My Privacy My Decision: Control of Photo Sharing on Online Social Media

Ms. S. Sri Ranjani[1], M. Sankar[2], S. Siva Suriyan[3], P. Balaji[4]
[1]*Asst. prof Department of Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, India*
[2,3,4]*Students, Department of Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, India*

***Abstract*—Managing photo privacy and secure sharing on online social media platforms has become increasingly critical as users frequently upload and distribute personal images. Traditional social media applications prioritize rapid content sharing, often neglecting sufficient privacy controls and user consent, leading to unauthorized access and misuse of personal photos. This paper presents "My Privacy My Decision," a secure, privacy-focused photo sharing platform that enables users to maintain complete control over ownership, access, and distribution of their images. The system incorporates multiple protection mechanisms including automatic watermarking, encrypted storage, permission-based access control, view-only modes, and anti-hotlinking protection. Furthermore, facial recognition and consent-based sharing mechanisms allow individuals appearing in photos to participate in sharing decisions before content is published. The platform employs React for the frontend and Python-Django for the backend, with role-based authentication ensuring only authorized users can access protected content. Experimental evaluation through unit, integration, and validation testing confirms the system's effectiveness in preventing unauthorized access and empowering users with comprehensive privacy controls.**

***Index Terms*—photo privacy; access control; social media security; consent-based sharing; watermarking; facial recognition; user privacy**

I. INTRODUCTION

In the digital era, online social media platforms have become a primary medium for sharing personal photos and visual content. While photo sharing enhances communication and social interaction, it introduces serious privacy concerns including unauthorized distribution, misuse of personal images, and lack of user control over shared content [1]. The growing number of privacy breaches on platforms such as Facebook, Instagram, and Twitter highlights the urgent need for privacy-preserving mechanisms in photo sharing systems.

Existing social media platforms are primarily designed to promote fast and easy sharing of photos without providing sufficient privacy controls. Once shared, images can be easily downloaded, copied, or redistributed without the owner's knowledge [2]. The absence of consent-based sharing for individuals appearing in photos further exacerbates the risk of misuse and unauthorized distribution.

This paper presents "My Privacy My Decision: Control of Photo Sharing on Online Social Media," a privacy-focused platform designed to address these limitations. The proposed system allows users to securely upload, manage, and share photos while maintaining full ownership and access control. Key contributions of this work include:

- A multi-layered privacy architecture combining encryption, watermarking, and permission-based access control.
- A consent-driven sharing mechanism enabling individuals in photos to participate in publication decisions.
- Role-based authentication and secure storage ensuring only authorized users access protected content.
- Anti-hotlinking and download prevention measures to protect image ownership.

The remainder of this paper is organized as follows: Section II reviews related work. Section III presents the system design and architecture. Section IV describes the implementation. Section V discusses

testing and evaluation. Section VI concludes with future directions.

II. RELATED WORK

Privacy control in social media has been extensively studied in the literature. Squicciarini et al. [3] proposed a collaborative privacy management system enabling users to negotiate access policies for co-owned content. Their work highlighted the challenge of reconciling conflicting privacy preferences among multiple stakeholders, a problem directly addressed by our consent-based mechanism.

Fang and LeFevre [4] introduced a privacy wizard for social networking sites that automatically suggests privacy settings based on user behavior patterns. While effective, their approach did not incorporate image-level protection mechanisms such as watermarking or encrypted storage.

Klare et al. [5] demonstrated the effectiveness of facial recognition in identifying individuals in shared photos, motivating the integration of such technology in privacy-aware systems. Our system leverages this capability to detect individuals in uploaded photos and trigger consent workflows accordingly.

Research by Besmer and Lipford [6] on photo tagging on Facebook revealed that users often feel violated when tagged in photos without consent, underscoring the importance of consent-based mechanisms. Unlike previous work, the proposed system integrates consent management, access control, and image protection into a unified platform.

III. SYSTEM DESIGN AND ARCHITECTURE

A. System Architecture

The proposed system follows a three-tier web architecture separating presentation, business logic, and data management concerns. This architectural separation enhances scalability, maintainability, and security.

- Client Tier: A React-based web interface allowing users to upload photos, configure privacy settings, and manage permissions.
- Business Logic Tier: A Python-Django backend processing authentication, photo encryption, privacy rule enforcement, and API communication.
- Database Tier: An SQLite/PostgreSQL database storing user profiles, image metadata, privacy configurations, and access control lists (ACLs).

B. Database Design

The database schema is designed to support flexible privacy configurations. Two core tables govern photo access:

Table I. Photos Table Schema

Field	Data type	Description
photo_id	Int (pk)	Unique image identifier
user_id	Int (fk)	Owner reference
photo_path	Varchar (255)	Stored image path
privacy_type	Varchar (50)	Public / Private / Custom
upload_time	Timestamp	Upload timestamp

Table II. Privacy Decisions Table Schema

Field	Data type	Description
decision_id	Int (pk)	Unique rule identifier
photo_id	Int (fk)	Associated photo
allowed_entity	Varchar (100)	Role or group permitted
access_level	Int (1)	1=View, 2=Download, 3=None

C. Privacy Control Modules

The system is composed of three primary functional modules:

- Admin Module: Provides system-wide monitoring and management capabilities including user account administration, content moderation, privacy policy enforcement, and generation of activity reports.
- User Module: Enables registered users to upload photos with configurable privacy levels (private, friends-only, public, custom group), manage access control lists, and receive notifications about photo interactions.
- Viewer Module: Grants authorized viewers access to permitted content, supports access request workflows, and enforces download/sharing restrictions.

