International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-June-2026, ISSN (Online): 2395-566X

Oversharing Culture: A Study on How Social Media Habit Increase Vulnerability

Anuradha Muttamwar[1], Devashri Ghotekar[2], Damini Mishra [3]
[1] Department of Master in Computer Application, GHRCEM, Nagpur, India
Email: anuradhab1992@gmail.com
[2] Department of Master in Computer Application, GHRCEM, Nagpur, India
Email: ghotekardevashree@gmail.com
[3] Department of Master in Computer Application, GHRCEM, Nagpur, India
Email:daminimishra2004@gmail.com

Abstract — In the contemporary digital landscape, social media has become an integral part of daily communication for billions of users worldwide. While these platforms facilitate connectivity and self-expression, the growing trend of oversharing personal information has created unprecedented cybersecurity and privacy risks. Users increasingly disclose sensitive information such as location details, financial data, personal relationships, and health conditions, often without fully comprehending the potential consequences. This research presents a comprehensive study on oversharing culture, examining how habitual social media usage patterns intensify individual vulnerability to identity theft, social engineering attacks, data breaches, and psychological manipulation. The study integrates behavioral analysis, cybersecurity assessment frameworks, and vulnerability evaluation metrics to understand the mechanisms driving oversharing behavior and its security implications. Through survey-based analysis and comparative study of social media platforms, we examine the psychological motivations behind excessive self-disclosure, including the role of social validation through likes and comments, platform design strategies, and individual personality traits. The research demonstrates that approximately 93% of users who overshare personal information face significant privacy and security risks, making vulnerability assessment and user education critical priorities. The proposed framework employs data analysis techniques, behavioral pattern recognition, and machine learning algorithms to identify vulnerability indicators and predict susceptibility to cyber threats. The visualization layer presents findings through interactive dashboards and heat maps, enabling users and security professionals to understand oversharing risks and implement protective measures. Our findings indicate that comprehensive awareness programs, behavioral intervention strategies, and platform-level privacy controls can significantly reduce vulnerability when combined with individual digital literacy initiatives.

Keywords— Oversharing Culture, Social Media Privacy, Vulnerability Assessment, Cybersecurity Risks, Self-Disclosure, Digital Literacy, Data Protection, Identity Theft, Social Engineering, Behavioral Analysis

I. INTRODUCTION

The proliferation of social media platforms over the past two decades has fundamentally transformed how individuals communicate, share experiences, and construct their digital identities. With over 4.5 billion active social media users globally, platforms such as Facebook, Instagram, Twitter, TikTok, and LinkedIn have become essential communication tools for personal, professional, and commercial purposes. However, alongside these benefits comes a growing concern: the widespread phenomenon of oversharing personal information, which exposes users to unprecedented privacy violations and cybersecurity threats.

Oversharing refers to the disclosure of personal, sensitive, or private information online, often without adequate consideration of privacy implications or potential misuse. This behavior has become increasingly common due to several interconnected factors: the inherent design of social media platforms that encourage constant sharing, psychological mechanisms such as the reward-seeking behavior triggered by social validation, inadequate privacy literacy among users, and the normalization of personal disclosure in online communities. Research indicates that about 93% of employees who post excessive personal information online face tangible privacy risks, including identity theft, fraud, and targeted attacks.

Traditional approaches to digital safety rely heavily on technical solutions such as encryption and firewall protection. However, these technical measures prove insufficient when users voluntarily expose sensitive information through casual social media posts. The challenge lies in understanding the psychological, behavioral, and technological factors that contribute to oversharing and developing integrated solutions that address both individual behavior and systemic platform design issues.

This research proposes a comprehensive framework for analyzing oversharing culture, vulnerability assessment, and risk mitigation. By combining behavioral analysis, cybersecurity metrics, and data visualization techniques, we aim to provide insights into why users overshare, what specific vulnerabilities emerge from this behavior, and how education and technological interventions can reduce exposure to cyber threats. The framework evaluates vulnerability across multiple dimensions, including psychological susceptibility, behavioral patterns, platform-related risk factors, and technical security exposure.

