International Journal of
ADVANCED RESEARCH & INNOVATIONS

Volume 15, Issue-1
Jan, 2025, P04
ISSN: 2319-9253

PRIVACY-PRESERVING PHOTO SHARING FRAMEWORK FOR SOCIAL MEDIA

#[1]Reddy Akhila, #[2]Solleti Tejashwini,
[1]MCA Student,Mca, Vaageswari College of Engineering (Autonomous), Karimnagar, Telangana.
[2]Assistant Professor, Department of Mca,Vaageswari College of Engineering (Autonomous), Karimnagar, Telangana.,

Abstract: Social media is a big part of our daily lives now that it's so easy to share special moments with friends and family. There is a sizable portion of the user base that is unaware of the potential privacy issues that can arise from the careless sharing of personal images. It is challenging to ensure the security of private information while also making sharing easy, because existing privacy solutions, such as encryption and access restrictions, have their limitations. A more robust method for protecting shared images is developed in this paper by employing more advanced cryptographic techniques such as secure multi-party computing and homomorphic encryption. Users are able to control who can view and utilize their images using these ways, all while keeping the full picture hidden. Encrypted data and intricate access rules allow only authorized users to view specific portions of an image. While preserving privacy and practicality, this strategy makes social media interactions safer and more trustworthy. The approach may be a solution to the current issues with digital privacy since empirical investigations have demonstrated its efficacy and scalability. Giving users greater agency over their data in an era where it's pervasive, this research alters the meaning of securely sharing images on social media platforms.

Keywords: 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

Visual content from people's everyday life is currently the most popular type of content to share on social media. There are legitimate concerns regarding users' privacy, despite the fact that people may communicate and share information on social networks instantly. Having unfettered access to uploaded photographs raises concerns about misuse, unauthorized distribution, and the possibility of tracking individuals through facial recognition technology. We must act decisively against this rising problem if we want picture sharing and user-generated content to retain their social aspects.

The majority of social media privacy settings rely on ACLs and user permissions, which may not offer complete security in all cases. After images are posted, users have no say over how they are handled, saved, or shared. From an ethical standpoint, things become much more problematic when platforms utilize machine learning algorithms to examine user-uploaded photographs for the sake of targeted advertisements or content management. This indicates that a more comprehensive and technologically sophisticated approach is necessary to secure true user privacy.

Photo encryption, cryptographic techniques, and privacy-aware algorithms are some of the ways that privacy-preserving systems handle these problems. Limiting access to facial recognition systems, hiding crucial image elements, and watermarking content for tracking are all possible with these technologies. To facilitate protected image processing and to ensure user anonymity during data changes, certain systems employ homomorphic encryption. Now that these improvements have taken place, there are more secure ways to send pictures online.

Artificial intelligence and machine learning should be utilized in settings that place a high emphasis on the privacy of its users. Algorithms driven by artificial

Volume 15, Issue-1
Jan, 2025, P04
ISSN: 2319-9253

intelligence can uncover sensitive data, which can subsequently be masked or concealed before being disseminated. In order to develop content recommendation algorithms that do not directly access people's personal images, researchers are also investigating federated learning methods and differential privacy. These technological advancements allow for the preservation of customers' comfort while simultaneously safeguarding their privacy.

An improved user interface can facilitate the usage of technology to safeguard personal information. Everyone who shares images has to know what their privacy settings are and how to adjust them. Simple and effective, our solutions empower businesses to take charge of their content management by providing fine-grained control over picture visibility, audience, and embedded metadata. So that photo sharing is both safe and rapid, a decent framework should have stringent security measures and user-friendly interface choices.

2. Literature Review

Farooq & Zainab (2020) Investigate an alternative method of securing social media images using homomorphic encryption. This technique allows users to edit their images privately, shielding them from view by third-party servers. Their privacy enhancement is analogous to being able to edit a locked photo without having to unlock it. Practical applications of contemporary photo-sharing platforms are extensively examined in the article. The objective is to maintain the distinctiveness of special events.

Sharma & Singh (2020) Create an original set of protocols for securing photo sharing on social media platforms, with an emphasis on authentication and encryption. Using this system, they can guarantee that only reliable individuals will be able to view the image, while also preventing unauthorized access. The security of users' images is ensured by employing stringent encryption technologies. In order to improve system security, the research examines existing risks and how their model could be used. The program's objective is to make memory-sharing networks on the internet more secure.

