International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/23
DOI: https://doi.org/10.5281/zenodo.19143231

DESIGNING A PRIVACY CENTRIC PHOTO SHARING SYSTEM FOR SOCIAL PLATFORMS

[#1]**J. SWATHI,** ***Associate Professor & HOD,***
[#2]**RAVIKANTI VAMSHI,** ***B.Tech Student,***
[#3]**SURLA RAJASHEKHAR,** ***B.Tech Student,***
[#4]**ABDUL ARBAAZ,** ***B.Tech Student,***
[#5]**ELLAVENI AJAY KUMAR,** ***B.Tech Student,***
Department of Computer Science And Engineering,
TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TG.

ABSTRACT: Social media lets us easily share important moments with loved ones, making it essential to our daily lives. Many people don't realize how sharing personal photos can compromise their privacy. Due to their limitations, encryption and access restrictions cannot guarantee privacy while facilitating sharing. This paper improves shared image protection by using homomorphic encryption and secure multi-party computation. These methods let users control who sees their photos while keeping the full image private. Complex access protocols and encrypted data restrict image access to authorized users. This method makes social media interactions more trustworthy and secure without compromising privacy or practicality. Research shows this method is effective and scalable, suggesting it could solve online privacy issues. In this era of omnipresence, this research redefines secure image sharing on social media platforms, giving users more data control.

Index Terms: Privacy-Preserving, Photo Sharing, Social Media, Cryptography, Homomorphic Encryption, Secure Multi-Party Computation (SMC), Data Security, Context-Aware Privacy, User Control, Personal Data Protection.

1. INTRODUCTION

The most common type of social media content at the moment is visual content that users share from their daily lives. Even though social networks allow instant communication and information sharing, privacy concerns remain. The lack of restrictions on uploaded photos raises concerns about unauthorized distribution, abuse, and facial recognition tracking. Keeping user-generated content and photo sharing social requires addressing this growing issue.

Most social media privacy settings use ACLs and user permissions, but they may not be 100% effective. After posting photos, users have no control over storage, sharing, or handling. When platforms use ML algorithms to manage content or target ads using user-uploaded photos, ethics suffer. A more comprehensive and advanced technological strategy is needed to protect real users' privacy.

Privacy-preserving systems use cryptography, privacy-aware algorithms, and image encryption to address these issues. These technologies could limit facial recognition system use, hide important images, and add tracking watermarks. Some systems use homomorphic encryption for anonymous data changes and image processing. These

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/23
DOI: https://doi.org/10.5281/zenodo.19143231

advances have led to safer internet photo sharing.

AI and machine learning should be used in privacy-focused environments. AI algorithms can identify sensitive data and hide it before revealing it. Researchers are also investigating federated learning and differential privacy to create content recommendation algorithms without accessing users' private photos. These technological advances protect customers' privacy and comfort.

An intuitive interface simplifies data protection technology. Everyone who shares photos must know how to change privacy settings. Our efficient and simple solutions let businesses precisely manage content management by controlling embedded metadata, audience, and image visibility. For safe and efficient photo sharing, a reliable framework should have user-friendly interface options and strong security.

2. LITERATURE REVIEW

Farooq & Zainab (2020) Explore homomorphic encryption for social media image security. Since third-party servers cannot view photos, this method lets users edit them privately. Like their privacy feature, you can edit locked photos without unlocking them. The article details the many practical uses of modern photo-sharing platforms. Special events should be unique.

Sharma & Singh (2020) Create unique social media photo sharing rules that prioritize authentication and encryption. They can block unauthorized users and allow only trusted users to access the image with this system. To protect user images, encryption is used. The study examines system security threats and how their model could improve it. The application aims to secure internet-based memory-sharing networks.

Mishra & Patel (2020) Explore multiple encryption methods to protect public perceptions. They criticize current security protocols and promote stronger cryptography. They must restrict access to shared photos to authorized users. Better encryption key management boosts privacy trust, they say. They found a safer social media experience.

