A Secure and User-Friendly Encrypted File Sharing System

In today’s digital world, file sharing is common but prone to data breaches. This project provides a secure and simple encrypted file sharing solution.

Team Members: ABHIMANYU LOCHAB [24BCY70093] , RAGHAV TIWARI [24BCY70096] , PARAS SHARMA[24BCY70123],DILPREET SINGH[24BCY70106] , VANSH GOLIA[24BCY70087]

Guide: DR. SYED IRFAN YAQOOB

System Architecture Overview

User Interface

Intuitive design for seamless file upload and download operations.

Encryption/Decryption

Utilising robust AES-256 for military-grade data protection.

Secure Link Generation

Links are protected with passwords and time-based expiry for enhanced security.

File Retrieval

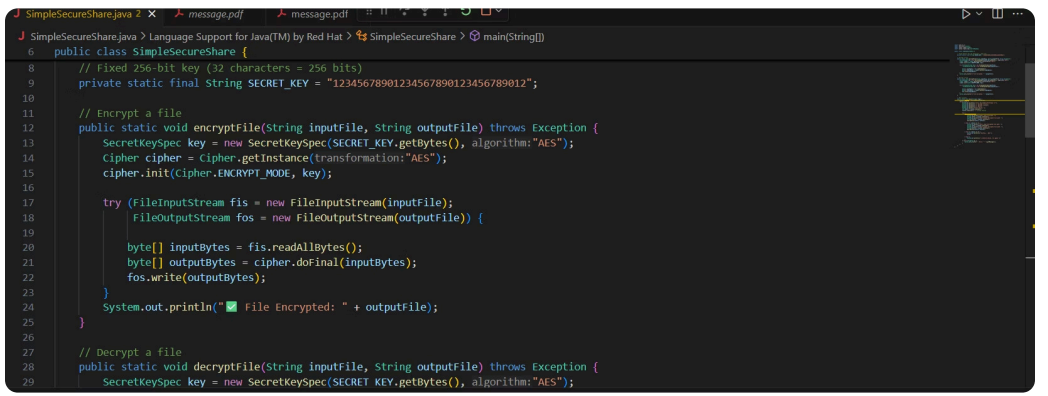
Efficient and secure access to encrypted files by authorised receivers.

Experimental Setup and Workflow

Setup Design

Our experimental setup leverages readily available resources to ensure replicability and accessibility.

- **Hardware:** Standard laptop/PC configuration.
- **Software:** Java JDK, VS Code, and standard AES cryptography libraries.



Workflow Illustration

The system's core functionality is demonstrated through a simple, yet effective, file sharing process.

1. User A uploads a document.
2. The system encrypts the document.
3. A secure, time-limited link is generated.
4. User B downloads and decrypts the document via the link.

Demo: We will provide a live demonstration, showcasing the upload, encryption, download, and decryption process, highlighting the seamless user experience.

Research Methodology and Data Collection

01

Literature Survey

Extensive review of cryptographic standards (AES vs DES) and existing secure file sharing platforms to inform design choices.

02

AES-256 Adoption

Selected AES-256 for its superior security posture and widespread industry endorsement.

03

Java Implementation

Developed the system in Java, focusing on a straightforward user interface for ease of use.

04

Comprehensive Testing

Rigorous testing with diverse file types and sizes to assess system performance and robustness.

Data Collection Plan

- **Performance Metrics:** Recording encryption and decryption times for various file sizes.
- **Efficiency Analysis:** Comparing original and encrypted file sizes to evaluate overhead.
- **Usability Feedback:** Gathering qualitative data on ease of use from team members to refine the user experience.

Feasibility Analysis

Technical Feasibility

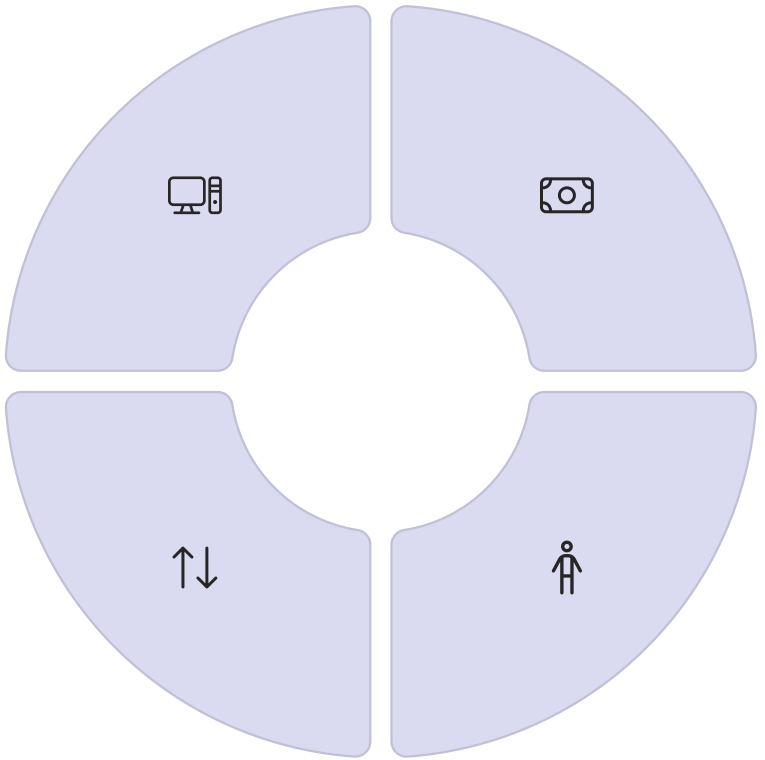
The system operates efficiently on standard computing hardware and utilises established software frameworks.

- Compatible with standard laptops and PCs.
- Relies on proven open-source tools and libraries.

Scalability Potential

The architecture supports future expansion with new features and integrations, enhancing its utility and reach.

- Supports multi-user environments.
- Adaptable for blockchain logging and mobile applications.



Economic Viability

Designed with a focus on cost-effectiveness, eliminating the need for proprietary software or additional hardware investments.

- Zero additional financial outlay for implementation.
- Leverages open-source resources for development.

Operational Ease

Engineered for simplicity, ensuring accessibility for users across all technical proficiencies.

- User-friendly interface for non-technical users.
- Streamlined workflow for sharing and retrieving files.

Innovations and Future Enhancements

Current Innovations

- **AES-256 Encryption:** Ensuring data confidentiality and integrity.
- **Time-Limited Links:** Enhancing security by restricting access duration.
- **Password Protection:** Adding an extra layer of authentication for shared files.

Future Work

- **Role-Based Access Control (RBAC):** Granular permissions for diverse user roles.
- **Blockchain Integration:** Tamper-proof logging for all file transactions.
- **Generate link:** Create a link to share the files more efficiently
- **Mobile Application:** Extending secure file sharing to mobile platforms.

Conclusion and Vision

> **"This project is not just a prototype, but a step towards building secure, practical, and user-friendly file sharing systems."**

We have developed a robust, accessible, and highly secure encrypted file sharing system, demonstrating a significant leap in data protection for everyday digital interactions. Our foundational work provides a strong platform for future innovations, ensuring adaptability and enhanced functionality in an evolving digital landscape.