

Secured File Share: A MERN Stack Solution for Secure Data Exchange

by Shrey Goel

Department of Computer Science, Bennett University

Abstract

Secure sharing of sensitive information is a critical challenge in modern digital interaction. Conventional platforms often expose users to data interception and cyber threats. This project introduces **Secured File Share**, a web application built on the MERN stack (MongoDB, Express, React, Node) that ensures data integrity and privacy through end-to-end encryption.

Introduction & Problem Statement

- **Context:** Security often lags behind convenience in file sharing.
- **The Problem:** Traditional sites are vulnerable to:
 - Man-in-the-middle attacks.
 - Weak authentication.
 - XSS and Injection threats.
- **Objective:** Create a platform where files remain private from upload to download.

Target Audience

- **Individuals:** Protecting personal documents.
- **Small Teams:** Sharing proprietary strategies.
- **Professionals:** Legal/Healthcare data compliance.

System Architecture

Full-stack JavaScript solution using the MERN architecture.

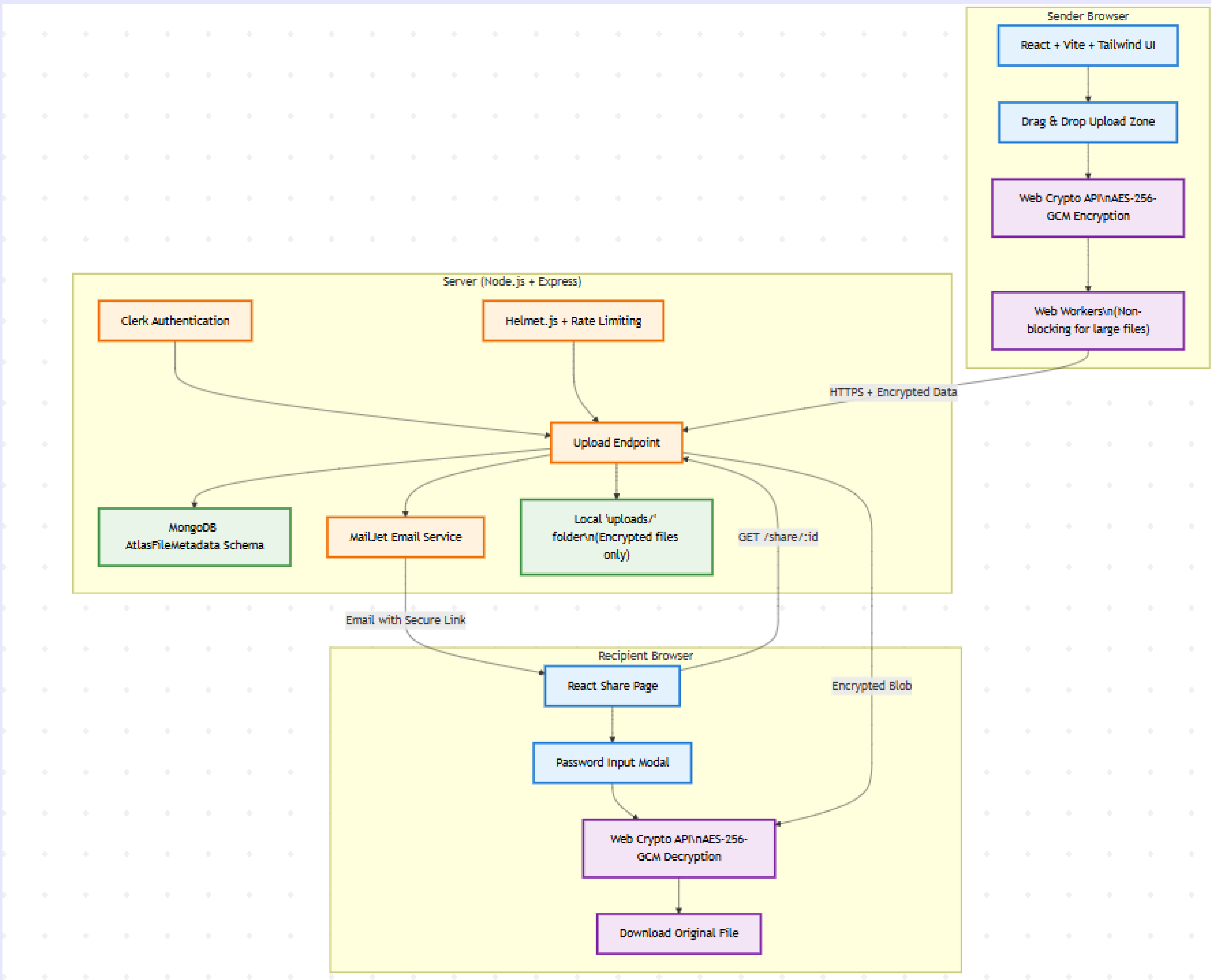


Figure: Overall System Architecture

- **Frontend:** React.js for UI.
- **Backend:** Node/Express encryption logic.
- **Database:** MongoDB for metadata.