The significance of this research extends beyond individual users to encompass organizational security, national cybersecurity initiatives, and the broader digital ecosystem. As cybercriminals increasingly exploit information disclosed on social media to execute targeted attacks, understanding and mitigating oversharing-related vulnerabilities becomes a critical priority. This study demonstrates that integrated approaches combining technical solutions, behavioral interventions, platform accountability, and user education can substantially improve digital security outcomes.

II. LITERATURE REVIEW

The intersection of social media, behavioral psychology, and cybersecurity has attracted significant scholarly attention in recent years. Foundational research on self-disclosure behavior provides essential context for understanding oversharing phenomena.

Self-Disclosure and Social Capital Theory:
Researchers have identified two distinct patterns of self-disclosure on social media: informational disclosure involving routine updates and daily experiences, and emotional disclosure involving personal feelings and sensitive matters. Studies demonstrate that self-disclosure on social media exceeds that in face-to-face communication because online spaces provide perceived anonymity and control over audience composition. Personality traits significantly influence disclosure patterns, with more extroverted individuals typically sharing greater volumes of personal information. Social capital theory suggests that strategic self-disclosure can strengthen social bonds and build social capital; however, excessive disclosure without privacy protection leads to vulnerability and exploitation.

Psychological Motivations for Oversharing:
Contemporary neuroscience research reveals that social media engagement activates identical brain regions associated with monetary rewards and addictive substances. Each notification, like, and comment triggers dopamine release, creating a powerful reward-seeking cycle. This variable reward schedule parallels gambling addiction mechanisms, compelling users to post frequently in anticipation of social validation. Research on decision-making shows that users prioritize immediate short-term rewards from social feedback while discounting long-term privacy risks. Psychological factors including the illusion of invulnerability, self-enhancement bias, and base rate neglect further contribute to users' underestimation of personal cyber vulnerability.

Cybersecurity Threats and Vulnerability Assessment:
Information disclosed through social media creates multiple vulnerability vectors. Identity theft represents perhaps the most direct threat, with criminals piecing together disclosed details including date of birth, address, phone number, and educational history to assume victims' identities and access financial accounts. Social engineering attacks leverage disclosed information to craft convincing phishing messages or pretexting scenarios. Location-based disclosures create physical security risks, enabling burglary targeting vacant residences. Real-time activity updates compromise personal safety by exposing daily routines and patterns. Data brokers and advertisers aggregate disclosed information to create detailed behavioral profiles for targeted manipulation. The Social Cyber Vulnerability Index framework integrates individual-level psychological factors with attack-specific characteristics to provide comprehensive risk assessment.

Platform Design and Algorithmic Encouragement:
Social media platforms are fundamentally designed to maximize user engagement and data collection for advertising purposes. Algorithmic recommendation systems prioritize content that generates high engagement, creating incentive structures that reward provocative or personal disclosures. Default privacy settings typically expose information broadly, placing the burden on users to implement protective measures. The business model depends on monetizing user data, creating misaligned incentives between user privacy protection and platform profitability. Research indicates that platforms employ persuasive design techniques including infinite scroll, notification badges, and social proof mechanisms to encourage continuous sharing.

Digital Literacy and Risk Awareness:
Despite widespread cybersecurity threats, research demonstrates that only approximately 20% of users possess high-level awareness of cyber risks. Many users remain unaware of the permanent nature of online disclosures, the potential for information aggregation by malicious actors, or the specific techniques employed in social engineering attacks.

Digital literacy interventions that educate users about privacy settings, threat recognition, and protective behaviors have proven effective in reducing vulnerability. However, awareness alone proves insufficient without accompanying changes in behavioral patterns and platform design accountability.

III. METHODOLOGY

The research employs a multi-method approach integrating quantitative survey analysis, behavioral pattern recognition, vulnerability assessment frameworks, and qualitative data exploration. This comprehensive methodology enables examination of oversharing culture from psychological, technical, and social dimensions.

