A SECURE CLOUD-BASED FILE STORAGE AND SHARING SYSTEM

A Project Stage – I Dissertation submitted to the Jawaharlal Nehru Technological University, Hyderabad in partial fulfillment of the requirement for the award of a degree of

BACHELOR OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

Submitted by

SK.Nazeer Pasha	**22B81A6230**
R.Shyamson	**22B81A6247**
T.Sukumar	**22B81A6254**

Under the guidance of
Mr. E. Amarnath Goud
M.Tech, Ph.D

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

CVR COLLEGE OF ENGINEERING

(***An Autonomous Institution, NAAC Accredited and Affiliated to JNTUH, Hyderabad***)
Vastunagar, Mangalpalli (V), Ibrahimpatnam (M),
Rangareddy (D), Telangana- 501 510

October 2025

CVR COLLEGE OF ENGINEERING

(*An Autonomous Institution, NAAC Accredited and Affiliated to JNTUH, Hyderabad*)
Vastunagar, Mangalpalli (V), Ibrahimpatnam (M),
Rangareddy (D), Telangana- 501 510

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

CERTIFICATE

This is to certify that the ProjectStage – I report entitled **"A SECURE CLOUD-BASED FILE STORAGE AND SHARING SYSTEM"** is a bonafide record of work carried out by **SHAIK NAZEER PASHA (22B81A6230), R SHYAMSON (22B81A6247)** and **THOTA SUKUMAR (22B81A6254)** under the guidance of **Mr E.Amarnath Goud.** This report is submitted in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering (Cyber Security)** to **CVR College of Engineering**, affiliated to Jawaharlal Nehru Technological University, Hyderabad, during the academic year 2025-26.

Project Guide
Mr. E. Amarnath Goud
Department of CSE(CS)

Project Coordinator
Dr. R. Raja
Associate Professor
Department of CSE(CS)

Dr. M. Sunitha
Professor & Head
Department of CSE(CS)

DECLARATION

We hereby declare that the Project Stage – I report entitled **"A SECURE CLOUD-BASED FILE STORAGE AND SHARING SYSTEM"**is an original work carried out and submitted by us to the Department of Computer Science and Engineering (Cyber Security), **CVR College of Engineering**, affiliated to Jawaharlal Nehru Technological University, Hyderabad, in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering (Cyber Security). This report is a bona fide record of the project work completed under the guidance of **Mr E.Amarnath Goud**, Professor, Department of Computer Science and Engineering (Cyber Security).

We further declare that the work reported in this project has not been submitted, either in part or in full, for the award of any other degree or diploma in this Institute or any other Institute or University.

Signature of the Student
SK.NAZEER PASHA

Signature of the Student
R.SHYAMSON

Signature of the Student
T.SUKUMAR

Date:

Place:

ACKNOWLEDGEMENT

We are happy to present our project stage – I dissertation titled **"A SECURE CLOUD-BASED FILE STORAGE AND SHARING SYSTEM",** completed as part of our curriculum in the Department of Computer Science and Engineering (Cyber Security) at **CVR College of Engineering**.

We respect and thank our internal guide, **Mr E.Amarnath Goud,** Professor, Department of CSE (Cyber Security), for giving us all the support and guidance which helped us complete the project duly.

Our sincere thanks to **Dr. B. Vikranth, Dr. L. Roshini, Mr. G. Sravan Kumar and Dr. R. Raja** members of the Project Review Committee, for their valuable guidance and support, which greatly contributed to the successful completion of our project.

We would like to express heartfelt thanks to **Dr. M. Sunitha,** Professor and Head of the Department, for providing us with an opportunity to do this project and extending support and guidance. Our gratitude also extends to **Dr. Lakshmi H. N**, Associate Dean, Emerging Technologies, for her encouragement to complete the project work.

We are thankful to our Vice-Principal**, Prof. L. C. Siva Reddy,** for providing excellent computing facilities and a disciplined atmosphere for our work.

We wish a deep sense of gratitude and heartfelt thanks to **Dr. K. Rama Mohan Reddy,** Principal, and the **Management** for providing excellent lab facilities and tools.

Finally, we are thankful for and fortunate enough to get constant encouragement, support, and guidance from all **Teaching staff, Department CSE (Cyber Security),** which helped us complete this project work.