Mishra & Patel (2020) Look into various types of encryption to ensure the security of public images. They prove that current security methods are inadequate and advocate for more robust cryptographic resources. Their efforts ensure that only authorized users can view shared photos and prevent unauthorized users from accessing them. Their view is that better management of encryption keys is crucial, since it increases confidence in privacy. They discovered that it is feasible to enjoy a less risky time on social media.

Patel & Mehta (2021) Define the term "differential privacy" in the context of photo sharing. This setup guarantees that users can safely share photos without disclosing any personal details. No amount of data analysis could ever lead to the identification of specific individuals. Finding a happy medium between privacy and usability, where security isn't sacrificed for convenience, is the subject of this research. You can communicate data without fear about being caught using their technology.

Nguyen & Lim (2021) Sites that allow users to exchange images can make them more secure and private by incorporating blockchain technology. Because blockchain is decentralised, consumers retain complete control over their images. People are more inclined to be truthful when they know they can't get away with deceitful or unlawful communication tactics. The authors used smart contracts to implement automatic and secure access control. As part of their strategy to enhance the security of social media platforms, they intend to integrate blockchain technology.

Lee & Park (2021) Encrypt user data and restrict access to prevent unauthorized users from viewing their shared photos. By encrypting images in transit and storage, their system reduces the likelihood of illegal access. Authors can manage who can view and download their work by assigning certain permissions. Findings from the research demonstrate how these tactics can be integrated into preexisting systems without negatively impacting user experience. While keeping their company functioning efficiently, they place a premium on discretion.

Wang & Yu (2022) Secure multi-party computation (SMPC) and homomorphic encryption can be used to enhance the security of your photographs. With their system, users may securely share photos without worrying about others viewing them. Without worrying about data breaches, we may create trusting relationships in this way. The authors consider various applications of their technology to demonstrate its potential for enhancing social media safety. Particular memories are kept alive through their work.

Bansal & Kumar (2022) Learning a great deal about the various methods of sending photos while maintaining anonymity is crucial. While doing so,

Volume 15, Issue-1
Jan, 2025, P04
ISSN: 2319-9253

they weigh the benefits and drawbacks of various approaches to encryption, anonymization, and access their findings pan out, users may feel more comfortable uploading photos to social media. In the future, it might serve as an example of how to make online interactions safer.

Tiwari & Bhatia (2022) Develop a privacy-preserving approach to sharing images on social media platforms using attribute-based encryption (ABE). Using this approach, which takes into account things like location or purpose, users can choose who can view their images. Security is enhanced by ensuring that the encrypted photographs can only be viewed by authorized individuals. People can still share safely within the system's framework, which is supposed to make it safer. Thanks to their actions, individuals no longer have to fear being bullied when they upload images on the internet.

Zhang, Chen & Wang (2022) Secure photo sharing is possible using a certain kind of visual cryptography. They fragment photographs into tiny bits that, when assembled, reveal the full image. Because of this additional safeguard, it will be more difficult for unauthorized individuals to gain access. Their system guarantees that no one can be fully exposed unless the required authorizations are acquired. Yet another ingenious strategy to prevent the theft of digital memories.

Chen & Wu (2023) Discussing providing clients greater control over how they publish images on social media. The system comes with built-in encryption and access controls, so users can choose exactly who can see their photos. The settings are designed to cater to each user's needs, and privacy is prioritized. Data breaches and unauthorized sharing of personal information are becoming increasingly common, and their research primarily focuses on the issues that arise from these situations. Improving and streamlining the protection procedure is our top priority.

Ali & Khan (2023) The usage of multi-layer encryption to protect shared photographs is strongly encouraged. If an encryption layer were to fail, the remaining layers would continue to function normally. Protecting against cyber dangers, such as hacking and illegal data access, is made easier with this. Their research highlights the significance of robust security measures, particularly in today's digital age. Ensuring the safety of photo sharing while also reducing unnecessary complexity is our aim.

control. In order to determine the most effective approach, the article compares various methods. If Zhou & Li (2023) Secure and anonymous photo sharing is possible with blockchain technology. People no longer have to trust any one entity with their images thanks to the distributed ledger technology known as blockchain. Because of the additional protection that cryptographic hashes provide, it is now physically impossible to determine who owns an image. When it comes to social media privacy concerns, their method employs cutting-edge security protocols. The internet is going to get better, more user-centered, and more personalized in the future.