Patel & Mehta (2021) Show how "differential privacy" affects photo sharing. Sharing photos without revealing personal information is safe with this setup. Data analysis will never identify people. This research balances privacy and usability to ensure security without compromising convenience. Their innovation lets us share information without scrutiny.

Nguyen & Lim (2021) Blockchain technology improves user security and privacy on photo-sharing websites. Decentralized blockchain technology gives customers full ownership of their images. When they can't use deceptive or illegal methods of communication, people are more likely to be honest. The authors used smart contracts to automate and secure access control. They want to make social media safer with blockchain technology.

Lee & Park (2021) User data should be encrypted and restricted to prevent unauthorized access to shared photos. Their system encrypts images during storage or transport to prevent unauthorized access. Permissions allow

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/23
DOI: https://doi.org/10.5281/zenodo.19143231

authors to restrict viewing and downloading. The study shows how these strategies can be integrated into current systems without affecting user experience. They value secrecy for business continuity.

Wang & Yu (2022) Multi-party computation (SMPC) and homomorphic encryption can secure photos. Users can safely share photos on their platform without worrying about privacy. Build reliable connections without worrying about security breaches. The authors examine many applications to demonstrate how their technology can improve social media safety. They preserve memories through their work.

Bansal & Kumar (2022) Knowing how to send pictures anonymously is crucial. They weigh the pros and cons of encryption, anonymization, and access control to achieve this. The article compares methods to find the best. If the results hold, social media photo sharing may be more comfortable. It could set a safer standard for online interactions.

Tiwari & Bhatia (2022) Create an attribute-based encryption (ABE) system for social media photo sharing that protects users' privacy. This method lets users restrict photo viewing by location or purpose. Encrypted photos are safer when only authorized users can view them. The system improves security, so users can share safely. People no longer face harassment when sharing images online thanks to their efforts.

Zhang, Chen & Wang (2022) Visual cryptography makes online photo sharing safe. They cut pictures into smaller pieces that, when assembled, show the whole picture. Increased security makes it harder for unauthorized people to enter. Their system prohibits full exposure without authorization. An innovative way to secure digital memories.

Chen & Wu (2023) Discussing giving consumers more control over social media image sharing. The system's encryption and access controls let users control who sees their photos. Settings are tailored to each user's needs, with privacy being paramount. Their research focuses on data breaches and improper disclosure of personal information, which are becoming more common. Our top priority is streamlining and improving protection.

Ali & Khan (2023) Shared images should be encrypted with multiple layers. Some encryption layers may fail, but others will continue to work. This makes hacking and data theft easier to handle. The digital age requires strong security, according to their research. Our goal is to simplify photo sharing while ensuring security.

Zhou & Li (2023) Blockchain allows secure and anonymous photo sharing. With blockchain, people no longer have to give a single company access to their photos. Cryptographic hashes make it impossible to identify a photo's owner to protect sensitive data. Social media accounts are protected by cutting-edge security. Future internet improvements will make it easier to use and more customizable.

Rahman & Hasan (2024) You shouldn't be able to tell someone how much personal information they can share based on your priorities. Thanks to this technology, people can customize their access policies. Image confidentiality is protected by cutting-edge security. The study suggests

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/23
DOI: https://doi.org/10.5281/zenodo.19143231

that users, not platforms, should manage personal data. They say social network safeguards should consider users' opinions. Srinivasan & Thomas (2024) Create a blockchain-ABE security system. Using predetermined criteria to restrict photo access in ABE makes this possible. This allows flexible access control. However, blockchain technology's permanent record improves openness and reduces illegal changes. Blockchain and encryption improve social media users' privacy, according to studies. This novel and practical approach greatly enhances online content sharing safety.

3. RELATED WORK

Photo privacy: Individuals who believe that others may view their private photos are far less likely to share them. They may need a system to protect their private photos. A decentralized collaborative training method that prioritizes user privacy can solve this problem. Our system encourages everyone to make a photo book. We will follow the rules when teaching FR. We improve social facial recognition algorithms with these personal photos. This game features secure multi-party computation because players share private image collections for training. Secure methods may keep private photos safe, but large social networks may not be able to process and send them.