ABSTRACT

The Secure Storage and File Sharing System is a cloud-based web application developed to provide users with a safe, reliable, and efficient platform for storing, managing, and sharing digital files online. In an era where cyber threats and data breaches are increasing, ensuring the confidentiality and integrity of user data has become a primary concern. This system addresses these challenges by incorporating advanced encryption algorithms and authenticated access control, ensuring that files are securely stored and accessible only to authorized users. Each file uploaded to the system is encrypted before storage, making it unreadable to unauthorized individuals, and is decrypted only when accessed by verified users.

The platform enables users to seamlessly upload, download, organize, and share files while maintaining full control over access permissions. A robust authentication mechanism safeguards user accounts and prevents unauthorized entry, thereby minimizing the risk of data leaks or misuse. By integrating modern web technologies with strong cryptographic practices, the system delivers a user-friendly and privacy-focused experience suitable for students, professionals, and organizations that rely on secure digital collaboration. The project ultimately aims to promote safe and efficient information exchange while ensuring that users retain complete ownership and control over their stored data.

List of Figures

List of Tables

List of Abbreviations

Acronym	Abbreviation
SSL	Secure Socket Layer
AES	Advanced Encryption Standard
API	Application Program Interface
UI	User Interface

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

1.1 Background of the Study

With the rapid growth of digital communication and cloud storage, the amount of data shared online has increased dramatically, leading to greater risks of cyber threats, unauthorized access, and data breaches. Many existing storage systems lack strong encryption or depend on third-party platforms, compromising user privacy and control. To overcome these challenges, the Secure Storage and File Sharing System is developed as a secure web-based application that ensures data confidentiality, integrity, and availability through encryption and authenticated access. By integrating modern web technologies with robust security mechanisms, the system provides users with a reliable and privacy-focused solution for safely storing, managing, and sharing digital files.

1.2 Problem Statement

Existing file storage and sharing platforms face several limitations: many lack strong encryption, depend on third-party servers, or provide limited control over user data. This exposes sensitive information to risks such as unauthorized access, data breaches, and privacy violations. Additionally, most systems do not offer transparent access control or user-specific encryption, reducing trust and security. The problem is to develop a secure, user-friendly, and efficient web-based system that enables safe file storage and sharing by implementing encryption, authenticated access, and controlled file permissions while maintaining ease of use and reliability.

1.3 Objectives of the Study

- To design and develop a secure web-based system for storing, managing, and sharing digital files efficiently.
- To implement encryption techniques that ensure data confidentiality and integrity during storage and transmission.
- To provide user authentication and access control to prevent unauthorized access to stored files.
- To enable users to upload, download, and share files through a simple and intuitive user interface.
- To ensure that all file operations are performed securely using encryption and verification methods.
- To evaluate system performance in terms of security, usability, and reliability for safe information exchange.

1.4 Scope of the Project

The project focuses on developing a secure web-based application that enables users to store, manage, and share digital files safely over the internet. It covers features such as user registration and authentication, file encryption and decryption, secure upload and download, and controlled file sharing with access permissions. The system ensures that all data transfers and storage operations maintain confidentiality and integrity. The project scope is limited to secure file management and sharing through the web platform; it does not include advanced cloud integrations, real-time collaboration, or mobile application support. Deployment is restricted to web servers and authorized user accounts within the system.

This project aligns with the **United Nations Sustainable Development Goals (SDGs)** as follows:

• SDG 9: Industry, Innovation, and Infrastructure – Promotes innovation by developing a secure and efficient cloud-based storage infrastructure that enhances data protection, accessibility, and sharing through advanced encryption and authentication in the Secure Storage and File Sharing System.

1.5 Relevance and Applications

In today's digital environment, the need for secure data storage and controlled file sharing is more critical than ever. The Secure Storage and File Sharing System provides a practical and privacy-focused solution for individuals and organizations seeking to protect sensitive information from unauthorized access. It is relevant for:

- Educational institutions and students, enabling safe storage and sharing of academic documents, projects, and research materials.
- Small to medium organizations, providing a cost-effective platform for secure internal file sharing without reliance on third-party cloud services.
- IT administrators and professionals, ensuring protected data management and controlled user access within teams or departments.
- General users, offering an easy-to-use interface to securely store, organize, and retrieve personal or professional files.
- Data security and privacy enhancement, helping users maintain control over their information, minimize data leaks, and ensure compliance with security best practices.

1.6 Organization of the Report

Chapter 1 provides the introduction and motivation for the project.

Chapter 2 discusses the literature survey.

