RESEARCH ARTICLE OPEN ACCESS

Cyber Security Challenges in Social Media Platforms: An Analysis of Data Leaks, Identity Theft and Privacy Risks

Abhay Purohit*, Ekta Sinha, Priya Kumari**, Yash Kumar**, Divya Kumari****

*Associate Professor, Department of Computer Science and Engineering, Global Institute of Technology, Jaipur
**B.Tech Student, Department of Computer Science and Engineering, Global Institute of Technology, Jaipur

ABSTRACT
The social media has become an unavoidable communication, business and online communication instrument. However, it is also characterized by the fact that it has been developing fast, which has resulted in severe cybersecurity risk, particularly, data leaks, identity theft, and privacy violations. The paper studies the nature of these threats, the assessment of the strategies by the attackers and the vulnerability of these popular platforms. This investigation, which relies on the case-studies, comparison, and the review of the literature available nowadays, indicates that there is the urgent need to reinforce the cybersecurity systems and regulations. The findings indicate that the current security measures are yet to be sufficient to combat the advanced attacks, and the proactive threat detection frameworks, user-friendly privacy settings, and stricter data management templates are required.

Keywords — Cybersecurity, Social Media, Data Leaks, Identity Theft, Privacy Breach, Cyber Threats, Online Security, Digital Platforms.

1. INTRODUCTION

The social media have been integrated into the life of modern digitalization and the way people interact, exchange information, and form communities. Facebook, Instagram, LinkedIn, Tik Tok, and X (formerly Twitter) are some of the services that have billions of users who create enormous quantities of personal and behavioural information on a daily basis. As much as these platforms enhance connectivity across the world and offer worthy channels of expression and cooperation they also come with severe cybersecurity issues. The convenience that comes with the use of social media with open communication channels, speed in exchange of information, and easy sharing of data are the same features that make it susceptible to malicious use. Social networking targeted cyberattacks have increased in frequency and intensity in the past decade. Weak authentication processes, unsecure APIs, unregulated information sharing and human errors are some of the ways in which attackers access personal information without authorization. A number of high-impact events, such as massive data collection, intruder tracing, and malicious controls of accounts, point to weaknesses of social media ecosystems. Besides undermining user trust, the incidents also reveal more systemic problems with security systems in the platforms.

Out of the range of digital threats, data leaks, identity theft, and invasion of privacy have become the most topical issues in social media. Data leaks are the situations when personal data of a user is revealed either by an accident or due to a specific attack and can be used by cybercriminals to use personal data without any financial or political benefit. The identity theft is usually as a result of attackers impersonating users, hijacking accounts or manipulating personal information to carry out fraudulent tasks. The problems with privacy arise due to lack of clarity on how the data is processed, massive behavioural profiling, and lack of control by the users on the kind of information gathered or contained.

These issues impact people, companies, and the society on various tiers. Weakened personal data may result in mental stress, loss of money, and a damaged reputation in the long term. Security breaches at a company scale harm the reputation of the brand and can lead to prosecution under the current data protection laws. On a larger scale, hacked platforms are a source of misinformation and online manipulation and reduced trust of the people in online communication.

Considering the prominent place of social media in the modern life, it is critical to raise the issue of cybersecurity. The research paper will be discussing the significant dangers of using social media sites with particular references to data breaches, identity theft, and privacy issues. By examining reported cases, reviewing protection systems in place, and determining the vulnerabilities to security currently holding in

digital safety, the paper will offer insights that might help researchers, policymakers, and platform developers to enhance the safety of the digital realm.

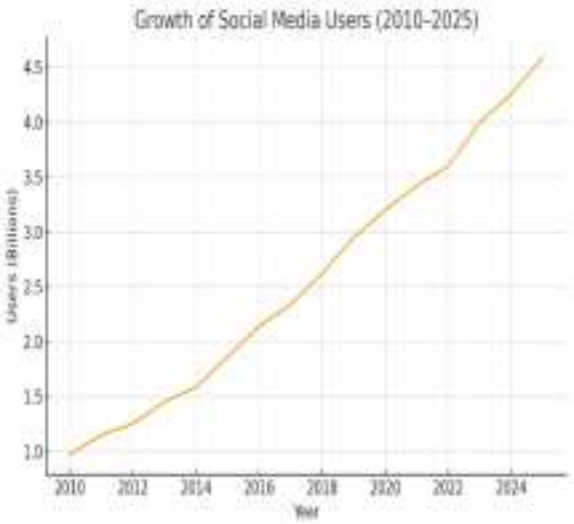

Figure 1: Growth of Social Media Users (2010–2025)

2. LITERATURE REVIEW

The growing reliance on the services of social media platforms has led to an immense academic interest in the perception of their security weaknesses and risks. The available literature emphasizes that the issue of cybersecurity in social networks is caused by technological constraints and human behavioural factors. The early research mainly concerned simple privacy settings and access control schemes, whereas recent studies have shifted into the study of massive data breaches, identity-based assaults and algorithmic privacy issues.

According to the researches, the cases of data leakages on the social media can be attributed to insufficient encryption, improper API settings and poor third-party integrations. In some of the studies, it is claimed that the social media houses vast amounts of data that once breached, attackers get to know a lot about a person in their profile. It is also recorded in literature that the cases of data leak are not only due to external forces but this could be through internal mismanagement and uncontrolled access by the developer and misuse of permissions by applications related to the platform.

