

Guardianbox End-To-End Encrypted File Sharing

Ms.I. Ramya¹, Ms.K. Preethi²

¹*Assistant Professor, Department of Master of Computer Applications,
Er.Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India.*

²*II MCA, Department of Master of Computer Applications,
Er.Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India.*

Abstract— File sharing has become an essential part of modern digital communication, allowing individuals and organizations to exchange documents, images, videos, and other data quickly through the internet. However, traditional file sharing systems often expose sensitive information to security risks such as data interception, unauthorized access, and privacy breaches. To address these issues, this paper proposes Guardian Box, an end-to-end encrypted file sharing platform designed to ensure secure data transmission and storage. The platform encrypts files before they are transmitted and ensures that only authorized recipients with the correct decryption key can access the shared content. Guardian Box provides secure file upload, encrypted sharing links, access control mechanisms, and user authentication features. The system also includes file management tools and activity monitoring to enhance data security and usability. Developed using modern web technologies, Guardian Box ensures high scalability, reliability, and security. By combining strong encryption with user-friendly file sharing functionality, Guardian Box offers a secure and efficient solution for protecting sensitive data during online file transfers.

Index Terms— End-to-End Encryption, Secure File Sharing, Data Privacy, Cryptography, Cloud Security.

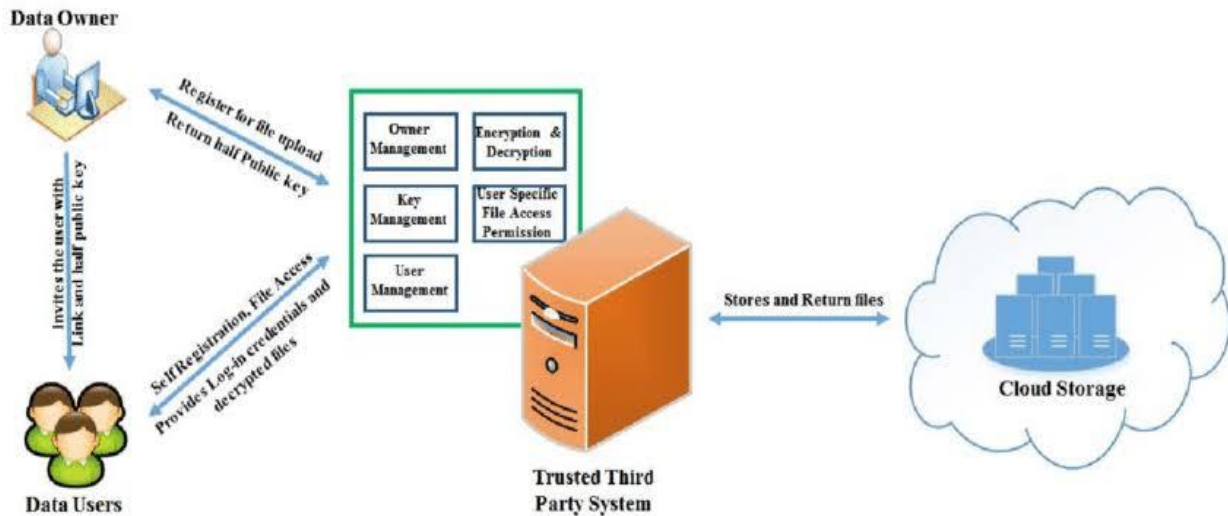
I. INTRODUCTION

With the rapid growth of digital communication and cloud services, file sharing has become a common activity for both individuals and organizations. Users frequently exchange documents, multimedia files, and confidential information through online platforms. However, many traditional file sharing systems do not

provide adequate security mechanisms to protect sensitive data from cyber threats. Unauthorized access, data interception, and privacy breaches are some of the major risks associated with unsecured file sharing. Attackers can intercept files during transmission or gain unauthorized access to stored data if proper security measures are not implemented. To address these concerns, secure file sharing solutions that protect data throughout the entire transfer process are essential. End-to-end encryption (E2EE) is one of the most effective techniques for protecting data privacy. In this approach, files are encrypted before they leave the sender's device and can only be decrypted by the intended recipient. This ensures that even service providers cannot access the shared data. The proposed system GuardianBox is designed to provide a secure file sharing environment using end-to-end encryption. The platform enables users to upload, encrypt, share, and download files securely while ensuring that only authorized users can access the data. The system also provides access control, secure sharing links, and activity monitoring features to enhance overall security.