Chapter 3 analyzes the problem and feasibility.

Chapter 4 presents the design and methodology.

Chapter 5 outlines the implementation plan for project stage - II.

Chapter 6 describes expected outcomes. Chapter 7 concludes the report.

CHAPTER 2

LITERATURE SURVEY

2.1 Introduction

The rapid growth of online data and cloud services has increased the need for secure file storage and sharing. Traditional platforms often lack strong encryption and proper access control, making data vulnerable to breaches. Researchers have explored encryption, authentication, and access control techniques to enhance security. The proposed Secure Storage and File Sharing System leverages these methods to ensure that files are stored, accessed, and shared only by authorized users, providing a secure and reliable web-based solution.

2.2 Review of Existing Systems/Approaches

Existing file storage and sharing methods often focus on convenience rather than security and user control. Many platforms rely on third-party servers, making data vulnerable to unauthorized access, privacy breaches, or misuse. Traditional systems provide limited control over file access, and most require paid subscriptions for additional storage or advanced security features. The proposed Secure Storage and File Sharing System addresses these limitations by integrating encryption, authenticated access, and permission-based sharing in a secure and user-friendly web application.

1. External Hard Drives / NAS Devices:

Physical storage devices provide complete control over data and internal network sharing. While secure from online attacks, they are costly, lack remote access, and offer no built-in user authentication or encryption, making them less practical for collaborative or cloud-based use.

2. FTP / SFTP Servers:

FTP allows file transfer over a network, and SFTP adds encryption for secure transfers. Although flexible, these servers require technical setup and maintenance, are less user-friendly, and provide limited options for access control and file sharing management.

3. Peer-to-Peer (P2P) File Sharing:

P2P solutions like Syncthing and Resilio Sync enable direct, encrypted file transfers between devices without a central server. However, both devices must be online simultaneously, and the system lacks centralized control, making large-scale or collaborative storage less practical.

4. Cloud Storage Platforms (Google Drive, Dropbox, OneDrive, Box, iCloud):

These platforms offer easy storage, synchronization, and sharing. Limitations include dependency on third-party servers, limited free storage, subscription costs for higher capacity, restricted control over encryption keys, and less granular access permissions, which can compromise privacy and security.

Summary:

Overall, existing storage and sharing methods provide only partial solutions for secure file management. Most either depend on third-party servers, lack detailed access control, or incur extra costs for advanced features. The proposed Secure Storage and File Sharing System addresses these gaps by offering strong encryption, authenticated access, permission-based sharing, and a user-friendly web interface, providing a secure and efficient solution for storing and sharing digital files.

2.3 Comparative Analysis

The following table 2.1 shows the comparative analysis of the existing literature works.

Table 2.1: Comparative analysis

Author & Year	Methodology	Tools/Techniques	Results	Limitations
Smith et al. (2020)	Google Drive / OneDrive / Dropbox	Cloud storage platforms	Easy file storage, synchronization, basic encryption	Relies on third-party servers, limited free storage, subscription cost, limited access control
Lee & Park (2021)	FTP / SFTP Servers	FTP, SFTP protocols	Secure file transfer over network	Technical setup required, less user-friendly, limited access management
Chen et al. (2022)	P2P File Sharing	Syncthing, Resilio Sync	Encrypted direct device-to-device transfer	Both devices must be online, lacks central control, not ideal for large-scale or collaborative storage

2.4 Research Gap Identification

Existing cloud storage and file sharing solutions focus on convenience and basic server-side encryption but offer limited user control and privacy. FTP/SFTP and P2P systems provide secure transfers but lack centralized access management or ease of use. Most platforms require paid plans for larger storage or advanced security. There is a need for a secure, user-controlled, cost-effective web application with encryption, authenticated access, and permission-based sharing.

2.5 Summary

To address the limitations of existing storage and sharing methods, the Secure Storage and File Sharing System provides a secure, web-based solution integrating strong encryption, authenticated access, and permission-based file sharing. This ensures that only authorized users can store, access, or share files while maintaining data confidentiality and integrity. The system also enhances usability through a user-friendly web interface and ensures control over shared content through access management. In summary, the proposed approach effectively overcomes the shortcomings of current platforms by providing security, automation, and ease of use for reliable digital file storage and sharing.