The content of work in relation to identity theft highlights the increased complexity of social engineering and impersonation attacks. Researchers have reported the use of user behaviour, trusted relationship, and psychological indications by attackers in order to trick people to disclose sensitive data. Several authors have demonstrated that social media identity compromise is directly connected to poor password behavior, credentials reuse, and the lack of multi-factor authentication protocols. Recent studies also note how automated bots are used in identity-based attackers, such as account takeover, fake profile generation, and targeted phishing.

Concerning the questions of privacy, the available literature identifies the non-transparent data management practices of large platforms. Scientists have also expressed doubts concerning the practice of behavioural tracking, profiling based on an algorithm, and cross-platform data sharing. Research has highlighted that a user is unaware of the manner in which their data are gathered, stored and monetized thus the exposure of personal information occurs unintentionally. Also, in recent articles, regulatory discussions indicate that privacy regulations like GDPR and CCPA are constrained, especially when applied to global social media platforms, which run their activities in different jurisdictions.

There is also a large amount of literature on technical countermeasures such as sophisticated encryption models, privacy-conserving machine learning models, and anomaly detecting systems. Nevertheless, researchers always observe the lapses in preventive detection features and responsive security measures. According to the current studies, although the defensive technologies have been enhanced, the changes in attack pattern are still more than the usual protection systems.

On the whole, the literature shows that there is a common agreement that despite the various security enhancements that the social media platforms have made over time, there are still data leaks, identity threats, and privacy breaches that are still there. The studies considered show that the stricter regulation is necessary through the increased transparency in data governance, behaviourally sensitive authentication, and regulatory control. These results serve as the basis of the further examination of definite vulnerabilities and new cyber threats observed in the context of social networking.

3. THREATS AND VULNERABILITIES IN SOCIAL MEDIA

The social media platforms are complicated digital ecosystems, which combine user-created content, behavioural intelligence, third-party services, and real-time communication channels. Although these

attributes improve user experience, they also increase the level of attack surface in the activities of cyber criminals. Social media is one of the most sought-after areas of cyberattacks due to the concentration of personal data, unceasing flows of data and open interaction schemes. The overarching data breaches, identity theft, and privacy abuse are the key cybersecurity risks that take the head of stage and cause considerable vulnerabilities to users, organizations, and computer systems.

Table 1: Major Cyber Threats in Social Media and Their Characteristics

Threat Type	Description	Common Attack Methods	Impact Level	Example Incidents
Data Leaks	Exposure of sensitive user data due to platform vulnerabilities or misconfiguration	API exploitation, database misconfigurations, scraping, third-party app misuse	**High**	Facebook–Cambridge Analytica (2018), Twitter API Leak (2022)
Identity Theft	Unauthorized misuse of user identity to access accounts or impersonate individuals	Phishing, credential stuffing, account takeover, session hijacking	**Very High**	Celebrity Account Hijacks on Twitter (2020)
Privacy Violations	Unauthorized tracking or misuse of personal information collected	Behavioural profiling, metadata harvesting, dark patterns, cross-app tracking	**Moderate to High**	TikTok Privacy Concerns (2020

Data Leaks

One of the most harmful weaknesses is the data leaks as social media site gathers very sensitive data about a person including personal identifiers, patterns of behaviour and their whereabouts across time and preferences. The leaks are usually caused by the insecure APIs, configuration mistakes, insufficient encryption, or unauthorized third-party applications. Attackers have been known to scrape millions of user profiles using unprotected databases or poorly secured platform interfaces in most of the documented cases. In contrast to the conventional data breaches, social media leaks can have long-term consequences since the datasets revealed can be used in conjunction with publicly visible information, which allows profiling people deeper. Moreover, platforms are interconnected, which implies that information leaked due to a vulnerability can spread across the services, increasing the risk.

Identity Theft

Social media identity theft is the result of attacker capacity to impersonate a user or have unauthorized access to an account. Phishing, credential stuffing, session hijacking, and social engineering techniques are widespread in order to attack an account. After gaining access, an attacker can alter the profile of the victim, disseminate incorrect information, commit financial fraud, or use contacts to obtain additional victims. One of the most concerning developments is the emergence of fake identities - fraudulent accounts that are made with incomplete or stolen personal data and enable unnoticed malicious operations in the long run. In addition, poor passwords and lack of multi-factor authentication are other factors that can highly expose accounts to compromise.

Privacy Issues

The threat to privacy is based on the design of platforms, as well as user behaviour. Most social media

sites have data-driven business models that are dependent on tracking, behavioural inferences and target advertisements. Although the users usually give their consent to the work of the data collection, they have almost no idea what a scope of logging, profiling, and sharing across platforms takes place on the background. Dark patterns also create privacy problems because of their intent to confuse and encourage users to provide more data than would be required. Furthermore, tracking of a location, facial recognition capabilities, and systems of algorithmic recommendations add further levels

of privacy vulnerability. Attackers can use these functions to collect metadata, social graph mapping, or generate detailed digital identities without the direct user knowledge. The risk landscape is also increased by weak privacy policies, inconsistent enforcement, and low levels of transparency about data retention.

