20MCA245 MINI PROJECT

SYNOPSIS

The Secure Photo Vault: Advanced Encryption and Authentication for Enhanced Data Privacy

Abstract

The ”The Secure Photo Vault” project aims to develop a secure web application for managing photos ensuring their confidentiality and integrity through advanced encryption techniques. Photos are stored in an encrypted format and can only be accessed after decryption. The project features local encryption and decryption using cryptographic algorithms. To further enhance user authentication and security, this project integrates Two-Factor Authentication (2FA) using Time-based One-Time Password (TOTP) algorithm to provide a second form of verification. The application offers a user-friendly interface and reliable performance. All communication between the client and server is secured with End-to-End Encryption (E2EE) ensuring that data transmitted over the network is protected from unauthorized access. It employs a secure password-based key derivation function for encryption key management. The gallery includes face recognition technology to automatically organize photos based on the people in them. The gallery also includes a search and filter system that allows users to find photos by name, date, or tags enhancing the ease of photo management. This improves the user experience by making photo retrieval more efficient. Additionally, the project integrates cloud storage for managing photos remotely, offering a flexible and secure way to handle sensitive data both locally and online.

Scope and Relevance

The project aims to ensure the confidentiality of user images through local encryption and decryption using advanced cryptographic algorithms, supplemented by Two-Factor Authentication (2FA) and End-to-End Encryption (E2EE). It includes essential features such as user authentication, image management (adding, deleting, updating), a comprehensive search and filter system and face recognition technology for automatic sorting. This project is highly relevant as it addresses critical privacy concerns by safeguarding sensitive data against unauthorized access while offering a practical and user-friendly tool for managing photos.

Requirement Analysis

The ”The Secure Photo Vault” project necessitates a secure user authentication system, including account creation, login, and Two-Factor Authentication via OTPs. It must support comprehensive image management with each photo encrypted before storing and decrypted before accessing using advanced cryptographic algorithms for local encryption and decryption. A search and filter system for efficient photo retrieval by name, date, or tags.All communication between the client and server is secured with End-to-End Encryption (E2EE). The integration of face recognition technology for automatic sorting based on humanface.

Development Methodology

The ”The Secure Photo Vault” project will use Agile methodology with Scrum for iterative development. The front-end will be created with HTML, CSS, and JavaScript for a responsive interface, while the back-end will use Python and Django for secure image management and user authentication. A relational database like PostgreSQL or MySQL. Regular feedback and iterative improvements will refine functionality and enhance user experience. Two-Factor Authentication (2FA) will be implemented using the TOTP algorithm and End-to-End Encryption (E2EE) will be employed to secure communication between client and server.

Keywords: Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), Two-Factor Authentication (2FA), Time-based One-Time Password (TOTP), End-to-End Encryption (E2EE)

Name and Signature of Student with date