The main objectives of the GuardianBox system include:

- Protecting files using strong end-to-end encryption
- Ensuring secure file sharing between users
- Preventing unauthorized access to sensitive data
- Providing a user-friendly and secure file management system



1.1 Growth of Online File Sharing

The increasing use of cloud storage services and remote collaboration tools has significantly increased the demand for online file sharing. Businesses, educational institutions, and individuals rely on file sharing platforms to exchange information quickly and efficiently. However, the growth of digital file sharing has also increased the risk of cyberattacks. Sensitive data such as financial records, personal information, and confidential business documents are often transmitted through the internet. Without proper encryption and security mechanisms, these files may be exposed to hackers and malicious actors.

1.2 Challenges in Secure File Sharing

- Organizations face several challenges when implementing secure file sharing systems:
- Unauthorized access to shared files
- Data interception during file transmission
- Lack of strong encryption mechanisms
- Weak authentication and access control systems
- Difficulty in managing secure sharing permissions
- These challenges highlight the importance of developing secure platforms that protect files throughout their lifecycle.

1.3 Need for an Encrypted File Sharing Platform

A secure file sharing platform with end-to-end encryption can help protect sensitive data from unauthorized access. By encrypting files before transmission and ensuring that only authorized users

can decrypt them, organizations can significantly reduce the risk of data breaches. The proposed system Guardian Box provides a secure and efficient solution for encrypted file sharing with enhanced privacy and access control features.

II. RELATED WORK

Several existing platforms and research studies focus on secure data transmission and encrypted file storage. Many cloud storage services implement encryption techniques to protect stored data. However, in some systems, encryption keys are managed by service providers, which may still allow unauthorized access under certain circumstances. Some secure messaging and file sharing platforms use end-to-end encryption to protect user data. These systems ensure that only the sender and recipient can access the encrypted content. Despite these advancements, many platforms lack integrated features such as secure link sharing, detailed access control, and efficient file management. Additionally, some systems focus primarily on cloud storage rather than secure file transfer, limiting their usefulness for organizations that require confidential file sharing. Other platforms may require complex configurations, making them difficult for users with limited technical knowledge. The proposed system Guardian Box aims to overcome these limitations by providing a simple yet highly secure file sharing platform that integrates encryption, access control, and file management in a single system.

III. METHODOLOGY

The Guardian Box system is designed to provide secure file sharing through end-to-end encryption and controlled access mechanisms. The development process follows a structured approach including requirement analysis, system design, implementation, and testing. The platform allows users to upload files that are automatically encrypted before being stored or shared. When a user shares a file with another user, a secure link or encrypted key is generated. The recipient must authenticate and use the correct key to decrypt the file. The system also records user activities such as uploads, downloads, and sharing operations to ensure transparency and security.

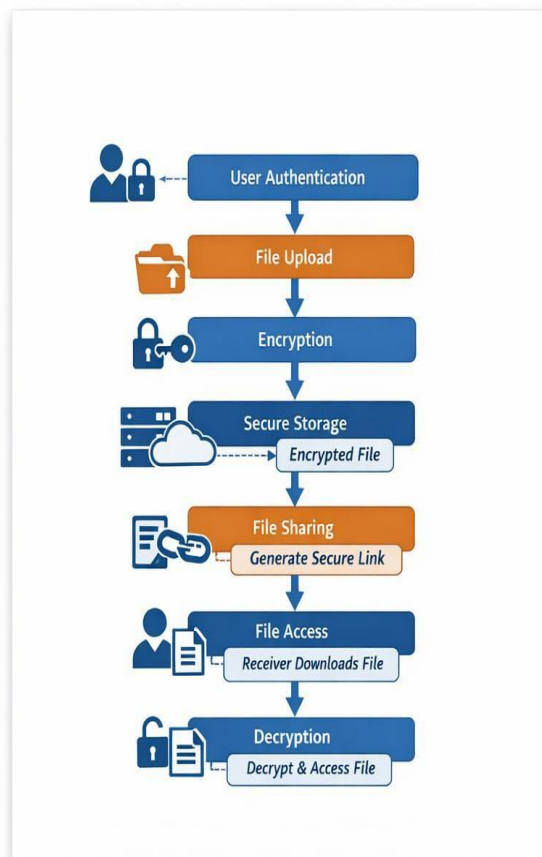


Figure 3: GuardianBox Secure File Sharing Methodology

3.1 Requirement Analysis

This phase identifies the security requirements needed for a secure file sharing platform. The system must support encrypted storage, secure transmission, authentication, and access control.

