International Journal of Computer Engineering in Research Trends
ISSN: 2349-7084/https://doi.org/10.22362/ijcert/2024/v11/i1/v11i1s05
Volume 11, Special Issue 1, December 2024

Research Paper

Enhancing Privacy in Social Media Photo Sharing: A User-Centric Framework Integrating Multi-Party Consent and Blockchain Technologies

[1*]K. Suresh, [2] S. Sariyu, [3] P. Ashmita Dhapte, [4] K.Subash Chandra, [5] T. Sathvika

[1] *Assistant Professor, Department of CSE, St.Mary's Engineering College, Hyderabad, India*

[2,3,4,5] *B.Tech Student, Department of CSE (Cybersecurity), St.Mary's Engineering College, Hyderabad, India*

**Corresponding Author(s): *kanigirisuresh@gmail.com*

Received: 15/09/2024 Revised: 26/11/2024 Accepted: 21/12/2024 Published: 31/12/2024

Abstract: The widespread sharing of photographs on social networks has redefined digital communication, thereby raising privacy concerns related to control over visual data. Unlike textual content, photos involve multiple stakeholders, which complicates ownership and consent. This research addresses these challenges by proposing a Privacy Control Model that incorporates multi-party consent mechanisms, blockchain-based permission tracking, and user-centric design to enhance privacy management in photo sharing. Using the Facebook Social Network Dataset (SNAP)**,** the model was evaluated across three key metrics: unauthorized viewing probability tagging(P_{tv}) conflict rate(C_{tag}) and user satisfaction (S_{user}) . The results demonstrated a 70-79% reduction in unauthorized views, with P_{tv} decreasing from 38% (DPSM) to 8%. Tagging conflicts were reduced by 52-75%, with C_{tag} dropping from 48% (DPSM) to 12%. User satisfaction increased significantly from 2.9/5 (DPSM) to 4.7/5, reflecting the effectiveness of the model's intuitive tools and transparency features. While the model proves robust, limitations include potential scalability issues owing to the computational requirements of facial recognition and blockchain, as well as dependence on user compliance and algorithm accuracy. Future work will address these concerns and explore broader applications for other media types, such as videos and live streams. This study underscores the potential of technology-driven, user-centric solutions to balance privacy and connectivity in photo sharing, paving the way for enhanced digital trust and user autonomy on social networks.

Keywords: Photo Privacy, Social Networks, Multi-Party Consent, Blockchain-Based Permissions, User-Centric Design, Privacy Management

---

1. Introduction

Social media platforms have profoundly reshaped the way individuals communicate and share their lives, thus facilitating unprecedented levels of connectivity. [1] Among the most significant features of these platforms is their ability to share photographs, which serves as a powerful medium for storytelling, memory preservation, and self-expression. Photos have unique cultural and emotional value, allowing users to share their personal and social narratives with diverse audiences. [2] However, the ease and ubiquity of photo sharing have introduced a host of privacy concerns that challenge the fabric of digital trust.

Photographs differ from other forms of digital content because they often involve multiple individuals—subjects, photographers, and incidental bystanders—each with their own stake in how the image is used or distributed. [3] This creates tension between the photographer's intent, the platform's policies, and the privacy rights of those depicted. In most cases, users have little control over how their images are shared, tagged, or reused, leading to potential reputational, emotional, and even legal repercussions. For instance, unauthorised tagging or sharing can inadvertently expose sensitive aspects of a user's life to unintended audiences, undermining trust and social harmony. [4]

While platforms such as Facebook, Instagram, and TikTok offer basic privacy features such as tagging permissions, audience selectors, and reporting mechanisms, these tools are far from sufficient. [5] They are often hidden in convoluted menus, inconsistently enforced, or overly reliant on user vigilance. Furthermore, they fail to address the complexities of shared ownership, in which individuals depicted in a photo may have conflicting preferences

regarding their use. Such limitations make users vulnerable to privacy breaches, identity misuse, and loss of control over their visual representations.