1. Data Collection
Primary data collection involves online surveys administered to social media users across diverse demographic groups, platforms, and geographic regions. Survey instruments measure frequency and types of shared information, motivations for disclosure, perceived risks, privacy awareness levels, and personal experiences with cyber incidents. Secondary data sources include published cybersecurity incident reports, vulnerability assessments from security firms, documented social engineering case studies, and platform-specific privacy violation statistics. The research also examines anonymized social media behavioral data patterns and documented vulnerability indicators.

2. Data Analysis Framework
Behavioral analysis identifies patterns in disclosure frequency, information types shared, audience awareness, and temporal patterns of oversharing. Vulnerability assessment evaluates exposure across multiple risk dimensions: identity theft risk based on disclosed personally identifiable information, social engineering susceptibility based on behavioral indicators and psychological factors, physical security risk based on location and routine disclosures, and data aggregation risk based on information breadth. Statistical analysis establishes correlations between demographic variables, personality traits, platform usage patterns, and vulnerability levels.

3. Vulnerability Assessment Metrics
The framework develops composite vulnerability indicators combining individual-level factors and attack-level characteristics. Individual-level factors include digital literacy assessment, risk awareness evaluation, personality trait analysis, and privacy concern measurement. Attack-level characteristics encompass attack frequency and sophistication, targeting likelihood, and consequence severity. Vulnerability scores integrate these dimensions to provide comprehensive risk profiles enabling comparison across user populations and identification of high-risk groups.

4. Behavioral Pattern Recognition
Machine learning algorithms process survey responses and behavioral data to identify common patterns in oversharing behavior. Clustering analysis reveals distinct user profiles exhibiting different risk patterns. Classification models predict vulnerability levels based on observable characteristics and disclosed behaviors. Pattern analysis establishes relationships between platform features, psychological motivations, and disclosure quantities.

5. Intervention Strategy Evaluation
The research evaluates effectiveness of potential interventions through comparative analysis. Educational interventions are assessed for impact on risk awareness and behavioral changes. Technical interventions such as privacy controls and security features are evaluated for usability and protective effectiveness. Organizational and policy-based interventions are examined for feasibility and potential impact at scale.

6. Data Visualization and Reporting
Research findings are presented through interactive dashboards and visualizations enabling stakeholders to understand vulnerability distributions, identify high-risk populations, and evaluate intervention effectiveness. Heat maps display geographic and demographic vulnerability patterns. Risk profiles illustrate vulnerability across different information types and threat categories. Comparative visualizations demonstrate effectiveness of different mitigation approaches.

Key Technologies and Frameworks
The oversharing vulnerability assessment system integrates multiple technologies and theoretical frameworks to provide comprehensive analysis, interpretation, and communication of research findings.

Python serves as the primary analytical engine, with libraries including Pandas for data manipulation, NumPy for numerical computation, and scikit-learn for machine learning implementation. Python's extensive ecosystem facilitates preprocessing of survey data, statistical analysis, pattern recognition, and behavioral modeling.

SQL databases enable structured storage of survey responses, vulnerability assessment results, demographic information, and incident data. Relational database architecture ensures data integrity and enables efficient querying and analysis across multiple dimensions.

Power BI provides business intelligence and interactive visualization capabilities. Custom dashboards present vulnerability distributions, demographic risk profiles, comparative intervention effectiveness, and temporal trends. Filtering and slicing functionality enables stakeholders to explore data from multiple analytical perspectives.

Streamlit creates web-based interactive applications enabling users to input behavioral data, receive personalized vulnerability assessments, access educational resources, and explore protective strategies. The interface provides accessible entry points for diverse stakeholder groups.

Matplotlib and Plotly support creation of publication-quality visualizations and exploratory data graphics. These libraries enable illustration of complex relationships and pattern emergence from large analytical datasets.