IV. IMPLEMENTATION

A. Technology Stack

The system is implemented using a modern web technology stack selected for security, scalability, and developer productivity:

Table III. Technology Stack

Component	Technology	Purpose
Frontend	React JS	Dynamic UI components
Backend	Python / Django	Server-side logic & APIs
Database	SQLite / PostgreSQL	Data persistence
Authentication	Django Auth	Secure session management
Image Protection	Pillow Library	Watermarking & processing

B. Privacy Protection Mechanisms

The system implements multiple layers of image protection:

- Watermarking: Uploaded images are automatically watermarked using the Pillow library before storage. The watermark embeds owner identity information, deterring unauthorized redistribution.
- Encrypted Storage: Images are stored using AES encryption, ensuring that even direct file system access cannot retrieve usable image data without proper authentication credentials.
- View-Only Mode and Anti-Hotlinking: The frontend disables right-click context menus and drag-and-drop functionality for protected images. Server-side referrer validation prevents external hotlinking of image URLs.
- Download Prevention: HTTP response headers are configured to prevent browser-level download prompts for view-only images, supplemented by client-side event handler restrictions.

C. Consent-Based Sharing Workflow

When a user uploads a photo and facial recognition detects additional individuals, the system automatically identifies registered users matching detected faces and sends consent notifications. The photo remains in a pending state until all identified individuals approve or reject publication. This workflow is implemented via the consent table in the database and managed by the privacy_controller module.

The filter_visible_photos() function in the privacy controller evaluates each photo against the requesting user's relationship, privacy level, and consent status before serving content, ensuring real-time enforcement of privacy decisions.

V. TESTING AND EVALUATION

A. Testing Methodology

The system was evaluated through three levels of testing: unit testing, integration testing, and validation testing, following IEEE software testing standards [7].

B. Unit Testing

Individual modules were tested in isolation. Key test cases included user registration and authentication, photo upload and storage, privacy setting configuration, admin monitoring functionality, and viewer access permission enforcement. All 24unit test cases passed, confirming correct individual module behavior.

C. Integration Testing

Integration testing verified seamless interaction between modules. Critical scenarios tested include: users setting privacy permissions and verifying immediate enforcement for viewers, admin monitoring and removing content, privacy setting updates being reflected in real time, and viewer access request approval workflows. Integration testing confirmed correct data flow across all module boundaries.

D. Validation Testing

Input validation was rigorously tested to ensure system security and data integrity. The following validation rules were verified:

Table IV. Validation Test Cases

Validation Type	Rule	Result
User Credentials	Min 8 chars, alphanumeric	Pass
Email Format	RFC 5322 compliant	Pass
Image Upload	JPG/PNG/JPEG, max 10MB	Pass

Validation Type	Rule	Result
Privacy Settings	Must select valid level	Pass
Unauthorized Access	Auto-blocked by ACL	Pass

All 18 validation test cases passed, confirming the robustness of the system against malformed inputs and unauthorized access attempts.

VI. CONCLUSION

This paper presented "My Privacy My Decision," a secure and privacy-centric photo sharing platform addressing critical limitations of existing social media systems. The proposed system provides users with granular control over photo access through a combination of encryption, watermarking, permission-based access control, and consent-based sharing mechanisms.

The three-tier architecture, implemented using React and Python-Django, ensures a scalable and maintainable solution. Testing results confirm that the system effectively prevents unauthorized access, enforces privacy decisions in real time, and maintains data integrity across all input scenarios.

Future work will focus on: (1) enhancing facial recognition accuracy using deep learning models, (2) implementing blockchain-based audit trails for photo access events, (3) developing mobile applications for iOS and Android, and (4) integrating differential privacy techniques to protect user analytics data.

REFERENCES

[1] d. m. 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] M. Madejski, M. Johnson, and S. M. Bellovin, “A study of privacy settings errors in an online social network,” in Proc. IEEE PERCOM Workshops, pp. 340–345, 2012.

[3] A. C. Squicciarini, M. Shehab, and F. Paci, “Collective privacy management in social networks,” in Proc. 18th International Conference on World Wide Web, pp. 521–530, 2009.

[4] L. Fang and K. LeFevre, “Privacy wizards for social networking sites,” in Proc. 19th International Conference on World Wide Web, pp. 351–360, 2010.

[5] B. F. Klare, et al., “Pushing the frontiers of unconstrained face detection and recognition: IARPA Janus Benchmark A,” in Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1931–1939, 2015.

[6] A. Besmer and H. R. Lipford, “Moving beyond untagging: Photo privacy in a tagged world,” in Proc. 28th International Conference on Human Factors in Computing Systems, pp. 1563–1572, 2010.

[7] IEEE Standard for Software and System Test Documentation, IEEE Std 829-2008, 2008.

[8] L. Welling and L. Thomson, PHP and MySQL Web Development, 4th ed. Addison-Wesley Professional, 2008.

[9] A. Silberschatz, H. Korth, and S. Sudarshan, Database System Concepts, 7th ed. McGraw-Hill Education, 2019.

[10] OWASP Foundation, “OWASP Top Ten Security Risks,” 2021. OWASP Top Ten