Ab Rahim, K. Hamid, M. Ibrar, U. Ahmad, and M. U. Ullah, "Ransomware Attacks: Tools and Techniques for Detection," in *2024 2nd International Conference on Cyber Resilience (ICCR)*, IEEE, 2024, pp. 1–5. Accessed: Oct. 15, 2025. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/10532926/>
- [23] I. Aslam, W. Tariq, T. Waheed, K. Hamid, S. M. Rizwan, and A. Ahmed, "Enhancing Privacy and Security in Multi-Party Computation for Data Mining in Cryptographically Protected Environments," *Annual Methodological Archive Research Review*, vol. 3, pp. 510–531, 2025
- [24] A. Tahir, K. Hamid, A. Kahloon, and S. Zubair, "Cyber Sovereignty Challenges: A Strategic Framework For National Data Protection Using Blockchain Authentication," *Contemporary Journal of Social Science Review*, vol. 3, no. 3, pp. 1314–1328, 2025
- [25] P. Lowry, J. Cao, and A. Everard, "Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures," *Journal of Management Information Systems*, vol. 27, no. 4, pp. 163–200, 2011.
- [26] P. Van Eecke and M. Truyens, "Privacy and social networks," *Computer Law & Security Review*, vol. 26, no. 5, pp. 535–546, 2010.
- [27] M. H. Akhtar, T. Jabeen, R. Aziz, M. N. Amin, S. M. Rizwan, and K. Hamid, "Intelligence based Self-Healing Network Design: An Automated Incident Response System for Troubleshooting of IoT Security Breaches," *Annual Methodological Archive Research Review*, vol. 3, no. 8, Aug. 2025, doi: 10.63075/6dhhj119.
- [28] A. Rauf and K. Hamid, "COMPARATIVE STUDY OF REQUIREMENTS PRIORITIZATION TECHNIQUES," *Contemporary Journal of Social Science Review*, vol. 3, no. 3, pp. 1301–1314, 2025
- [29] U. Sagheer, F. Hussain, and K. Hamid, "Social Media Activities and Its Influence on Customer-Brand Relationship: An Empirical Study of Apparel Retailers' Activity In Pakistan," *Journal of Computing & Biomedical Informatics*, 2025, Accessed: Oct. 15, 2025. [Online]. Available: <https://www.jcbi.org/index.php/Main/article/view/1061>
- [30] M. Zia, A. Khalid, and K. Hamid, "AI-Enhanced Software Architectures: Bridging Technology and Strategy," *Journal of Computing & Biomedical Informatics*, 2025, Accessed: Oct. 15, 2025. [Online]. Available: <https://jcbi.org/index.php/Main/article/view/1045>
- [31] I. Manzoor, R. Ghani, and K. Hamid, "Challenges of Data Extraction from Facebook & WhatsApp Applications," *Journal of Computing & Biomedical Informatics*, 2025, Accessed: Oct. 15, 2025. [Online]. Available: <https://www.jcbi.org/index.php/Main/article/view/1050>
- [32] A. M. Delshadi et al., "Empowerment of Artificial Intelligence (AI) In Preventing and Detecting Ransomware: An Analytical Review," *Spectrum of Engineering Sciences*, vol. 3, no. 9, pp. 36–48, Sept. 2025.
- [33] M. Ibrar et al., "Econnoitering Data Protection and Recovery Strategies in the Cyber Environment: A Thematic Analysis," *International Journal for Electronic Crime*

- Investigation, vol. 8, Dec. 2024, doi: 10.54692/ijeci.2024.0804216
- [34] Federal Trade Commission (FTC), "Social media a gold mine for scammers in 2021," FTC Consumer Protection Data Spotlight, Jan. 2022. [Online]. Available: <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/social-media-gold-mine-scammers-2021>
- [35] Federal Trade Commission (FTC), "Who's who in scams: A spring roundup," FTC Data Spotlight, 2023. [Online]. Available: https://www.ftc.gov/system/files/ftc_gov/pdf/data-spotlight-who-s-who-in-scams-a-spring-roundup.pdf
- [36] Federal Trade Commission (FTC), "FTC data shows consumers report losing \$2.7 billion to social media scams since 2021," FTC Press Release, Oct. 2023. [Online]. Available: <https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-data-shows-consumers-report-losing-27-billion-social-media-scams-2021>
- [36] Investopedia, "Social media scams are surging," 2024. [Online]. Available: <https://www.investopedia.com/social-media-scams-surging-5217274>
- [37] Finance Magnates, "Social media identity fraud rises 16% as cybercriminal tactics evolve," Jun. 2024. [Online]. Available: <https://www.financemagnates.com/institutional-forex/social-media-identity-fraud-rises-16-as-cybercriminal-tactics-evolve-report>
- [38] The Fintech Times, "Identity fraud surges as social media scams evolve," Oct. 2023. [Online]. Available: <https://thefintechtimes.com/identity-fraud>
- [39] K. Hamid, M. W. Iqbal, M. Aqeel, and T. Rana, "Cyber Security: Analysis for Detection and Removal of Zero-Day Attacks (ZDA)," Artificial Intelligence & Blockchain in Cyber Physical Systems, vol. ?, pp. 172-196, 2023, doi: 10.1201/9781003190301-10