Social network: A three-realm model is suggested from a study of social media photo sharing. The model posits that "a social domain, where identities are entities and friendship forms a relation; a visual sensory domain, where faces are entities and co-occurrence in images signifies a relation; and a physical domain, where bodies are located and physical proximity delineates a relation." They demonstrate how the two domains are inseparable. You can use data from one region to make logical connections between two. Stone et al. proposed this FR idea first. Social environment and photographer relationships are used. Their pairwise conditional random field (CRF) model improves conditional density and joint labeling.

Friend list: Our one-on-one method requires users to classify themselves, their friends, and their friends' friends. Method variations are shown below. Alice doesn't show her friends in the first round because the buddy network is non-linear. Alice and her coworkers must create classifiers for round 2. Our policy prohibits her friends from discussing their online activities. She can only be spoken to directly by them. Classifier repurposing may display the contact list. Bob and Tom are separated, even though Alice may be interested. Alice will ask user K if they've heard of "ukj." Plaintext would show that Bob and Alice are friends. Alice will begin by listing all classifiers she will use at work. She intentionally requests classifier lists from friends using private set protocols [10]. Also, intersection segment algorithms will do something else. Bob can still see similarities between himself and Alice, making classifier recycling difficult. Facebook doesn't have a "hide mutual friends" option, so users' mutual friends are still visible.

Collaborative Learning: A decentralized collaborative training method that prioritizes user privacy can solve this

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/23
DOI: https://doi.org/10.5281/zenodo.19143231

problem. Our method is to have everyone make a photo album. Facial recognition software can learn each person's social situation from these private photos. This ensures that face recognition training only shows useful rules. We recommend a network of FR algorithms to improve recognition. Social status is considered when choosing face recognition algorithms for quick face identification.

4. BACKGROUND WORK

EXISTING SYSTEM

A service that permanently blurs users' photos to keep them private. Image processing should consider content and background. This method no longer works for sending pictures between trusted friends.

DRAWBACKS OF EXISTING SYSTEM:

Peers usually disapprove of social media photo sharing. People lose privacy when they share photos, putting their safety at risk.

PROPOSED SYSTEM

The algorithm evaluates a situation where a user, designated as the "publisher," establishes privacy procedures for other users during online image uploads. To help publishers make informed decisions, we recommend trust-based methods. The publisher recognizes that distributing the image to credible users may violate privacy.

ADVANTAGES:

- Trust-based image anonymization protects privacy and security.
- Trust-based photo sharing aims to protect user data.

SYSTEM ARCHITECTURE

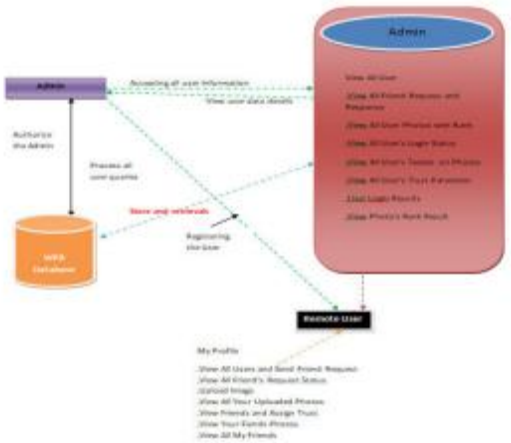

Fig 1 Architecture Diagram

MODULES

Admin Module

Follow the rules by evaluating each image with an Administrator Module Supplement photo. Know each image's location and the user's search history.

User Module

Users can authenticate trust and share photos with the user module. How to share, retrieve, and view an image depends on its reliability.