Rahman & Hasan (2024) People should be given the ability to select how much information they wish to disclose and how much privacy they value. People can choose their own access rules according to their preferences with this technology. To guarantee the confidentiality and safety of images, they employ cutting-edge security measures. The findings of the research provide credence to the argument that personal data management responsibilities should lie with users and not with platforms. They argue that users' perspectives should be considered while designing social network security.

Srinivasan & Thomas (2024) Construct a two-tiered security system utilizing blockchain technology and attribute-based encryption (ABE). The ability to easily limit photo access to specific users based on established criteria is a feature of ABE that makes this possible. This allows for more adaptable access control. Blockchain technology, on the other hand, prevents unlawful alterations and makes everything more transparent due to its immutable record. There is research that demonstrates how users' privacy on social media platforms can be enhanced with the utilization of blockchain technology and encryption. Using this ingenious and practical approach, sharing content online is much safer.

3. Related Work

Photo privacy: People who are concerned about others seeing their private images are considerably less inclined to do so. Those individuals may have the most need for a system that can protect their personal images. Our proposed decentralized collaborative training approach prioritizes user privacy and aims to address this issue. Our system is based on the idea that everyone should create their own photo book. Rest assured, while FR instruction, we will strictly adhere to the discerning guidelines.

Volume 15, Issue-1
Jan, 2025, P04
ISSN: 2319-9253

We train facial recognition algorithms with these private images to be more useful in group settings. Players in this game often share private image collections for training purposes, making it a typical example of secure multi-party computing. Large

Social network: A three-realm model is proposed after researching photo sharing statistics on social media. The model states: "a social realm, where identities are entities and friendship constitutes a relation; a visual sensory realm, where faces are entities and co-occurrence in images represents a relation; and a physical realm, where bodies are situated and physical proximity defines a relation." They demonstrate the inseparable link between the two domains. With data from one region, we can develop reasonable assumptions regarding the connection between the other. Stone et al. were the first to propose this concept for FR. It makes use of co-photo associations and social environment information. Joint labeling can be optimized by enhancing the conditional density using their pairwise conditional random field (CRF) model.

Friend list: A user needs to build classifiers for themselves, friend, and friend of friend in our one-versus-one approach. The two iterations of the method are known as these. Alice keeps her friend list under wraps for the first round due to the non-linear nature of the buddy network. Round two requires Alice and her colleagues to collaborate on classifiers. Our policy states that her friends should only communicate with her directly and should not explain their internet activities to her. It is possible to display the contact list while reusing the classifier. Although Alice may be interested in knowing the distance between Bob and Tom, Bob has already done it. The discussion will begin with Alice inquiring of user k whether they had previously understood ukj. Transcribing this query into plaintext would make Bob and Alice's friendship obvious. Alice will begin her task by compiling a comprehensive inventory of all the classifiers that will be utilized in her role. Ask her friends' classifier lists in a deliberate manner using the private set protocols defined in [10]. There will be another purpose for the algorithms utilized by the intersection segment. Bob can still determine the commonalities between Bob and Alice when using recycling classifiers, which is an issue. Users' mutual friends will always be visible on online social networks such as Facebook, even when a "hide mutual friends" function does not exist. online social networks may not be able to afford the processing and transmission expenses of secure techniques, despite their apparent usefulness in protecting private photographs.

Collaborative Learning: Our proposed decentralized collaborative training approach prioritizes user privacy and aims to address this issue. Our approach relies heavily on the idea that everyone should create their own photo album. With these personal images, we can train facial recognition systems to adapt to people's unique social contexts. That manner, when training for face recognition, we can be sure that only the rules that are actually useful are revealed. To increase the recognition rate, we advocate for a network of independent FR algorithms to cooperate. To determine the most effective face recognition algorithms for easier face identification, they consider the person's social context.

4. BACKGROUND WORK

Existing System

An arrangement for photo sharing that visibly hides the photos, protecting users' privacy. The proposed framework for image processing takes into account both the picture's background and what it depicts. People who know and trust each other cannot now communicate images using this technique.