3.2 System Design

The architecture of the system is designed to integrate encryption algorithms, secure file storage, user authentication, and sharing mechanisms. The system also includes a simple user interface to improve usability.

3.3 Implementation

During implementation, the GuardianBox platform is developed using modern web technologies. The frontend handles user interactions such as file uploads and sharing, while the backend manages encryption, storage, and authentication processes.

3.4 Database Management

A centralized database stores user information, file metadata, access permissions, and activity logs. Sensitive file content is stored in encrypted form to prevent unauthorized access.

3.5 Testing and Validation

Various test cases are performed to ensure that encryption, file sharing, and access control features function correctly. Functional and security testing are conducted to verify system reliability.

IV. SYSTEM ARCHITECTURE

The architecture of the GuardianBox system consists of three main layers:

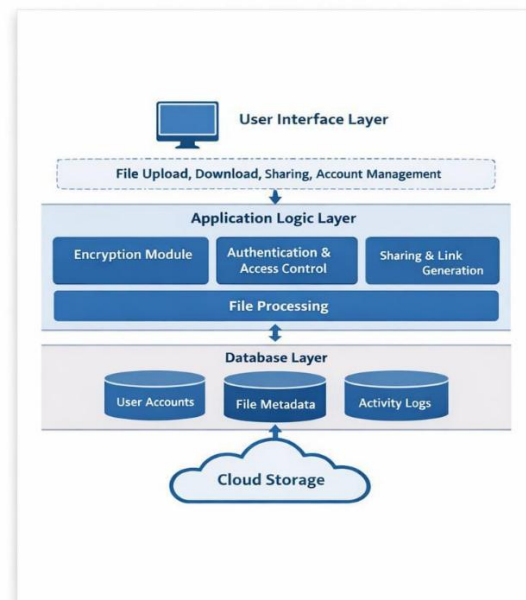


Figure 2: GuardianBox System Architecture

4.1 User Interface Layer

This layer provides a web-based interface where users can upload files, generate secure sharing links, and manage shared files. The dashboard allows users to easily interact with the platform.

4.2 Application Logic Layer

The application layer manages core system operations such as encryption, file processing, authentication, and sharing mechanisms. It acts as the bridge between the user interface and the database.

4.3 Database Layer

The database layer securely stores user accounts, encrypted file records, access permissions, and system logs. This centralized storage ensures organized and secure data management. The system also integrates encryption algorithms that protect files before transmission and ensure secure decryption by authorized users.

V. SYSTEM MODULES

The GuardianBox system is divided into several functional modules.

5.1 User Management Module

This module handles user registration, login authentication, and profile management. It ensures that only authorized users can access the platform.

5.2 File Upload Module

This module allows users to upload files to the system. Before storing the file, the system encrypts the data to ensure secure storage.

5.3 Encryption and Decryption Module

This module performs end-to-end encryption of files before sharing. Only users with the correct decryption key can access the original file.

5.4 Secure File Sharing Module

Users can generate secure sharing links or grant access to specific users. Access permissions ensure that only authorized individuals can download or view the shared files.

5.5 Monitoring and Activity Logging Module

This module tracks file sharing activities, downloads, and user actions. These logs help maintain system transparency and detect suspicious activities.

VI. EXPERIMENTAL RESULTS AND ANALYSIS

The GuardianBox system was implemented and tested to evaluate its performance and security effectiveness.

6.1 System Implementation

The platform was developed as a web-based application that allows users to securely upload, encrypt, and share files through an intuitive interface.

6.2 Functional Testing

Functional testing verified that all modules including file upload, encryption, sharing, and access control operate correctly.

6.3 Performance Evaluation

System performance was analyzed based on file upload speed, encryption efficiency, and secure link generation. The results indicate that the platform performs efficiently even with multiple users.

6.4 User Experience Analysis

The system interface was designed to be simple and user-friendly. Users can easily upload files, generate secure links, and manage file access permissions.

6.5 Result Discussion

The experimental results demonstrate that the GuardianBox system effectively protects files using end-to-end encryption while providing efficient and secure file sharing functionality. The integration of encryption, access control, and monitoring enhances overall data security.

REFERENCES

- [1] W. Stallings, *Cryptography and Network Security*. Noida, India: Pearson Education, 2017.
- [2] N. Ferguson, Bruce Schneier, and T. Kohno, *Cryptography Engineering*. Hoboken, NJ, USA: Wiley, 2010.
- [3] Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press.
- [4] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems," National Institute of Standards and Technology (NIST).
- [5] D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography*. Stanford, CA, USA: Stanford University.