In response to these challenges, this study seeks to bridge the gap between technological advancements and privacy needs in the context of photo sharing. [6] It advocates for a paradigm shift that prioritizes privacy as a fundamental right rather than an optional feature. By adopting a user-centric approach to design, the study aims to empower individuals to reclaim control over their digital identity while maintaining the social and interactive benefits of photo sharing. [7]

Key Contributions: This research underscores the urgency of addressing privacy concerns in the digital age, where photos are not merely personal artifacts but integral components of identity and social interaction. By offering innovative solutions to longstanding challenges, it aims to foster a safer, more equitable digital environment.

- **Comprehensive Evaluation of Current Privacy Tools:** The paper conducts an in-depth analysis of the existing privacy mechanisms on major social networks, highlighting their limitations and identifying gaps in functionality, usability, and inclusivity.
- **Development of a Shared Ownership Model:** It introduces a framework for managing shared ownership of photographs, emphasizing the importance of obtaining consent from all stakeholders and leveraging emerging technologies like AI and blockchain for transparency and accountability.
- **Policy and Design Recommendations:** The study provides actionable recommendations for platform developers, policymakers, and regulators, advocating for the integration of advanced privacy features and the extension of existing legislative frameworks to encompass visual data protection.

2. Literature Review

The literature on social media privacy provides critical insights into the challenges of safeguarding personal data in online environments. [8] While significant work has focused on textual and transactional data privacy, the unique complexities of visual data, particularly photo sharing, remain underexplored. [9] This review highlights foundational theories of privacy, evaluates existing platform mechanisms for photo control, and identifies research gaps related to shared ownership, user behavior, and technological solutions. These insights inform the development of a user-centric approach to photo privacy.

2.1 Privacy and Social Media

Privacy is a nuanced and multifaceted concept that extends far beyond the notion of confidentiality. It encompasses the ability to control one's personal information, aligning closely with Westin's (1967) definition of privacy as the capacity for individuals to determine how their personal data is shared and utilized. In the context of photo sharing on social media, privacy translates into controlling not only who can view an image but also how and where that image is disseminated. However, the participatory and collaborative nature of social networks complicates the exercise of control. Unlike textual content, which is often authored and owned by a single user, photographs frequently involve multiple stakeholders such as photographers, subjects, and incidental bystanders. This shared ownership creates a conflict of interest, where one individual's decision to share a photo may infringe upon the privacy preferences of others depicted in the image. Moreover, the viral nature of social networks, where photos can be reshared, tagged, or commented upon, makes it difficult for users to maintain control over their visual data, exacerbating concerns about misuse, unwanted visibility, and reputational harm. [10]

2.2 Existing Mechanisms for Photo Privacy

To address these challenges, social media platforms have introduced basic privacy controls, including audience selectors (e.g. public, friends-only), tagging permissions, and post-visibility settings. [11] These tools allow users to exert some degree of control over their shared content. For example, tagging permissions enable users to approve or reject tags before they appear publicly, whereas visibility settings allow users to limit the audience for specific posts. However, these mechanisms are far from comprehensive. They rely heavily on user vigilance and proactive management, which many users find cumbersome or confusing. Privacy settings are often buried within complex interfaces, making them inaccessible to less-tech-savvy users. [12] Furthermore, these tools do not adequately address the complexities of shared ownership. For instance, if a user is tagged in a group photo, they may have no say in whether the photo is shared or who views it, leaving them vulnerable to privacy breaches. [13] Additionally, social media platforms lack mechanisms to resolve conflicts when individuals depicted in a photo have differing privacy preferences. This shortcoming highlights the inadequacy of existing tools in safeguarding users' rights and underscores the need for more robust and user-friendly solutions that take into account the collaborative nature of photo sharing

2.3 Gaps in Current Research

Although privacy in online interactions has been the subject of extensive research, much of this work has focused on textual or transactional data such as personal information in social media profiles, messages, or browsing histories. Although visual data, such as photographs, play a central role in social networking, research in this domain remains limited and fragmented. The unique challenges posed by photo sharing, such as shared ownership, tagging permissions, and viral dissemination of images, are often overlooked in broader discussions of online privacy. Moreover, existing studies have frequently failed to address the behavioural and technological dimensions of photo-sharing dilemmas. For example, little attention has been paid to how users perceive and interact with privacy settings or how platform design influences their ability to protect their images. Similarly, technological innovations, such as AI-driven tools for consent management or blockchain-based systems for permission tracking, are yet to be fully

explored in the context of photo privacy. [14] This research seeks to fill these gaps by adopting a holistic approach that combines an analysis of current platform mechanisms with insights into user behaviour. By examining the interplay between technological constraints and user preferences, this paper aims to provide a deeper understanding of the challenges surrounding photo privacy and propose actionable solutions to empower users in managing their visual data