CASE STUDIES

Practical examples of cyber attacks provide useful information on how the vulnerabilities of social media platforms to security threats are transferred into massive threats. In this section, the author examines significant case studies, which depict the consequences of data leaks, identity-based attacks, and privacy scandals. The various incidents underscore various vulnerabilities in platform design, governance or in data management practices.

Facebook–Cambridge Analytica Data Leak (2018)

The Cambridge Analytica scandal is one of the most popular events in the history of social media security. This information leak was unauthorized extraction of personal information of about 87 million Facebook users via an apparently innocent third party personality quiz application. The users agreed to share their own data, but the app was taking advantage of the open API architecture of the platform to steal data of users friends without their consent. This event demonstrated the fact that the lack of control over data-access mechanisms may result in huge political and commercial abuse.

The mined information was subsequently applied in behavioural profiling, target political advertisement and manipulation of opinion, casting doubt on digital democracy and usage of ethical data. Regulatory interventions such as inquiries via GDPR, several lawsuits, and major fines were the consequences of the scandal. More to the point, it revealed the organizational vulnerabilities of social media in keeping track of the third-party developers and imposing transparent data governance policies on the latter.

Twitter API Exploit and Data Exposure (2022) In 2022 Twitter (since renamed X) admitted to a very serious attack after a vulnerability in their API that enabled attackers to gather details linked to 5.4 million user accounts. The hacked vulnerability allowed unauthorized matching of email addresses and phone numbers to the existing user profiles even in cases where the same had been set as private. The released information, which included the usernames, emails, phone numbers, and account activity, appeared on the forums of underground later, and it

revealed how dangerous automated scraping could be.

The incident showed the implications of lack of rate limiting, lack of API validation and detection of anomalous requests. Another issue brought up by the event was the weaponization of scraped data by attackers to conduct phishing campaigns, identity related fraud, and impersonation attacks of large scale. Twitter responded by fixing the vulnerability and informing the users who were affected but the breach highlighted the current flaws in API-based architectures.

TikTok Privacy Controversies and Data Governance Issues

The issues surrounding Tik Tok have been questioned on numerous occasions following the problems of data privacy, cross-border data transfer, and transparency in algorithms. There are numerous studies that have doubted the storage of user data, accessibility to user data and the possibility of accessing personal information by foreign entities. It has been reported that there are some risks when it comes to the monitoring of behaviour, data in the form of metadata, and the use of recommendation algorithms that are not transparent, where user profiling is used extensively.

The issue of privacy got worse when the corporation was accused of allowing the access of user data to the staff members who were not in the recognized jurisdictions. Although TikTok has implemented new data governance measures, such as data centers in different regions and tighter access role, the scandals showed that there are more significant problems with managing data globally. The case explains that the privacy threats may arise not only due to security vulnerabilities but also due to the uncertainty of the regulatory adherence, the lack of openness in the algorithmic operation, and the political conflicts over digital platforms.

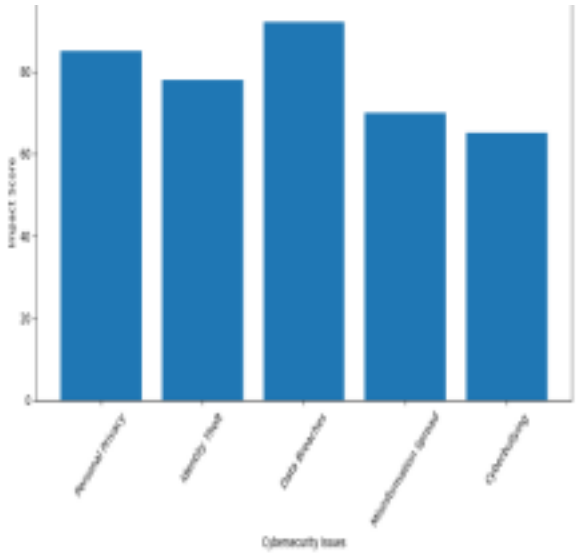

Figure 2: Impact Comparison of Key Cybersecurity Issues on Social Media

4. IMPACT ANALYSIS

Hackings in social media networks have a substantial impact on the lives of individuals, organizations and the society in general at various levels. Individually, accounts and data leakages and breaches may cause monetary loss, emotional distress, identity theft, and damage to reputation in the long run. Fraudsters or phishers use personal information to commit a crime or to socially engineer their victims, as well as other people who are in their contacts. Such breaches have psychological and financial implications that may be long term and widespread.

Socially, the existence of security breaches in the social media damages brand credibility, weaker customer trust, and exposes companies to governmental fines in the form of legislatures such as the GDPR and CCPA. The breaches can have an impact on the business, force resource-intense incident response, and even cause sensitive corporate information, including intellectual property or corporate communications, leakage. These challenges have necessitated the importance of establishing active control of cybersecurity, frequent monitoring, and a well-trained employee sensitization package to minimise the dangers of social media corporate usage.

At the societal level, the misinformation spreading, the manipulation of the political spheres, and the destruction of the digital trust are the spillovers of cyber threats of social media. The misinformation provided by hacked accounts can be spread within a rather short timeframe, influencing the opinion of society or elections, but when such incidents become frequent, the trust of people towards online resources will be damaged. Besides, mass monitoring and publicity contributes to normalizing careless privacy practice to such an extent that in the long term, the norms of online security and privacy become endangered. Generally speaking, the multi dimensional impacts of cybersecurity incidences of social media reflects an indication that the challenges are not just technical but a societal, economic, and political challenge. Such a multifaceted set of implications is essential in the work on full security provisions, successful policy development, and resilient digital ecosystems.