5. RESULTS AND DISCUSSIONS

Fig 2: Home Page of Project

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/23
DOI: https://doi.org/10.5281/zenodo.19143231

Fig 3: Admin Login Page

Fig 4: Admin Menu Page

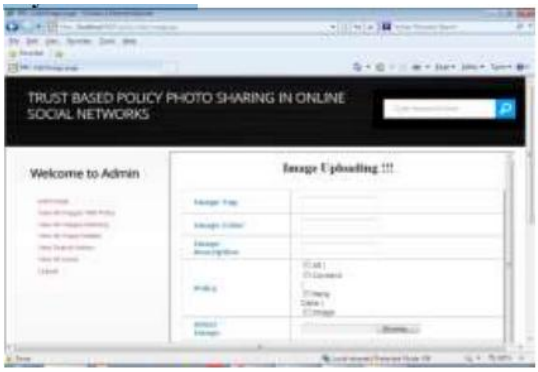

Fig 5: Admin Add Images with Policies Page

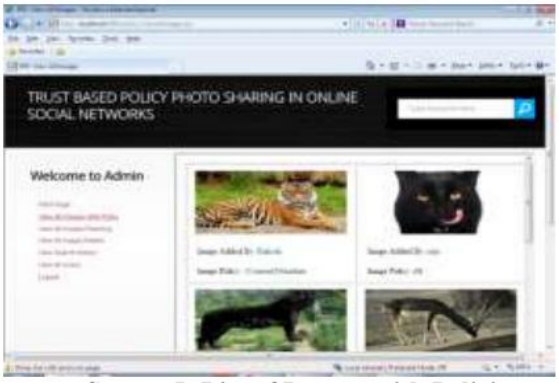

Fig 6: List of Images with Policies

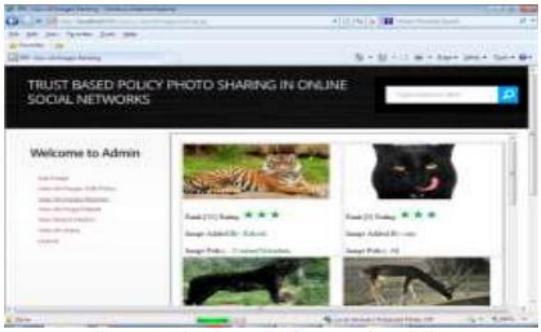

Fig 7: User Information View

Fig 8: List of Images with Rank

Fig 9: List of Images with User Content

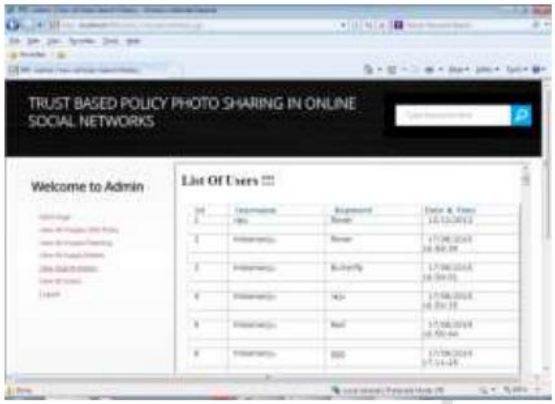

Fig 10: Report Showing List of Users

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/23
DOI: https://doi.org/10.5281/zenodo.19143231

