Encryptora

A Middleman Website for End-to-End Encryption of Your Cloud Files

PROPOSAL

Submitted in partial fulfilment of the requirement for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

SUBMITTED BY

Ashutosh Jha (21103029)

Under the supervision of

Dr. K.P. Sharma

Assistant Professor

Department of Computer Science and Engineering

Dr. B. R. Ambedkar National Institute of Technology Jalandhar

-144008, Punjab (India)

September 2024

Dr. B. R. Ambedkar National Institute of Technology Jalandhar

ABSTRACT

In an era of increasing data breaches and concerns over cloud security, **Encryptora** will offers a solution that empowers users to maintain full control over their sensitive data. This middleman platform enables seamless, client-side encryption of files before they are uploaded to any cloud provider. By encrypting the data locally, users ensure that even cloud service providers have no access to the contents of their files, offering a robust layer of security and privacy.

With a simple and user-friendly interface, Encryptora integrates with major cloud platforms, providing a seamless encryption process. Users can upload their files to the cloud with peace of mind, knowing their data remains private and secure. The platform aims to revolutionize how individuals and businesses approach cloud security, offering an intuitive, scalable, and secure solution for file encryption.

Plan of Action

1. Problem Identification

- Cloud storage is widely used, but users often have concerns over privacy and security. Cloud providers can access unencrypted data, posing potential risks for sensitive files.
- Existing encryption tools can be complicated for non-technical users to implement, often interrupting workflow and reducing efficiency.

2. Solution Overview

- **Encryptora** acts as a middleman between the user and their chosen cloud storage provider, enabling users to encrypt files locally before they are uploaded.
- The encryption process is seamless, requiring minimal effort from users, but offering maximum security by ensuring the cloud provider cannot access the encrypted data.

3. Key Features

- **Client-Side Encryption**: Files are encrypted locally on the user's device before uploading to the cloud. Only the user holds the decryption keys.
- **Cloud Provider Integration**: Integrates with popular cloud services (Google Drive, Dropbox, OneDrive, etc.) for easy file management.
- **Cross-Platform**: The website will be accessible from various devices, including desktops, tablets, and mobile devices.
- **User-Friendly Interface**: Designed for both technical and non-technical users with intuitive navigation.
- **Security and Privacy**: Utilizes AES-256 encryption for file security, ensuring no data is accessible to cloud providers or third parties.

4. Technical Architecture

- **Frontend**: Developed using **React.js** or **Vue.js** for a dynamic and responsive user interface.
- **Backend**: Secure backend using **Node.js** to manage user authentication, encryption, and cloud storage API integrations.
- **Encryption**: Files are encrypted using **AES-256** algorithm with local key generation. The encryption key is never sent to the cloud.
- **Cloud Integration**: Secure integration with cloud providers using their respective APIs (e.g., Google Drive API, Dropbox API) to handle file uploads.

5. Project Timeline

- **Week 1-2**:
    - Finalize user requirements and cloud provider integrations.
    - Create wireframes and UI mockups for the platform.
- **Week 3-4**:
    - Build the frontend interface with encryption options.

    - Develop the backend for user authentication and cloud API integration.
- **Week 5-6**:
    - Implement file encryption and decryption functionality.
    - Integrate cloud storage options and perform initial testing.
- **Week 7-8**:
    - Testing and bug fixes for seamless encryption and file uploads.
    - Conduct a security audit to ensure robust encryption mechanisms.
- **Week 9-10**:
    - Finalize deployment strategy and prepare for the formal launch.

6. Target Audience

- **Individuals**: Those looking for personal cloud security without trusting cloud providers with their unencrypted data.
- **Small Businesses**: Firms needing to store sensitive data securely without heavy IT infrastructure.
- **Enterprises**: Large-scale organizations that require scalable encryption solutions for compliance and security.

7. Business Model

- **Freemium Model**:
    - Basic free tier offering limited storage and encryption features.
    - Premium tier for businesses and power users with unlimited file size, advanced encryption, and priority cloud integrations.

8. Conclusion

Encryptora is designed to be a game-changer in data security, offering users complete control over their privacy while using cloud services. By ensuring that only the user has access to their encryption keys, the platform guarantees that sensitive information remains confidential, no matter the cloud provider.