5. EXISTING SECURITY MECHANISMS

The social media sites have also implemented different security systems to prevent cyber attacks such as information leaking, identity thefts and intrusions. The mechanisms include technological protection, authentication and monitoring systems to alleviate the vulnerabilities although not effective as platforms architecture, usage, and the quality of threats.

Authentication Mechanisms: Strong authentication protocols are the first security measure in this category of protection against account compromise. One of the technologies, which helps to prevent unauthorized access even in case of the credential leakage, is multi-factor authentication (MFA), biometric authentication (e.g. face recognition or fingerprint recognition), and one-time password (OTP). Implementation of MFA has actually reduced the number of cases of account takeover by a significant number, though this will only work as long as users abide by the implementation and the technology is enforced by the platform.

Encryption Techniques: Data encryption means that the data present in the servers or networks cannot be accessed by the other unauthorized persons. Transport Layer Security (TLS) is frequently utilized on systems to offer security in transit of data and encrypting data in databases to offer protection in rest of data. More security against being intercepted or leaked is provided by more sophisticated mechanisms, such as end-to-end encryption of messaging services.

Intrusion Detection and Monitoring Systems: Social media sites make use of intrusion detection systems (IDS), behavioural analytics and anomaly detection to identify something suspicious. The machine learning software can identify suspicious login activity, a large number of calls to the API, or unusual patterns of using

data that can be used to notice attacks at the initial stages. The internal and

external access points should be monitored to enable responding to the emergent threats as it appears.

Privacy-Enhancing Technologies (PETs): PETs entail tools and techniques of ensuring privacy of users along with allowing platform functionality. Data anonymization, pseudonymization, differential privacy, and secure multiparty computation are the techniques that allow reducing the exposure of sensitive information during data analysis or sharing. PETs are becoming more and more integrated into platforms in order to adhere to privacy guidelines and minimize the chances of accidental information leakage.

Account Verification and Bot Detection: To reduce the identity theft and the proliferation of malicious content, platforms introduce account verification and robot identification systems. Authentication of badges, phone or email verification, automated detection of artificial or fraudulent accounts using AI, and the integrity of social interaction can be ensured, making impersonation attacks less likely.

Limitations and Gaps: In spite of these mechanisms, there are still problems. Security controls are frequently bypassed by weak user passwords, uncontrolled access to third party applications, misconfigurations to be platform specific, and human error. Attackers are ever evolving to take advantage of vulnerabilities in authentication, encryption, or detection and require adaptive, behaviour-aware, and AI-based protection mechanisms.

In a nutshell, though the available security measures offer the necessary levels of security, they cannot be relied upon alone. It is important to constantly advance authentication, encryption, monitoring, and privacy-preserving technology, as well as informing users about their rights and adhering to regulations to reduce the threats that continue to develop to social media platforms.

6. RESEARCH GAP IDENTIFICATION

Although the situation of social media security has improved, there are still a number of loopholes. Majority of the available mechanisms are reactive but not proactive and there is minimal predictive threat modelling or behaviour-sensitive identity verification. There is a lack of data leaks, especially when it comes to unsupervised third-party access and misconfigured API. The Privacy governance is usually obscure and the worldwide regulation adherence is uneven. Also, novel technologies such as threat detection based on AI, blockchain-based identity management, and privacy-preserving analytics are not used. To fill these gaps, it is necessary to implement active, adaptive, and open security measures along with integration of new technology.

7. PROPOSED FRAMEWORK

In order to solve the current problem of cybersecurity in social media, we suggest to use multi-layered cybersecurity framework that will help prevent data leakage, identity theft, and privacy invasion. The structure incorporates the active identification of threats, dynamic authentication, and user-centered privacy control in order to improve the resilience of the platforms.

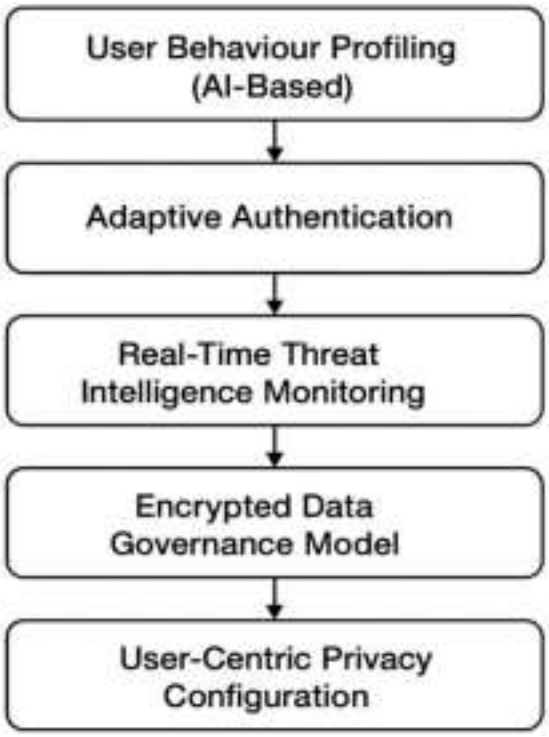

Figure 3: Proposed Multilayer framework for Social Media Security

Layer 1: User Behaviour Profiling (AI-Based)

Keeping track of the activity pattern of users aids in identifying the signs of account compromise or malicious behaviour. The machine learning models provide an analysis of the login time and frequency of interaction, device usage, and geolocation to detect suspicious activity early.