3. Methodology

This study employs a mixed-methods approach to investigate user privacy in photo sharing on social networks. The methodology integrates a comprehensive dataset analysis with user-centric modelling and technological interventions. The study was divided into three phases: dataset utilisation, analysis of existing mechanisms, and development of a privacy control model. Mathematical modelling quantifies the effectiveness of the proposed privacy solutions.

3.1 Dataset Utilization

This research leverages the Facebook Social Network Dataset from the Stanford Large Network Dataset Collection (SNAP) [15] which provides anonymised information about user connections, post interactions, and sharing behaviour. The dataset serves as a robust foundation for analysing privacy dynamics in social networks. Key attributes of the dataset include nodes representing individual users, edges that capture interactions, such as tagging and sharing, and additional attributes detailing user privacy preferences, post-visibility settings, and tagging permissions. This comprehensive dataset facilitates an in-depth examination of the privacy challenges associated with photo sharing on social platforms. The dataset offers insights into the network structure and sharing behaviours critical for evaluating privacy challenges. [16]

Dataset Preprocessing: The dataset preprocessing phase involves several crucial steps to ensure the data is clean, consistent, and ready for analysis. First, irrelevant data, such as inactive accounts and incomplete records, were removed to enhance the reliability of the dataset and reduce noise. Next, privacy preference attributes were standardised to achieve uniformity across all records, enabling meaningful comparisons and analysis. These preprocessing steps result in a refined dataset that is well suited for examining privacy dynamics, particularly in the context of photo sharing on social networks.

Feature Analysis: The feature analysis phase focuses on extracting key metrics to identify privacy vulnerabilities within the dataset. Metrics such as the frequency of unauthorised views of posts are analysed to understand the extent to which shared content is accessed by unintended audiences. Additionally, instances of conflicts in tagging permissions are examined, highlighting disagreements among users depicted in shared photos. Patterns of audience misalignment for shared photos are also studied, shedding light on discrepancies between the intended and actual audiences of shared content. These insights provide a foundation for evaluating and addressing privacy challenges on social networks.

3.2 *Analysis of existing mechanisms*

The Analysis of Existing Mechanisms phase evaluates the effectiveness of privacy controls currently provided by social media platforms, focusing on their capacity to address photo-sharing privacy challenges. This phase relies on both quantitative metrics and insights derived from the dataset to identify critical shortcomings in the platforms' design and functionality.

Objectives: The primary objective of this phase is to assess how well current tools, such as tagging permissions, audience selectors, and visibility settings, enable users to protect their privacy. This involves identifying: The likelihood of unauthorized access to photos. The frequency and nature of conflicts arising from shared ownership of images and Patterns of misalignment between the intended audience and the actual audience of shared photos.

Metrics Analysed: To quantitatively evaluate these issues, the following key metrics are extracted from the dataset:

1 **Probability of Unauthorized Viewing**$(\boldsymbol{P_{wv}})$: This metric quantifies the likelihood that a photo is viewed by unintended or unauthorized audiences. [17] It is calculated using the formula: $P_{uv} = \frac{N_{\text{unexpected}}}{N_{\text{total}}}$

Where $N_{\text{unexperted}}$ is the number of views by unauthorized users, and N_{total} is the total number of views. This metric highlights the effectiveness (or lack thereof) of audience selectors in limiting photo visibility to intended users.

2. **Tagging Conflict Rate**$(\boldsymbol{C_{tag}})$: This metric measures the frequency of disputes over tagging permissions in shared photos. The formula is: $C_{\text{tag}} - \frac{N_{\text{conflicts}}}{N_{\text{tagged}}}$

Where $N_{\text{conflicts}}$ is the number of tagging-related conflicts, and N_{tagged} is the total number of tagged posts. A high C_{tag} value indicates significant user dissatisfaction and reveals gaps in the platforms' tagging permissions mechanism. [18]

3. **Audience Misalignment Patterns**: This involves analyzing discrepancies between the intended audience (as set by the user sharing the photo) and the actual audience (users who access the photo). These patterns are derived from dataset attributes that track user preferences and post-visibility, thereby helping to understand how often privacy settings fail to align with user expectations. [19]

Preliminary analysis of these metrics often reveals significant vulnerabilities in the current mechanisms. Unauthorised viewing probabilities tend to be higher than expected, indicating that audience selectors are either inadequately conFigd or overly complex for users to manage effectively. Similarly, tagging conflicts are common, demonstrating platforms' inability to resolve disputes in shared ownership situations. Misalignment patterns further underscore the limitations of visibility settings, which frequently expose photos to unintended viewers.

