Privacy-Focused Encrypted Notes App – Project Report

Introduction

The Privacy Notes App is a secure, offline-first note-taking application designed to protect user data through client-side encryption. All note content is encrypted using AES before storage, ensuring privacy and security even if storage is accessed without authorization.

Abstract

This project focuses on building a note-taking system where security is the priority. The app uses React for UI, CryptoJS for encryption, and Indexed DB for persistent browser-based storage. No plaintext data is ever saved, making it a true zero-knowledge design. The system allows users to create, edit, delete, and manage encrypted notes with features like search, pin, archive, and backup export.

Tools Used

1. React – For building a fast, component-based UI.

2. CryptoJS – Used to implement AES encryption for secure note storage.

3. Indexed DB – Provides persistent, offline storage for encrypted notes.

4. Vite – For efficient development and bundling.

5. UUID – For generating unique note identifiers.

Steps Involved in Building the Project

1. Setup Environment:

- Initialized a React project with Vite.

- Installed dependencies: CryptoJS, uuid

2. Implemented Client-Side Encryption:

- Built encryption module using AES.

- Implemented secure key derivation using SHA-256.

3. Designed Indexed DB Storage Layer:

- Created wrapper functions for CRUD operations.

- Stored only encrypted content in database.

4. Developed Core Application Logic:

- Unlock/lock mechanics using user passphrase.

- CRUD operations integrated with encryption and Indexed DB.

- Added features: search, edit, delete, pin, archive.

5. Built User Interface:

- Responsive UI using React components.

- Structured editor, notes list, and settings panel.

6. Implemented Backup System:

- Export encrypted notes to JSON.

- Restore functionality planned for future versions.

Conclusion

This project demonstrates a complete privacy-first note-taking application suitable for users who require secure and offline access to sensitive data. By integrating client-side AES encryption and Indexed DB, the system ensures that data remains confidential at all times. The modular and scalable architecture allows for future upgrades such as PBKDF2 key derivation, biometric unlock, cloud sync with zero-knowledge encryption, and UI enhancements. This app can be expanded further to become a production-grade secure notes platform.