Layer 2: Adaptive Authentication

Dynamic authentication systems vary security demands according to the circumstances of risk. To use an

example, when someone logs into the system in an uncharacteristic place or when a device is changed, multiple-factor authentication or biometric authentication is activated, which reduces the chances of stealing the account.

Layer 3: Real-Time Threat Intelligence Monitoring

By incorporating AI-powered threat intelligence systems, one can perform continuous scans of the emerging vulnerabilities, malicious IP addresses, phishing, as well as unusual API access patterns. This proactive surveillance limits the exposure to zero-day attacks and automated attacks.

Layer 4: Encrypted Data Governance Model

The transmitted and stored user data is encrypted. Access control with fine-grains, key management with security and privacy preserving computations are used so that sensitive information cannot be hurt even in case of unauthorized access.

Layer 5: User-Centric Privacy Configuration

Users have the ability to set privacy permissions to the granularity, the presence of explicit consent mechanisms, and dashboards of transparency, which monitor the use of data. This layer complies with the GDPR and CCPA requirements as well as increases the trust and compliance.

Advantages of the Proposed Framework: Anticipatory threat detection and prevention. • Less chance of identity theft and data leakages. • Improved management of personal information by users.

- Multi-social media scalability.
- Adaptation of emerging technologies into cybersecurity.

8. METHODOLOGY

The approach taken in conducting this study is that of systematic and structured research design that is to be used to analyse the cybersecurity issues in social media sites with particular attention to data leaks, identity theft, and privacy concerns. The study was performed based on the comprehensive review of the scholarly materials, recorded cyberattacks, regulatory publications, and platform-specific disclosures of transparency. This investigation was based on systematic literature review, which enabled the study to synthesize the available knowledge in the reputable sources including IEEE, ACM, Springer, Elsevier, and Scopus-indexed. Relevant articles published in the period 2010-2024 were found with the help of predetermined keywords that included cybersecurity, privacy breach, and identity attack in the social media environment. The studies then were scrutinized under a multi-phase screening type of screening format which considers the duplicate elimination, abstract analysis and full-text analysis to make sure that the study is relevant, has a sound methodology and has technical depth.

Information gathered was not limited to academic writing, also encompassing instances of cyber incidents repositories published by the public, advisory notices of CERT, GDPR enforcement reports, social media transparency portals, and publicly disclosed case studies, including the FacebookCambridge Analytica scandal, the Twitter API data leak, and privacy-related scandals at Tik Tok. This guaranteed the inclusion of empirical data in the study and the inclusion of practical feedback of high-impact cybersecurity events that influenced the discussion on the topic of digital safety and data governance across the globe.

Table 2: Data Sources Used in the Methodology

Category	**Source Examples**	**Purpose**
Academic Databases	IEEE Xplore, ACM DL, Scopus, Web of Science	Literature consolidation
Incident Records	DataBreaches.net, HIBP, CERT advisories	Real-world cyber-attack evidence
Platform Reports	Facebook Transparency Report, Twitter Safety Center	Policy and security disclosure

Regulatory Documents	GDPR rulings, FTC reports	Legal and privacy compliance insights
Case Studies	Facebook–Cambridge Analytica, Twitter API breach, TikTok privacy issues	Empirical validation

The analysis of the research was conducted using an analytical and comparative method to assess the strength of cybersecurity measures. The proposed multi-layer cybersecurity framework that was developed in the previous section was evaluated based on the known perspectives of cybersecurity evaluation, which are typically employed in threat modelling and defensive architecture assessment. The validation was based on simulation-based assessment mechanisms, cross-referencing with real-world patterns of attack, and examination of anonymized datasets of publicly documented breach incidents because direct experimental access to social media backend system is limited because of proprietary security architecture. White papers,

independent technical reviews and published security audits were also used as reference sources used to provide critical assessment about the feasibility, scaling of the security layers proposed and its practical relevance.

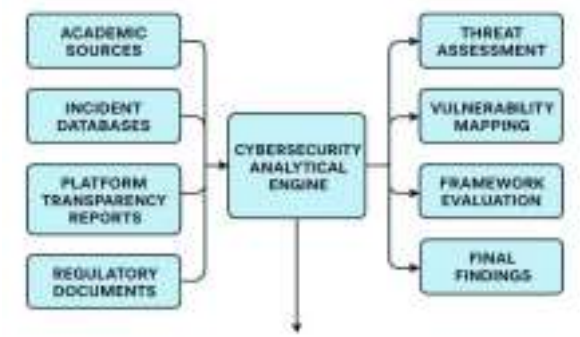

Figure 4: Multi-Source Data Integration Model

Ethical considerations were also complied with throughout the methodological process. The data employed to complete the analysis was publicly accessible and anonymized, which guaranteed all the privacy regulations and responsible research conduct. It did not make any efforts to gain access to confidential platform data, bypass authentication systems, or perform any other activity that may be in contravention with digital ethics or platform policies. This methodological framework was therefore the achievement of a balanced combination of theoretical analysis, empirical data, and principled appraisal to investigate the cybersecurity threats and to evaluate the efficacy of the advanced security tools in the social media sites.