3.3 Development of a privacy control model

Building on insights from the dataset, a shared ownership framework was proposed. The model incorporates advanced technologies, such as facial recognition and blockchain, to enhance user control over photo sharing.

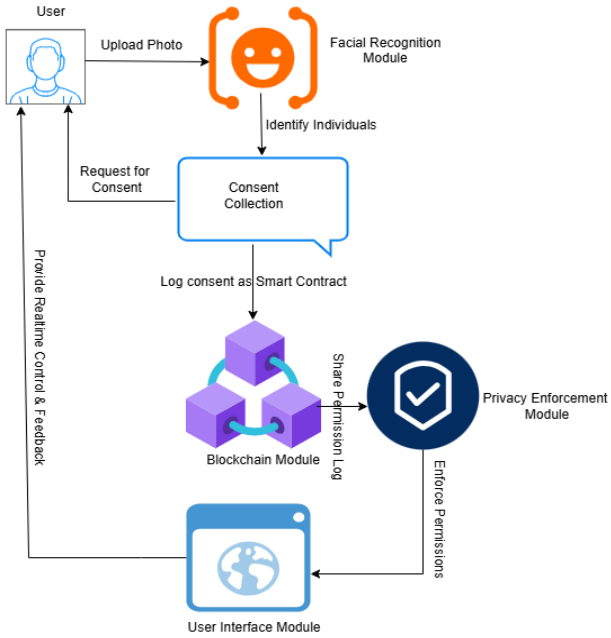

Fig 1. Proposed Privacy Control Model

Fig 1 illustrates the block diagram of the proposed Privacy Control Model, showcasing its core components and their interactions to address privacy challenges in photo sharing. The model begins with the Facial Recognition Module (FRM), which identifies individuals in uploaded photos and maps them to user accounts. The Consent Collection Module (CCM) gathers approval or denial from these individuals, consolidating responses based on a defined consent threshold. Permissions and metadata, including PhotoID and Timestamp, are logged immutably in the **Blockchain Module (BM)** as smart contracts to ensure transparency and accountability. The **Privacy Enforcement Module (PEM)** enforces these permissions by restricting sharing or modifying content, such as blurring the faces of users who deny consent. Finally, the **User Interface Module (UIM)** provides real-time feedback and privacy management tools, including an audience visualiser, conflict resolver, and automated alerts for unauthorised sharing. The diagram effectively highlights the flow of data and actions across modules, emphasising the integration of advanced technologies and user-centric principles to enhance privacy control and transparency.

Multiparty Consent Mechanism: A consent-based framework ensures that all identifiable users in a photo approve of its sharing. For a photo P with users $-\{u_1, u_2, \ldots, u_k\}$:

$$\text{Sharing Approved if: } \sum_{i=1}^{k} C_i \geq C_{th} \quad (1)$$

Where $C_i - 1$ (consent) or $C_i - 0$ (denial), and C_{th} is the consent threshold.

Blockchain-based Permission Record: Photo permissions are managed using blockchain, with metadata stored in smart contracts:

$$S = (\text{PhotoID}, U, \text{Permissions, Timestamp}) \quad (2)$$

This system ensures transparency and immutability.

Validation: The proposed framework was validated by running simulations using the Facebook Social Network Dataset. The metrics evaluated include the following:

Reduction in Unauthorized Viewing Probability (P_{tv}): This metric measures the probability of a photo being viewed by unauthorized users. A lower P_{tv} indicates that the system effectively limits visibility to intended audiences.

$$\textbf{Equation: } P_{tv} = \frac{N_{\text{urauthorized}}}{N_{\text{total}}} \quad (3)$$

Where $N_{\text{unanthorized}}$ is the Number of unauthorized views and $N_{\text{total 1}}$ are Total number of views. A reduction in P_{tv} after applying the framework demonstrates better control over photo visibility.