Drawbacks Of Existing System:

Online social network users tend to be wary of individuals who publish photos.

Users lack complete control over their privacy when sharing photographs, which puts security at risk.

Proposed System

Here, the algorithm considers a scenario in which a user (the "publisher") chooses processing actions to take in order to safeguard the privacy of other users while uploading pictures online. To assist publishers in making the most informed decision possible, we propose a trust-based strategy. The publisher is cognizant of the fact that sending the image to each relevant user depending on their trustworthiness could lead to an invasion of privacy.

Advantages:

- Security is enhanced by using trust-centric methods for image anonymization, which preserve privacy.

International Journal of
ADVANCED RESEARCH & INNOVATIONS
Volume 15, Issue-1
Jan, 2025, P04
ISSN: 2319-9253

- Protecting user data from unauthorized access is the primary goal of trust-based picture sharing.

System Architecture

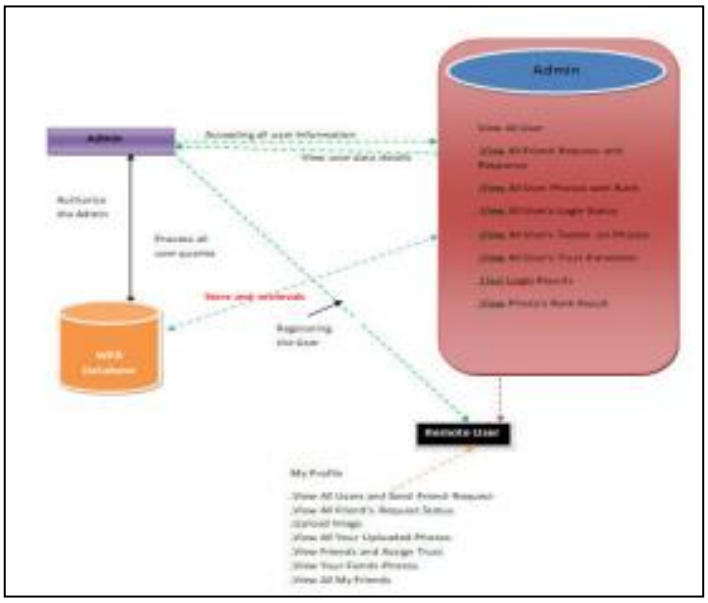

Fig 1 Architecture Diagram

Modules

Admin Module

Assess each photo in accordance with the regulations using a photograph from the Administrator Module Supplement. Be sure you're familiar with the location of each image and examine the user's search history thoroughly.

User Module

The user module allows users to publish photographs and check trust values. The reliability of an image determines how it is shared, retrieved, and seen.

5. Results and Discussions

Fig 2: Home Page of Project

International Journal of
ADVANCED RESEARCH & INNOVATIONS
Volume 15, Issue-1
Jan, 2025, P04
ISSN: 2319-9253