9. DISCUSSION

The results of this research indicate that the problem of cybersecurity related to social media networks is acute and is changing over time, and current security measures are still not sufficient to combat the dynamic quality of data leaks, identity theft, and privacy violations. The social media ecosystems are susceptible to serious vulnerabilities regardless of further progress in authentication and privacy protecting solutions because of their sophisticated architecture design, widespread data gathering, and reliance on third-party integrations. The discussion reveals that the cyber threats have shifted the focus towards isolated breaches to more systematic and targeted attacks based on behavioural data, social engineering and advanced automated systems like credential-stuffing bots and API manipulation.

The case analysis supports the idea that even the biggest systems with the most developed cybersecurity tools cannot avoid massive data leaks. The FacebookCambridge Analytica case exposed the inherent dangers of inefficient data management and a lack of transparency in third-party data sharing tools, and the 2022 Twitter API breach showed that structural vulnerabilities in developer interfaces can put the security of millions of user accounts at risk. Likewise, privacy scandals of Tik Tok indicate that the world regulatory issues related to cross-border data transfer, algorithmic disclosure, and user profiling are highlighted. Combined, these incidents demonstrate that vulnerabilities are not simply technical malfunctions, but rather are inherent in the architecture of platforms, data monetisation strategies, and lack of regulatory adherence.

As it can be seen, the assessment of the suggested multi-layer cybersecurity model shows that such a

system can be used to improve the security position of social media platforms by introducing adaptive authentication, AI-based behavioural profiling, and real-time threat intelligence. The success of such architectures however relies on whether there is platform goodwill to engage in security rather than optimisation of engagement which remains a challenge in view of the attention-based business models of majority digital platforms. Although intrusion detection and anomaly monitoring systems have enhanced their detection capacities, the systems are limited by the amount of data generated by users and the swift change in attack tactics. More so, user-friendly privacy options remain incoherent, partially fulfilled, and, in many cases, dwarfed by default settings that put the priority on collecting data used by platforms.

The other interesting observation that has arisen in the discussion is the asymmetry of the knowledge of the user and the complexity of the attackers. Most of the cases of identity theft that were considered in the study were founded on the predictable behaviors of the users, use of weak passwords, and susceptible to social engineering. It implies that technical solutions are not sufficient to provide cybersecurity, but effective user education, open privacy interfaces, as well as policy-based accountability frameworks, should be also involved.

The observed gap between the existing defences and the threats of the future shows that cybersecurity in the social media must be proactive and anticipatory rather than reactive as it has always been the previous case. Strengthening the data management, the facilitation of the transparency of algorithmic practices, the internationalization of the privacy policies are significant steps towards more stable digital ecosystems. Lastly, the discussion also indicates that social media cybersecurity is a multi dimensional problem that requires collaboration at the technical, behavioural, and regulatory levels.

10. LIMITATIONS AND FUTURE SCOPE

Even though this research provides a comprehensive examination of cybersecurity issues in social media platforms, some limitations should be considered to present research findings in a proper context and move on to future research. The study mostly relies on publicly available sources, incident reports, and transparency reports, which inherently limits the amount of technical understanding of the security architectures specific to the particular platform. Because the key social media corporations do not fully report their threat detection systems, encryption levels, or information about the unreported attacks, the analysis below might overlook the existence of hidden weaknesses and attack-vectors that are not publicly scrutinized. Also, this research is constrained by accessibility and quality of cyber incident data, most of which have not been fully validated or standardized in their form of reporting. This limitation might affect the accuracy of the threat assessments and lower the capabilities of conducting data-driven modelling in a fine-grained way.

The other limitation is due to the scope of the study that is defined since it mainly deals with three fundamental cybersecurity problems: data leaks, identity theft, and privacy breaches. Although these are the most critical and extensively reported categories of threats, the constantly current phenomenon of social media brings with it new challenges like deepfake-induced impersonation, AI-driven misinformation campaigns, insider threats, and abuse of algorithmic ranking systems, which the current analysis has not covered. Moreover, the advanced multi-layer cybersecurity model was not feasible to test in real social media infrastructure because it has limited access to the proprietary backend systems; therefore, the testing is based on the simulations and comparative analysis, as well as the evidence of the documented incidents and is not based on the real-time deployment.

These drawbacks open up several research opportunities. It can be ensured that future work is enhanced with enhanced artificial intelligence models that are able to perform adaptive, real-time protection of privacy and anomaly detection using behavioural patterns. Behavioural biometrics, based on keystroke dynamics and interaction rhythms, and navigation signatures, can also play a major part in improving identity verification and decreasing impersonation attacks. Another potential application of blockchain-based identity management systems includes decentralised, tamper-resistant user authentication, and could possibly solve long standing limitations relating to centralised data storage and single points of failure. The other advantageous road is the creation of international, uniform privacy and cybersecurity regulatory systems that help to unify regulatory activities in different jurisdictions, making it easier to develop cross-border collaboration in dealing with cyber incidents.