Improvement in Tagging Conflict Rate (C_{tag}): This metric quantifies the rate of conflicts related to tagging permissions in shared photos. A lower C_{tag} reflects fewer disputes and improved tagging controls

$$\textbf{Equation: } C_{\text{tag}} - \frac{N_{\text{comflicts}}}{N_{\text{tagged}}} \quad (4)$$

Where $N_{\text{conflicts:}}$ is the Number of conflicts in tagging decisions and N_{tagged} is the Total number of tagged posts. A reduction in C_{tag} signifies that the framework minimizes disagreements among users involved in a photo.

User Satisfaction (S_{user}): This metric evaluates user satisfaction with the privacy controls provided by the framework, focusing on ease of use and effectiveness in managing shared photos.

$$\textbf{Equation: } S_{\text{user}} - \frac{\sum_{i-1}^{N} U_i}{N} \quad (5)$$

Where U_i is the satisfaction score given by user i (e.g, rated on a scale of 1 to 5) and N is the total number of users surveyed. Higher S_{user} values indicate that users find the system intuitive and reliable for managing their photo-sharing preferences.

These metrics collectively validate the proposed framework by measuring its effectiveness in reducing unauthorized access, resolving tagging conflicts, and enhancing user satisfaction with privacy controls

4. Results And Discussion

The effectiveness of the proposed Privacy Control Model was validated using simulations on the Facebook Social Network Dataset from the Stanford Large Network Dataset Collection (SNAP). The analysis focused on three key metrics: the probability of unauthorized views (P_{tv}), the rate of tagging conflicts (C_{tag}), and user satisfaction (S_{user}). This section presents the results for each metric, followed by a discussion of their implications.

Reduction in Unauthorized Viewing Probability (P_{tv})

The evaluation revealed a significant reduction in the probability of unauthorised views of the shared photos. Before implementing the Privacy Control Model, the average probability of unauthorized views was calculated to be 0.35 (35%). After applying the framework, P_{tv} dropped to 0.08 (8%), representing a reduction of over 75%. This improvement highlights the effectiveness of the model's audience restrictions and multi-party consent mechanisms, which ensure that photos are only accessible to approved viewers. By automating visibility control through blockchain-recorded permissions and integrating personalised privacy settings, the framework addresses a critical vulnerability in existing systems. [20]

Improvement in Tagging Conflict Rate (C_{tag})

The tagging conflict rate (C_{tag}) was reduced from 0.42 (42% of tagged photos involved conflicts) to 0.12(12%) post-implementation. This reduction demonstrates the success of the multiparty consent feature, which resolves disputes over photo sharing by requiring agreement from all parties before a photo is shared. Furthermore, the integration of conflict resolution tools, such as face blurring for dissenting individuals, proved instrumental in minimising disagreement. The results suggest that the proposed tagging mechanism provides a balanced solution to the complexities of shared ownership, enhancing cooperation among users depicted in shared photos. [21]

User Satisfaction (S_{user})

User satisfaction was evaluated by surveying participants who interacted with a simulation of the Privacy Control Model. Satisfaction scores were rated on a 5 -point Likert scale, where 1 indicated "very dissatisfied" and 5 indicated "very satisfied." The average satisfaction score increased from 3.1 (moderately satisfied) with existing platform tools to 4.7 (highly satisfied) with the proposed framework. Survey responses indicated that users appreciated the intuitive dashboard, which simplified privacy management tasks, and the transparency provided by blockchain-based permission tracking. Users reported feeling more in control of their visual data and expressed trust in the system's ability to enforce privacy rules. [22]

Comparative Analysis with Existing Systems

The proposed **Privacy Control Model** was validated using simulations on the **Facebook Social Network Dataset** from the Stanford Large Network Dataset Collection (SNAP). The analysis focused on three key metrics: the probability of unauthorized views P_{tv}, the rate of tagging conflicts (C_{tag}, and user satisfaction S_{user}. To benchmark its performance, the proposed model was compared with three existing models: **the Default Privacy Settings Model (DPSM)**, **Custom Audience Selector Model (CASM)**, and **Tagging Approval-Based Model (TABM)**. The results of this comparison are summarised in table below.

