Project Proposal: Secure File Sharing Platform

1. Project Title:

Secure File Sharing Platform

2. Team Members:

- Mohsin Wazir. 2022309
- Ibrahim Imran 2022301
- Zain memon. 2022630
- Sagar Kumar. 2022522

3. Project Overview:

The Secure File Sharing Platform is a web-based application designed to facilitate secure and efficient file sharing between users. The primary goal of this project is to address security challenges associated with file sharing, such as unauthorized access, data breaches, and interception during transmission. The platform will integrate advanced security measures like end-to-end encryption, multi-factor authentication, and role-based access control to ensure the confidentiality, integrity, and availability of shared files.

4. Objectives:

- To develop a user-friendly platform for secure file sharing.
- To ensure the confidentiality of files through encryption.
- To protect user accounts and file access with strong authentication methods.
- To prevent unauthorized access with fine-grained access control.

5. Key Features:

1. User Authentication:

- OAuth 2.0: Secure login via Google, Microsoft, or email-based authentication.

- Multi-Factor Authentication (MFA): OTP verification for enhanced security.

2. End-to-End Encryption:

- AES-256 Encryption: For files at rest to prevent unauthorized access.
- TLS Protocol: For secure transmission of files between users.

3. Access Control:

- Role-Based Access Control (RBAC):
- Define permissions for admins, uploaders, and viewers.
- Time-limited access links for external users.

4. File Integrity and Anti-Tampering:

- Digital Signatures: Verify file authenticity and integrity during downloads.
- Checksum Verification: Detect file corruption or tampering.

5. Activity Monitoring:

- Detailed logs for upload, download, and access activities.
- Alerts for suspicious activities like multiple failed login attempts.

6. Secure File Deletion:

- Implement secure wipe algorithms to ensure files are permanently deleted.

6. Security Measures:

- Authentication:
- OAuth 2.0 and MFA for strong user verification.
- Session management with tokens and expiry time.
- Encryption:
- AES-256 for file storage and SSL/TLS for data transmission.
- Encrypted metadata to prevent information leakage.
- Access Control:
- RBAC with custom policies for upload, download, and view access.
- Time-based access expiry for shared files.

- Monitoring and Alerts:
- Real-time monitoring with alerts for unusual login locations or failed attempts.
- Backup and recovery options to prevent data loss.

7. Technology Stack:

- Frontend: HTML5, CSS3, JavaScript (React or Angular).
- Backend: Node.js or Django for handling APIs.
- Database: MySQL or MongoDB with encryption for stored data.
- Security Libraries: OpenSSL for encryption, JWT for authentication tokens.

8. Expected Challenges:

- Balancing encryption security with file upload/download speed.
- Managing key distribution and storage securely.
- Ensuring compliance with data protection regulations (e.g., GDPR).

9. Conclusion:

The Secure File Sharing Platform aims to provide a robust solution for secure file sharing, addressing common vulnerabilities like unauthorized access, data breaches, and tampering. By integrating encryption, strong authentication, and access control, the platform will ensure that files remain confidential and secure during storage and transmission.