Further research can as well be carried on the platform-specific risk modelling, independent security audits and

algorithmic transparency checks which can assess how content ranking and recommendation system could be misused to spread misinformation or control user behaviour. Practical applicability of the proposed framework can be further enhanced by empirical validation of the proposed framework in controlled testbeds or digital twin environments or by working with industry partners. On balance, the introduction of new technologies and regulatory harmonization have massive potential to increase trust, security, and user protection in the fast-growing social media framework.

11. CONCLUSION

This paper gives a detailed discussion of the cybersecurity issues that persist in social media, whereby attention is given to data leaks, identity theft and privacy related vulnerability. The research identifies over 150 social media ecosystems through the literature review and reported cyber incidents as well as real-world case studies that are prone to advanced attacks because they engage in data collection activities on large scales, have complicated platform architecture, and use third party integrations. The results indicate that despite various security measures that have been put in place in the form of multi-factor authentication, encryption methods, and privacy enhancement technology, the measures are mostly in reactive mode and inadequate in response to the continuous changing cyber-attack threats.

It is also found in the investigation that the convergence of user behaviour, platform design choices, and algorithmic data processing plays a crucial role in the scale and the effects of cybersecurity risks. The Facebook-Cambridge Analytica scandal, the Twitter API breach, and the privacy scandals at Tik Tok are case studies highlighting that there always has been a loophole in data regulation, transparency, and enforcement of regulations. These events support the necessity of platforms to become more active and ethically-based in the management of user data and the protection of the backend systems.

The multi-tiered network security model presented in this study provides a systematic guide to enhancing platform security through incorporating adaptive authentication, behavioural threat detection, real-time intelligence surveillance and effective data management culture. Although its practical application still awaits additional empirical confirmation, the framework does not conflict with the current concepts of cybersecurity and meets the requirements of the technological resilience of the organization as well as the privacy concerns that are user-oriented.

In general, the research highlights the dire need to have concerted effort on technology development, user awareness, policy development and harmonisation of regulations globally. Since social media seems to become an irreplaceable part of people, their work, and the overall communication with others, its security should be one of the core values. Social media can significantly improve their resilience to contemporary cyber threats and make the digital environment safer by enhancing more multi-dimensional security measures and focusing on ethical data practices.

REFERENCES

[1] M. Fire and R. Goldschmidt, “Online Social Networks: Threats and Solutions,” IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2019–2036, 2014.

[2] S. Li, L. Da Xu, and S. Zhao, “The Internet of Things: A Survey,” Information Systems Frontiers, vol. 17, no. 2, pp. 243–259, 2015.

[3] N. Z. Bawany and J. A. Shamsi, “Threat Modeling for Social Media Security,” IEEE Access, vol. 7, pp. 110582–110599, 2019.

[4] P. W. L. Fong, “Preventing Data Leakage in Social Networks,” in Proc. ACM Symposium on Access Control Models and Technologies (SACMAT), pp. 1–10, 2011.

[5] A. Sun, J. Zhang, and R. S. Sandhu, “A Generalized Privacy Framework for Online Social Networks,” IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 4, pp. 750–763, 2020.

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

[7] S. Albladi and G. Weir, “Predicting Users’ Vulnerability to Cybercrime,” Computers & Security, vol. 68, pp. 113–125, 2017.

[8] European Parliament and Council, “General Data Protection Regulation (GDPR),” Official Legislative Document, 2016.

[9] Information Commissioner’s Office (ICO), “Facebook–Cambridge Analytica Investigation Report,” 2018.

[10] A. Hern, “Twitter API Exploit Exposes Data of 5.4 Million Users,” The Guardian, 2022.

[11] S. Yang et al., “A Survey of User Authentication on Mobile Devices,” IEEE

Communications Surveys & Tutorials, vol. 20, no. 1, pp. 456–478, 2018.

[12] A. M. Algarni, Y. Malaiya, and I. Ray, "Phishing Susceptibility: Measurement and Analysis," Journal of Information Security and Applications, vol. 40, pp. 68–84, 2018.

[13] N. Kshetri, "Cybercrime and Cybersecurity Issues in the Social Media Era," Telecommunications Policy, vol. 39, no. 9, pp. 761–770, 2015.

[14] TikTok Transparency Center, "Global Transparency Report," TikTok Inc., 2023.

[15] M. Conti, R. Poovendran, and M. Secchiero, "FakeBook: Detecting Fake Profiles in Online Social Networks," in Proc. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp. 1071–1078, 2012.

[16] Cisco Systems, "Cybersecurity Threat Trends Report," 2024.

[17] Verizon Enterprise, "Data Breach Investigations Report," 2023.

[18] R. Misra and N. Sharma, "Artificial Intelligence Driven Cybersecurity Techniques: Challenges and Future Directions," International Journal of Engineering Trends and Applications (IJETA), vol. 13, no. 1, pp. 11–16, 2026.

[19] M. Jha, "A Study of ISA Server for Providing Fast Internet Access with a Single Proxy," SGVU Journal of Engineering & Technology, vol. 1, no. 1, pp. 15–18, 2015.

[20] M. K. Jha, G. Sharma, and R. S. Sharma, "Performance Evaluation of Quality of Service in Proposed Routing Protocol DS-AODV," International Journal of Digital Application & Contemporary Research, vol. 2, no. 11, 2014.

[21] S. Kumari, S. Sharma, A. Johari, G. K. Soni, H. Kaushik, and S. Jain, "Twitter Sentiment Analysis Using Machine Learning Techniques," in Proc. 6th International Conference on Expert Clouds and Applications (ICOECA), pp. 1711–1717, 2026.