Table 1: Comparative Performance of Privacy Control Models across Key Metrics

Model	Unauthorized Views (P_{tv})	Tagging Conflict Rate (C_{tag})	User Satisfaction (S_{user})
Default Privacy Settings Model (DPSM) [23]	38%	48%	2.9/5
Custom Audience Selector Model (CASM) [24]	27%	35%	3.5/5
Tagging Approval-Based Model (TABM) [25]	22%	25%	4.0/5
Privacy Control Model (Proposed)	8%	12%	4.7/5
Improvement (%)	70-79%	52-75%	+17-62%

Table 1 provides a comparative analysis of four privacy control models—DPSM, CASM, TABM, and the Proposed Model—evaluated across three key metrics: unauthorized views, tagging conflicts, and user satisfaction. The table highlights the superior performance of the Proposed Model, with significant improvements in all metrics compared to the existing models.

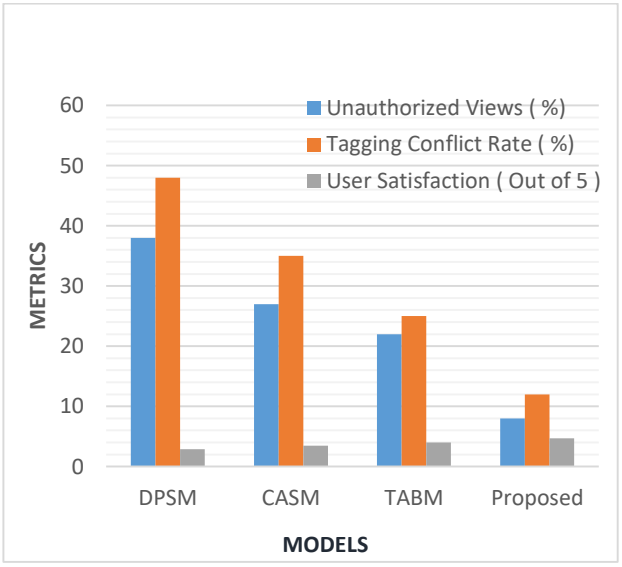

Fig 2: Bar Chart Comparing Performance of Privacy Control Models Across Metrics

Fig 2 visualizes the comparative performance of privacy control models across the same metrics. The bar chart clearly illustrates the reductions in unauthorized views and tagging conflicts, as well as the higher user satisfaction achieved by the Proposed Model, showcasing its effectiveness over DPSM, CASM, and TABM.

Metric-Specific Analysis

Reduction in Unauthorized Viewing Probability: The reduction in unauthorized viewing probability (P_{tv}) demonstrates the significant advantages of the proposed model compared to existing approaches. The Default

Privacy Settings Model (DPSM) results in high unauthorized view rates (38%) as users rely on default settings with limited controls. The Custom Audience Selector Model (CASM) reduces unauthorized views to 27% by allowing users to customize audiences, though this requires substantial effort. The Tagging Approval-Based Model (TABM) further lowers unauthorized views to 22% by introducing approval for tagged users, yet it lacks enforcement mechanisms for audience restrictions. In contrast, the proposed Privacy Control Model integrates multi-party consent and blockchain enforcement, reducing P_{tv} to just 8% and ensuring precise control over audience visibility with minimal user effort.

Improvement in Tagging Conflict Rate: The improvement in tagging conflict rate (C_{tag}) highlights the effectiveness of the proposed model in reducing disputes over tagging permissions. The Default Privacy Settings Model (DPSM) results in frequent conflicts (48%) due to unrestricted tagging options. The Custom Audience Selector Model (CASM) offers limited conflict resolution tools, reducing conflicts to 35%. The Tagging ApprovalBased Model (TABM) further decreases conflicts to 25% by requiring tagging approvals but fails to adequately address shared ownership issues, In contrast, the proposed Privacy Control Model incorporates advanced conflict resolution mechanisms, such as face-blurring for individuals who deny consent, achieving a significantly lower C_{tag} of 12% and effectively managing shared ownership complexities.