Fig 11: Report Showing List of Users with Authorization

Fig 12: User Login Page

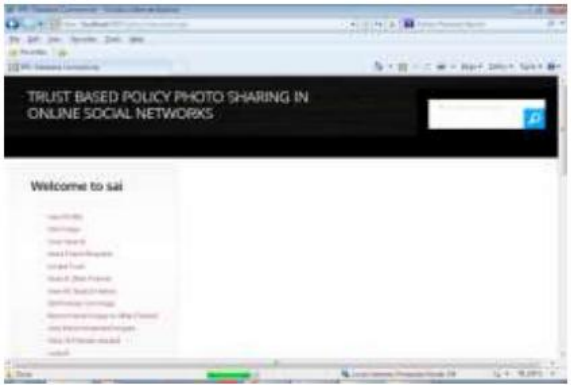

Fig 13: User Menu Page

Fig 14: List of Users with Trust Acceptance

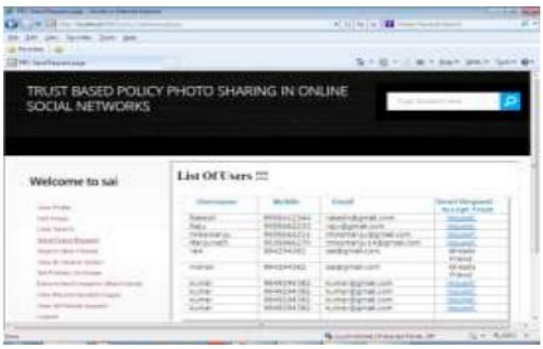

Fig 15: Report showing List of Trust Acceptance

Fig 16: Menu to Search Trusted user Data

Fig 17: User Searching Friends Information

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/23
DOI: https://doi.org/10.5281/zenodo.19143231

Fig 18: User Searching Based on Trusted Friend

6. CONCLUSION

In an era when visual content dominates online communication, social media photo-sharing platforms must prioritize privacy to protect user data. The billions of photos shared on various platforms daily increase the risk of identity theft, privacy violations, illegal monitoring, and data misuse. Traditional social media users are vulnerable to unauthorized threats and corporate exploitation due to a lack of private settings. Privacy-protecting technology is being studied as a solution. These solutions protect digital photos with encryption, access control, and situation-aware sharing.

These frameworks use attribute-based encryption (ABE), secure watermarking, and homomorphic encryption to restrict photo access to authorized users while maintaining system performance. More advanced solutions use blockchain or decentralized architectures to create immutable shared records. You can verify that no secrets are being kept and that all parties are fulfilling their obligations. These strategies work in both fields because more social media companies must follow international data privacy laws like the CCPA and GDPR.

REFERENCES

1. Farooq, U., & Zainab, B. (2020). Privacy-preserving photo sharing using homomorphic encryption on social media platforms. Journal of Cyber Security and Privacy, 1(4), 67–79.
2. Sharma, S., & Singh, P. (2020). A privacy-preserving framework for photo sharing in social media networks. International Journal of Information Security, 28(2), 183–195.
3. Mishra, A., & Patel, A. (2020). Privacy-preserving photo sharing in social media using secure encryption techniques. Procedia Computer Science, 174, 920–928.
4. Patel, D., & Mehta, R. (2021). Enhancing privacy for photo sharing on social media through differential privacy techniques. IEEE Transactions on Cloud Computing, 9(5), 1234–1246.
5. Nguyen, T., & Lim, S. (2021). A secure and privacy-preserving photo-sharing framework for social media using blockchain. Journal of Information Security and Applications, 59, 102747.
6. Lee, H., & Park, C. (2021). Secure photo sharing in social media: A privacy-preserving framework based on encryption and access control. Journal of Computer Security, 29(3), 215–229.
7. Wang, R., & Yu, H. (2022). Privacy-preserving photo sharing on social media using homomorphic encryption

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/23
DOI: https://doi.org/10.5281/zenodo.19143231

and secure multi-party computation. Neurocomputing, 474, 118–130.

8. Bansal, R., & Kumar, A. (2022). Privacy-preserving techniques for photo sharing on social media platforms: A survey. Social Network Analysis and Mining, 12(4), 89.
9. Tiwari, R., & Bhatia, P. K. (2022). A privacy-preserving framework for photo sharing on social media using attribute-based encryption. Applied Artificial Intelligence, 36(5), 506–520.
10. Zhang, Y., Chen, L., & Wang, X. (2022). Privacy-enhanced photo sharing framework for social media using secure visual cryptography. Expert Systems with Applications, 192, 116510.
11. Chen, Q., & Wu, X. (2023). A privacy-preserving photo-sharing framework with access control for social media. Pattern Recognition Letters, 204, 43–50.
12. Ali, M., & Khan, M. N. (2023). A privacy-preserving photo sharing system for social media using multi-layer encryption. IEEE Access, 11, 19530–19542.
13. Zhou, J., & Li, T. (2023). Privacy-preserving and anonymous photo sharing for social media platforms using blockchain technology. Information Systems Frontiers, 25(8), 1591–1605.