Key Features

- 1 **End-to-End Encryption:** Server-side AES-256 encryption.
- 2 **Secure Authentication:** Hashed passwords using bcrypt.
- 3 **Link Protection:** Expiration times and download limits.

Results & Interface

The interface focuses on usability and visible security status.

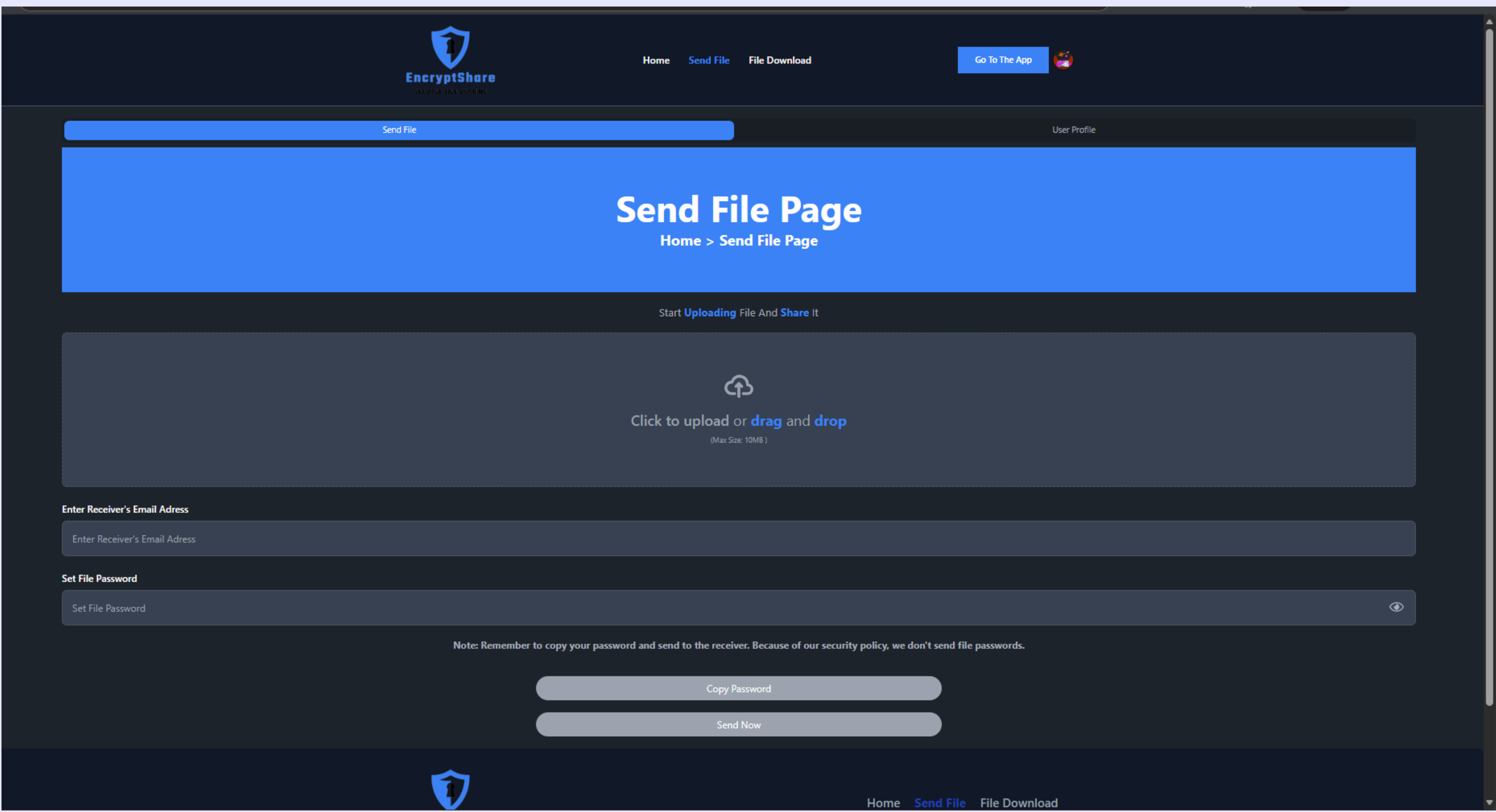


Figure: Secure File Upload