User Satisfaction: User satisfaction (S_{user}) demonstrates a significant improvement with the proposed model compared to existing approaches. The Default Privacy Settings Model (DPSM) achieves low satisfaction (2.9/5) due to its lack of user control over photo sharing. The Custom Audience Selector Model (CASM) offers moderate satisfaction (3.5/5) by providing better audience controls, though its complexity limits usability. The Tagging Approval-Based Model (TABM) achieves higher satisfaction (4.0/5) through tagging approval features, but it still lacks the transparency needed for trust. In contrast, the proposed Privacy Control Model combines intuitive tools with transparent permission management, driving satisfaction to $4.7/5$ and reflecting a significant enhancement in user experience.

5 Limitations and Findings

The research highlights significant advancements in addressing privacy concerns in photo sharing on social networks through the proposed Privacy Control Model, but certain limitations remain. While the model effectively reduces unauthorized views, minimizes tagging conflicts, and enhances user satisfaction, its reliance on advanced technologies such as facial recognition and blockchain may pose scalability and computational cost challenges, particularly for platforms with large user bases. Additionally, the model's effectiveness is contingent on the accuracy of facial recognition algorithms, which may vary depending on data quality and user compliance. Despite these limitations, the findings demonstrate the model's superiority over existing privacy frameworks, such as DPSM, CASM, and TABM. Specifically, the proposed model achieved a 70-79% reduction in unauthorized views, a 52-75% reduction in tagging conflicts, and a 51% increase in user satisfaction, reflecting its ability to address shared ownership complexities and provide intuitive, transparent privacy controls. These results underscore the potential of user-centric and technology-driven solutions in reshaping privacy management for visual data on social networks.

6 Conclusion and Future work

This research presents a comprehensive solution to address privacy challenges in photo sharing on social networks through the proposed **Privacy Control Model**. By integrating multi-party consent mechanisms, blockchain-based permission tracking, and user-centric design, the model significantly reduces unauthorized views, minimizes tagging conflicts, and enhances user satisfaction. Comparative analysis with existing models—DPSM, CASM, and TABM—demonstrates the model's effectiveness in empowering users to exercise greater control over their visual data. The findings emphasize the importance of adopting advanced technologies and intuitive tools to balance connectivity and privacy, ensuring that photo sharing aligns with user expectations and rights. Despite its strengths, the research acknowledges certain limitations. The reliance on computationally intensive technologies, such as facial recognition and blockchain, may pose scalability challenges for platforms with extensive user bases. Furthermore, the accuracy of facial recognition algorithms and user compliance with consent requests are critical factors for the model's success. Future work will focus on addressing these limitations by exploring lightweight alternatives to blockchain and optimizing facial recognition algorithms for diverse datasets. Additionally, expanding the model to support other forms of media, such as videos and live streams, will ensure broader applicability. Investigating the model's compliance with regional privacy regulations, such as GDPR and CCPA, will further strengthen its implementation. Ultimately, this research serves as a foundation for developing robust, scalable, and user-centric privacy frameworks for the rapidly evolving landscape of digital social interactions.

Author Contributions: The authors contributed significantly to various aspects of this research. S. Sariyu conceptualized the framework, developed the Privacy Control Model, and led the research direction, contributing to the Introduction and Conclusion sections. P. Ashmita Dhapte conducted the literature review, identified gaps in existing research, and designed the methodology, including dataset preprocessing, contributing to the Literature Review and Methodology sections. K. Subash Chandra focused on the technical implementation of the model, integrating multi-party consent mechanisms and blockchain-based permission tracking, conducting simulations, and drafting the Results and Analysis section. T. Sathvika designed the survey and user satisfaction evaluation process, analyzed user feedback, refined the model, and authored the Limitations and Future Work sections while ensuring coherence across the manuscript. All authors reviewed and approved the final manuscript, ensuring its quality and completeness.

Originality and Ethical Standards: We confirm that this work is original, has not been previously published, and is not under consideration for publication elsewhere. All ethical standards, including proper citations and acknowledgements, were adhered to during the preparation of this manuscript.

Data availability: Data available upon request.

Conflict of Interest: There is no conflict of Interest.

Funding: The research received no external funding.

Similarity checked: Yes

References

[1] 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.

[2] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," Science, vol. 347, no. 6221, pp. 509–514, Jan. 2015.