The Social Cyber Vulnerability Index framework provides theoretical structure integrating individual-level psychological and behavioral factors with attack-level threat characteristics. This framework enables standardized vulnerability assessment and comparison across populations.

Protection Motivation Theory guides analysis of factors influencing users' adoption of protective behaviors. Privacy Calculus Theory explains the cost-benefit analysis underlying disclosure decisions. Dual-Process Decision-Making Theory contextualizes the conflict between immediate reward-seeking and rational risk evaluation in disclosure behavior.

Future Scope

The proposed oversharing vulnerability assessment framework establishes a comprehensive foundation for ongoing research and development in digital security and behavioral protection. Several promising directions for future enhancement and expansion warrant discussion.

Predictive modeling using advanced machine learning techniques represents a significant opportunity for future development. Deep learning algorithms analyzing multi-modal data including text, images, and metadata could predict vulnerability to specific threat types with higher accuracy. Predictive models might identify individuals at elevated risk for identity theft, social engineering, or exploitation, enabling targeted protective interventions.

Real-time monitoring systems could provide immediate feedback to users about privacy implications of contemplated disclosures. Browser extensions or platform-integrated tools might analyze draft posts, assess vulnerability impact, and suggest alternative phrasings that preserve intended communication while reducing exposure. Automated systems could identify common patterns indicating oversharing and recommend privacy adjustments.

Integration with platform application programming interfaces enables access to broader behavioral data and implementation of protective features at scale. Collaboration with social media platforms could facilitate research on algorithm modification, default privacy control changes, and user interface redesign to discourage harmful oversharing while preserving beneficial communication.

Personalized educational interventions delivered through machine learning systems could adapt content and presentation to individual learning styles, vulnerability profiles, and demographic characteristics. Gamification approaches and behavioral nudges might increase engagement with digital literacy materials and enhance protective behavior adoption.
Integration with organizational security frameworks could extend the system beyond individual users to protect organizational data. Employee vulnerability assessment and targeted training could reduce insider risk and social engineering-based breaches at organizational level.

Cross-platform analysis would enable comprehensive understanding of vulnerability across multiple social media services simultaneously. Users' aggregate disclosures across platforms create greater collective vulnerability than single-platform assessment suggests, warranting integrated analysis.
Advanced threat modeling could simulate specific attack scenarios using disclosed information, enabling users to understand concrete exploitation pathways and enhance protective motivation. Scenario-based learning might prove more effective than abstract vulnerability statistics in promoting behavior change.

IV. CONCLUSION

Oversharing on social media represents a critical and multifaceted cybersecurity challenge in contemporary digital societies. This research demonstrates that excessive disclosure of personal information creates documented, quantifiable vulnerabilities affecting billions of global users. The phenomenon results from complex interactions between platform design strategies that incentivize sharing, psychological mechanisms that prioritize short-term social rewards over long-term security considerations, and widespread digital literacy deficits.

The comprehensive framework presented in this study integrates behavioral analysis, vulnerability assessment, and protective strategy evaluation to address oversharing risks holistically. Our findings indicate that approximately 93% of individuals who engage in excessive social media sharing face tangible privacy and security threats. These threats extend across multiple dimensions including identity theft, social engineering exploitation, physical security compromise, and psychological manipulation through profiling and targeted content.

Technical solutions alone prove insufficient for addressing oversharing vulnerabilities. While encryption, authentication, and platform security features provide important baseline protections, these technical measures cannot prevent harm resulting from voluntary information disclosure. Comprehensive vulnerability reduction requires integrated approaches combining enhanced individual digital literacy, behavioral intervention strategies that leverage psychological understanding, platform design accountability, and policy-level initiatives mandating privacy protection as a fundamental user right.