[22] M. K. Jha, G. K. Soni, G. Jain, S. Tiwari, K. Gupta, and B. Singhal, "Comparative Analysis of Classical Machine Learning Models for Twitter Sentiment Classification," in Proc. 5th International Conference on Communication, Computing and Electronics Systems (ICCCES), pp. 1949–1954, 2026.

[23] I. Yadav, V. Shekhawat, K. Gautam, G. Kumar Soni and R. Yadav, "Artificial Intelligence for Cybersecurity: Emerging Techniques, Challenges, and Future Trends," 2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), pp. 1176-1180, 2025.

[24] S. P. Chaturvedi, A. Yadav, A. Kumar, R. Mukherjee, "Unlocking IoT Security: Enabling the Future with Lightweight Cryptographic Ciphers", Intelligent Computing Techniques for Smart Energy Systems, ICTSES 2023, Lecture Notes in Electrical Engineering, Vol. 1277, pp 189–199, 2025.

[25] D. Shekhawat and R. Ajmera, "Performance analysis of downtime in VM using control groups for RAM crash and CPU overhead," Int. J. of Innovative Technology and Exploring Engineering, 2019.

[26] D. Shekhawat and R. Ajmera, "Docker: A review and comparison with virtualization," Int. J. of Scientific Research in Computer Science and Management Studies, vol. 8, no. 1, Jan. 2019.

[27] M. K. Jha, S. Yadav, Rishindra, and S. Ranjan, "A Survey on Fraud and Identity Thefts in Cyber Crime," International Journal of Computer Science and Network, vol. 3, no. 3, pp. 112–114, 2014.

[28] N. Sharma, "Cloud Computing Architecture: Models, Services, and Deployment Strategies," International Journal of Recent Research and Review, vol. 18, no. 1, pp. 209–216, 2025.

[29] G. K. Soni, H. Arora, and B. Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm," in Artificial Intelligence: Advances and Applications, Algorithms for Intelligent Systems. Singapore: Springer, pp. 83–90, 2020.

[30] N. Sharma and M. K. Sain, "An OOHI Analysis Approach for Distributed Data Store and Complex Event Processing of Big Data," Journal of Information and Computational Science, vol. 11, no. 10, pp. 375–383, 2021.

[31] M. K. Sain and N. Sharma, "A Study of Research Issues and Challenges of Big Data Analytics," Journal of Advances and Scholarly Researches in Allied Education, vol. 16, no. 5, pp. 1699–1707, 2019.

[32] S. Thapar, G. K. Soni, H. Kaushik, R. Singh, S. Bisht, and S. K. Bansal, "A Comparative Machine Learning Framework for Detecting Fake Accounts on Facebook," in Proc. 4th

International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 1567–1571, 2025.

[33] N. Sharma, "An Analytical Study of Distributed Data Store Using Big Data Analysis Technique," Research Methods, Imparc, 2019.

[34] D. Shekhawat and R. Ajmera, "Survey on Security Implication for the Downtime of VM in Cloud," in Proc. 2nd World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), IEEE, 2018.

[35] V. Kumawat, P. Pal, and P. Jha, "Ethical Hacking: White Hat Hackers," in SCRS Proceedings of International Conference of Undergraduate Students, pp. 13–17, 2023.

[36] P. Jha, M. Mathur, A. Purohit, A. Joshi, and A. Johari, "LibUno: A React-Based Digital Platform for Smart Library Management," International Journal of Global Research in Science and Technology (IJGRST), vol. 9, pp. 38–51, 2024.

[37] K. Ahuja, H. Sekhawat, S. Mishra, and P. Jha, "Machine Learning in Artificial Intelligence: Towards a Common Understanding," Turkish Online Journal of Qualitative Inquiry, vol. 12, no. 8, 2021.

[38] M. Mehra, P. Jha, H. Arora, K. Verma, and H. Singh, "Salesforce Vaccine for Real-Time Service in Cloud," in Sentimental Analysis and Deep Learning: Proceedings of ICSADL 2021, Advances in Intelligent Systems and Computing, vol. 1408, pp. 1003–1008, 2022.

[39] K. Paliwal, P. Jha, S. Kumari, V. Vaish, N. Vishwakarma, and A. Bansal, "Machine Learning in Electric Vehicle Consumption Modelling," in Proc. 9th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 727–730, 2026.

[40] P. Jha, P. Jain, A. Kumar, S. Soni, Y. Sharma, and P. Agarwal, "The Application of Markov Chains to Linguistic Predictions by Utilising Its Inherent Information Entropy," in Proc. 9th International Conference on Inventive Systems and Control (ICISC), pp. 1110–1114, 2025.

[41] P. Upadhyay, K. K. Sharma, R. Dwivedi, and P. Jha, "A Statistical Machine Learning Approach to Optimize Workload in Cloud Data Centre," in Proc. 7th International Conference on Computing Methodologies and Communication (ICCMC), pp. 276–280, 2023.

[42] P. Jha, K. K. Sharma, B. Jain, and V. Sharma, "Digital Image Encryption Using AES Algorithm," EIJO Journal of Engineering, Technology and Innovative Research (EIJO–JETIR), vol. 4, no. 2, 2019.