Fig 3: Admin Login Page

Fig 4: Admin Menu Page

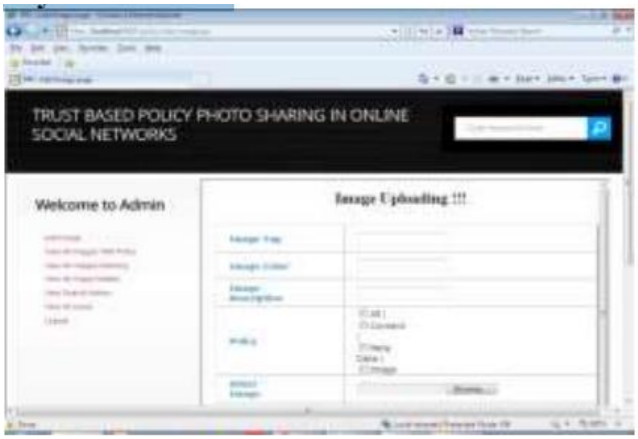

Fig 5: Admin Add Images with Policies Page

International Journal of
ADVANCED RESEARCH & INNOVATIONS

Volume 15, Issue-1
Jan, 2025, P04
ISSN: 2319-9253

Fig 6: List of Images with Policies

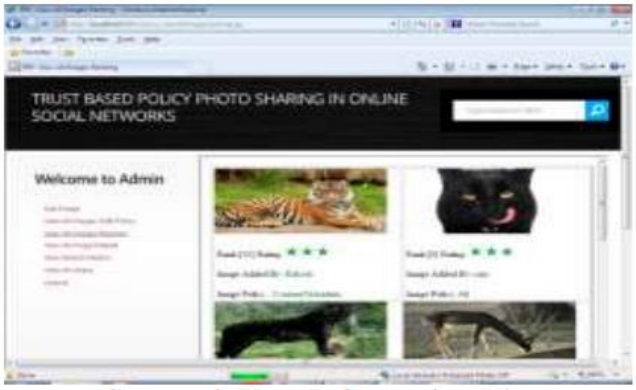

Fig 7: User Information View

Fig 8: List of Images with Rank

International Journal of
ADVANCED RESEARCH & INNOVATIONS
Volume 15, Issue-1
Jan, 2025, P04
ISSN: 2319-9253

Fig 9: List of Images with User Content

Fig 10: Report Showing List of Users

Fig 11: Report Showing List of Users with Authorization

International Journal of
ADVANCED RESEARCH & INNOVATIONS
Volume 15, Issue-1
Jan, 2025, P04
ISSN: 2319-9253

Fig 12: User Login Page

Fig 13: User Menu Page

Fig 14: List of Users with Trust Acceptance

International Journal of
ADVANCED RESEARCH & INNOVATIONS

Volume 15, Issue-1
Jan, 2025, P04
ISSN: 2319-9253

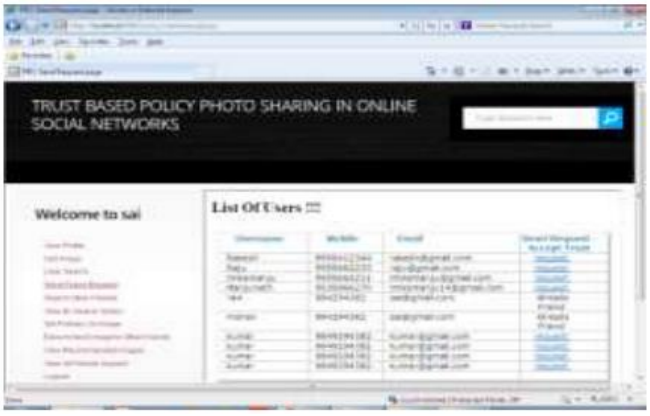

Fig 15: Report showing List of Trust Acceptance

Fig 16: Menu to Search Trusted user Data

Fig 17: User Searching Friends Information

International Journal of
ADVANCED RESEARCH & INNOVATIONS
Volume 15, Issue-1
Jan, 2025, P04
ISSN: 2319-9253

Fig 18: User Searching Based on Trusted Friend

6. Conclusion

Social media photo-sharing system that prioritizes privacy is crucial for safeguarding user data during an era in which visual content is the most prevalent form of online communication. With the daily sharing of billions of photographs across multiple platforms, there is a greater likelihood of identity theft, privacy breaches, unlawful monitoring, and the use of personal data. Because private settings are consumers maintain ownership and control over their digital photographs.

Secure watermarking, homomorphic encryption, and attribute-based encryption (ABE) are common methods used by these frameworks to limit photo access to authorized users while maintaining system performance and usability. More sophisticated solutions create immutable shared records using either not available or are insufficient, users of traditional social media platforms are vulnerable to exploitation by companies and attacks by unauthorized individuals. A potential remedy to these concerns is now being investigated, and it involves privacy-protecting technology. Encryption, situation-aware sharing tactics, and access control are some of the ways these solutions enable decentralized architectures or blockchain technology. In this way, we can be sure that everyone is holding themselves to their word and that no secrets are being kept. These strategies are effective in both domains because global data privacy rules such as the CCPA and GDPR are requiring an increasing number of social media platforms to adhere to them.

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

Volume 15, Issue-1
Jan, 2025, P04
ISSN: 2319-9253

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.
14. Rahman, A., & Hasan, M. (2024). Privacy-preserving and user-centric photo sharing framework for social media networks. Knowledge-Based Systems, 297, 110301.
15. Srinivasan, K., & Thomas, M. (2024). A secure and privacy-preserving photo sharing protocol for social media using attribute-based encryption and blockchain. ACM Transactions on Information and System Security, 19(3), Article 17.