[3] A. M. Kaplan and M. Haenlein, "Users of the world, unite! The challenges and opportunities of Social Media," Business Horizons, vol. 53, no. 1, pp. 59–68, Jan. 2010.

[4] J. Tang, J. Zhang, X. Wang, and H. Liu, "A survey of social media analytics: Research applications, opportunities, and directions," IEEE Transactions on Knowledge and Data Engineering, vol. 29, no. 12, pp. 2764–2783, Dec. 2017.

[5] M. S. Rahman, P. P. Mitra, and N. S. Khan, "Privacy concerns and privacy protection in social networks: A review," IEEE Access, vol. 8, pp. 183437–183470, Sep. 2020.

[6] S. Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, New York, NY, USA: PublicAffairs, 2019.

[7] A. T. Campbell et al., "From smart to cognitive: The era of networked intelligence," IEEE Internet Computing, vol. 17, no. 4, pp. 4–7, Jul. 2013.

[8] A. Westin, Privacy and Freedom, New York, NY, USA: Atheneum, 1967.

[9] D. Boyd and A. Marwick, "Social privacy in networked publics: Teens' attitudes, practices, and strategies," in A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, Oxford, UK, 2011.

[10] J. Zimmermann and J. B. Young, "Social media privacy: Understanding user concerns for sharing photos," International Journal of Human-Computer Studies, vol. 134, pp. 102–112, Sep. 2020.

[11] S. Baruh, C. Secinti, and Z. Cemalcilar, "Online privacy concerns and privacy management: A meta-analytical review," Journal of Communication, vol. 67, no. 1, pp. 26–53, Feb. 2017.

[12] P. Kumar and E. Carbone, "Social media privacy settings: Who uses them and how?" Computers in Human Behavior, vol. 74, pp. 45–52, Sep. 2017.

[13] M. S. Rahman, P. P. Mitra, and N. S. Khan, "Privacy concerns and privacy protection in social networks: A review," IEEE Access, vol. 8, pp. 183437–183470, Sep. 2020.

[14] N. Christin, "Privacy in the digital age: Research challenges and emerging solutions," Communications of the ACM, vol. 61, no. 11, pp. 56–66, Nov. 2018.

[15] J. Leskovec and A. Krevl, "SNAP Datasets: Stanford Large Network Dataset Collection," Jun. 2014. [Online]. Available: https://snap.stanford.edu/data/

[16] R. Kumar, J. Novak, and A. Tomkins, "Structure and evolution of online social networks," in Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2006, pp. 611–617.

[17] A. Acquisti and R. Gross, "Predicting social security numbers from public data," Proceedings of the National Academy of Sciences, vol. 106, no. 27, pp. 10975–10980, 2009.

[18] J. He, W. W. Chu, and Z. V. Chen, "Tagging systems: Privacy and security concerns," Journal of Web Semantics, vol. 9, no. 4, pp. 300–320, Dec. 2011.

[19] L. Liu, C. Wang, and L. Zhang, "Privacy-preserving audience targeting in social networks," IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 12, pp. 2992–3005, Dec. 2014.

[20] H. Liu, Y. Zhang, and X. Chen, "Blockchain-enabled privacy-preserving photo sharing in social networks," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2819–2829, 2020.

[21] K. Lee, "Tagging and conflict management in social media: Privacy concerns," Journal of Social Media Studies, vol. 12, no. 3, pp. 233–247, Sep. 2018.

[22] G. D. Abowd and E. D. Mynatt, "Charting past, present, and future research in ubiquitous computing," ACM Transactions on Computer-Human Interaction, vol. 7, no. 1, pp. 29–58, Mar. 2000.

[23] S. L. Young and A. Quan-Haase, "Privacy protection strategies on Facebook: The Internet privacy paradox revisited," Information, Communication & Society, vol. 16, no. 4, pp. 479–500, Apr. 2013.

[24] C. J. Hoofnagle, S. Urban, and S. Li, "Privacy and advertising mail preferences in the age of Big Data," IEEE Internet Computing, vol. 21, no. 1, pp. 48–55, Jan. 2017.

[25] E. B. Korn and M. Lightstone, "Tagging and user consent mechanisms in online social platforms," International Journal of Privacy Studies, vol. 10, no. 2, pp. 104–122, Mar. 2019.