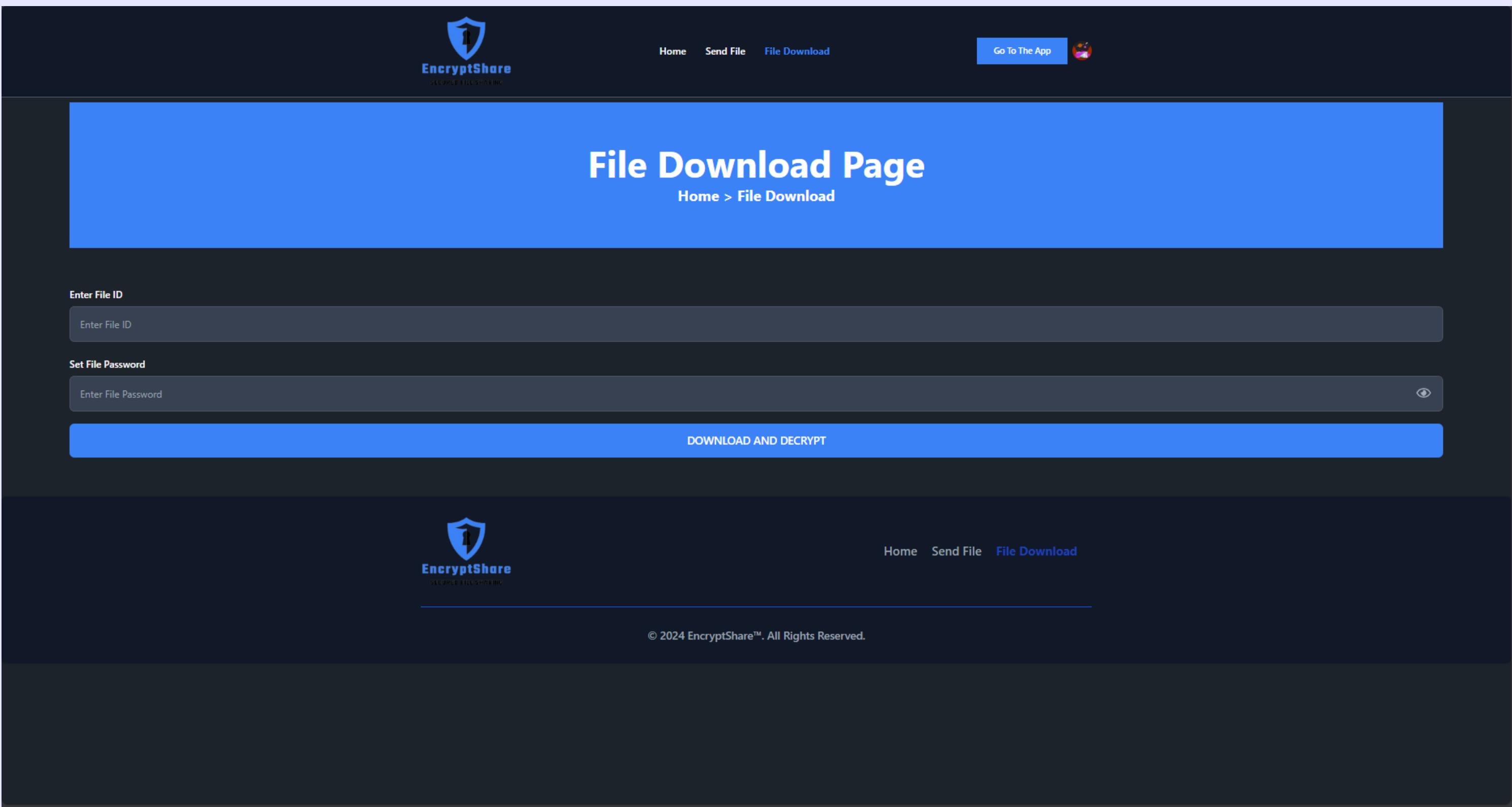


Figure: Password Protected Download

Conclusion

Secured File Share successfully mitigates web vulnerabilities in file transfers. By leveraging the MERN stack and AES encryption, it provides a trusted environment for sensitive data exchange.

Future Work

- Multi-Factor Authentication (MFA).
- Cloud Storage Integration (AWS S3).
- Real-time Malware Scanning.