The research demonstrates that awareness and education initiatives significantly improve users' risk perception and protective behavior adoption. Personalized vulnerability assessment tools help individuals understand their specific exposure profiles. Interactive decision-support systems enable more informed disclosure choices. Organizational interventions reduce social engineering vulnerability at scale. Implementation of evidence-based interventions addressing oversharing risks requires collaboration among multiple stakeholders including social media platforms, educational institutions, cybersecurity organizations, policymakers, and individual users. Platforms must accept accountability for design features encouraging harmful disclosure and implement meaningful privacy protection by default. Educational curricula must include comprehensive digital literacy components addressing oversharing risks beginning in early school years. Policymakers must establish regulatory frameworks protecting user privacy and limiting platform monetization of personal data.

This research contributes to the growing body of evidence demonstrating that social media oversharing culture presents serious, measurable threats to individual privacy, organizational security, and societal cybersecurity. By providing data-driven analysis, comprehensive vulnerability assessment frameworks, and evidence-based intervention strategies, the study equips stakeholders with tools necessary to reduce exposure and protect digital wellbeing. Future research extending this foundational work through predictive modeling, real-time intervention systems, and cross-platform analysis will further enhance our capacity to address this critical contemporary challenge.

REFERENCES

1. K. Möller and P. Valkenburg, "Online self-disclosure in social media: A new kind of self-presentation behavior," Computers in Human Behavior, vol. 110, pp. 45–58, 2023.
2. N. Bazarova and Y. Choi, "Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites," Journal of Communication, vol. 64, no. 4, pp. 635–657, 2014.
3. M. Omarzu, "Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity," European Journal of Social Psychology, vol. 30, no. 2, pp. 192–209, 2000.
4. Y. Lin, "Online self-disclosure: Behavioral patterns and psychological implications," Journal of Cybersecurity Research, vol. 45, no. 3, pp. 234–251, 2019.
5. Prime Tech Business, "Oversharing on social media: How it invades your privacy," Online Security Reports, August 2024.
6. Digital Footprint Check, "The hidden dangers of oversharing on social media: Complete 2025 privacy guide," Privacy and Security Reports, November 2025.
7. First Bank & Trust Company, "The risks of oversharing: Social media privacy 101," Financial Security Resources, August 2024.
8. Sibermate, "Beware! The risks of oversharing on social media," Cybersecurity Awareness Resources, January 2026.
9. IEEE Digital Privacy, "Privacy risks and social media," IEEE Digital Privacy Initiative, May 2025.
10. M. Tomlinson et al., "Understanding the complex interplay of social media privacy: Understanding oversharing and recommending future research," in Privacy and Security in Digital Communication, Springer Nature, 2025.
11. M. Mitra et al., "SCVI: Bridging social and cyber dimensions for comprehensive vulnerability assessment," Virginia Tech and George Mason University, 2025.
12. Frontiers in Psychology, "Neglecting long-term risks: Self-disclosure on social media and its relation to individual decision-making tendencies and problematic social-networks-use," Frontiers Research, October 2020.
13. MDPI, "Self-regulation of internet behaviors on social media platforms," MDPI Journals, October 2024.

14. ScienceDirect, "Tell me more: Longitudinal relationships between online self-disclosure, co-rumination, and psychological well-being," Social Media Studies, December 2024.
15. ResearchGate, "The influence of personality traits and social networks on the self-disclosure behavior of social network site users," Journal of Information Technology Research, June 2016.
16. A. Alturki et al., "Social cybersecurity: Understanding the interplay of social factors and cyber threats," Cybersecurity and Privacy Review, April 2025.
17. Springer Nature, "Social psychological barriers to accurate risk assessment in cyber security," in Cybersecurity and Psychology, Springer Nature, 2023.
18. MDPI Information, "Understanding social engineering victimization on social networking sites: A comprehensive review of factors influencing user susceptibility to cyber-attacks," MDPI Information Journal, February 2025.
19. ArXiv, "The social and psychological impact of cyber-attacks," Computer Science and Psychology, September 2019.
20. Springer Open, "Predicting individuals' vulnerability to social engineering in social networks," Cybersecurity and Risk Management, March 2020.