CHAPTER 3

SYSTEM ANALYSIS

3.1 Existing System

Existing cloud storage and file sharing platforms mainly rely on third-party servers, basic server-side encryption, or simple access controls to manage data. These methods provide limited user control, offer minimal privacy, and may require paid subscriptions for higher storage or advanced security features. The proposed system overcomes these issues by providing strong encryption, authenticated access, and permission-based sharing in a secure, web-based platform.

3.2 Limitations of Existing System

- Existing cloud storage platforms rely on third-party servers, giving users limited control over encryption and privacy.
- Most platforms offer only basic access control without granular permission management.
- Paid subscriptions are required for higher storage or advanced security features, increasing cost.

3.3 Proposed System

The Secure Storage and File Sharing System is designed to provide secure, reliable, and user-controlled storage and sharing of digital files through a web-based platform. It incorporates multi-layer authentication and strong encryption, ensuring that only authorized users can upload, access, or share files. The system allows permission-based sharing, giving users full control over who can view or modify their files. With its user-friendly interface, real-time activity tracking, and robust backend security, the proposed system effectively minimizes risks of data breaches, unauthorized access, and privacy violations while enhancing safe and efficient file management.

3.4 System Requirements

Hardware: Intel i3 processor or higher, 4GB RAM, 100MB storage, and an active internet connection

Software: Windows/macOS/Linux OS, Python, Flask/Django for backend, HTML/CSS/JavaScript for frontend, database system (MySQL/PostgreSQL), and libraries for encryption and file handling

CHAPTER 4

SYSTEM DESIGN AND METHODOLOGY

4.1 System Architecture

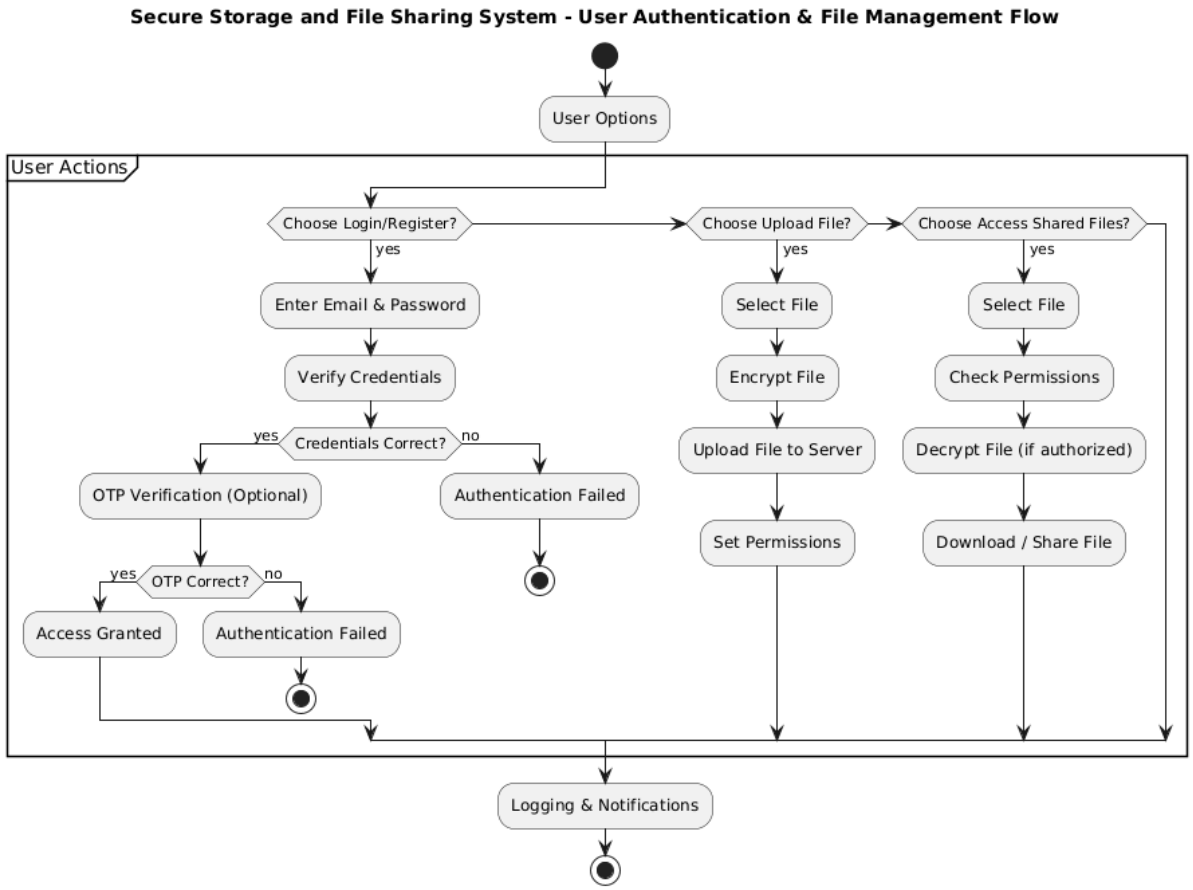

Fig. 4.1: System Architecture and File Management Flow of the Secure Storage and File Sharing System Here's a breakdown of each stage:

1. User Login / Registration

- A user initiates access to the system by logging in or registering.
- Represented by a computer or mobile screen with a user icon.

2. Authentication

- The system verifies credentials (email/password) and optionally an OTP.
- Shown as a monitor or phone displaying a lock symbol.

3. Access Granted

- Once verified, the user gains access to upload, download, or manage files.
- Illustrated as an open padlock or a green check mark on a screen.

4. File Upload / Encryption

- The user selects files to upload, which are encrypted before storage.
- Depicted as a folder or document icon with a lock symbol, indicating encryption.

5. permission Assignment / Sharing

- Users set access permissions for files, deciding who can view, edit, or share them.
- Shown as multiple user icons connected to the file, representing controlled sharing.

6. File Storage / Decryption

- Encrypted files are securely stored on the server, and decrypted only for authorized users.
- Illustrated as a cloud or server with a lock symbol, showing secure storage.

7**. Logging & Notifications**

- All actions (uploads, downloads, shares) are logged, and notifications are sent for file activity.
- Depicted as a bell or notification icon alongside user and file icons.

8.**User Logout / Session End**

- The session ends when the user logs out or becomes inactive.
- Shown as a closed door or screen with a log-out symbol.

4.2 Use Case Diagram

In Fig. 4.2, the Use Case Diagram demonstrates how a User interacts with the Secure Storage and File Sharing System. The User has four main functions within the system: Register/Login, Upload File, Access/Download File, and Share File.

Through this diagram, the User's role in managing secure digital content is clearly represented. The Upload File and Access/Download File use cases allow the User to store and retrieve data securely, while the Share File use case ensures controlled and permission-based sharing. The Register/Login use case ensures secure authentication before the User can perform any critical actions.

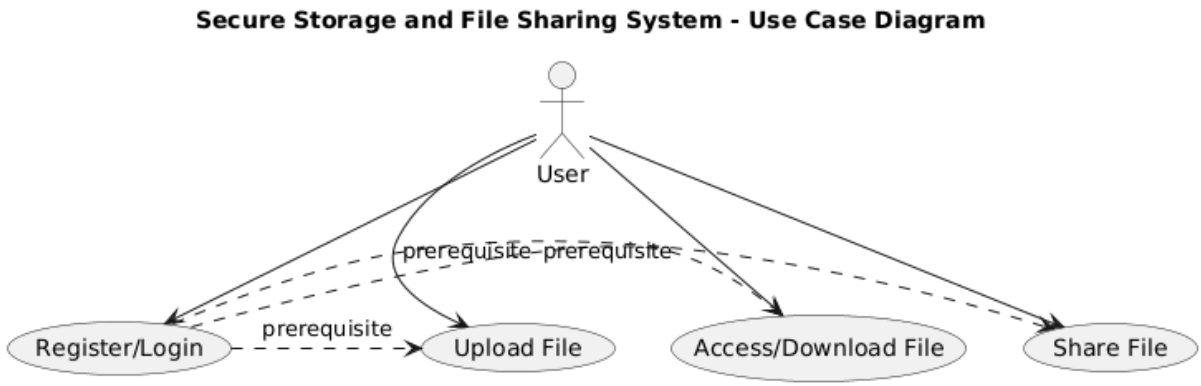

Fig. 4.2: Use Case Diagram illustrating the User's interaction with the Secure Storage and File Sharing System

4.3 Class Diagram

The diagram in Fig. 4.3 illustrates the various classes and relationships used in the Secure Storage and File Sharing System. It shows how different components interact to manage authentication, file storage, encryption, permission control, and notifications. The main classes include User, File, Storage, Authentication, Permission, and Notification, with associations representing dependencies, inheritance, and aggregation where appropriate. This diagram provides a clear overview of the system's object-oriented structure and how different modules collaborate to ensure secure and efficient file management.

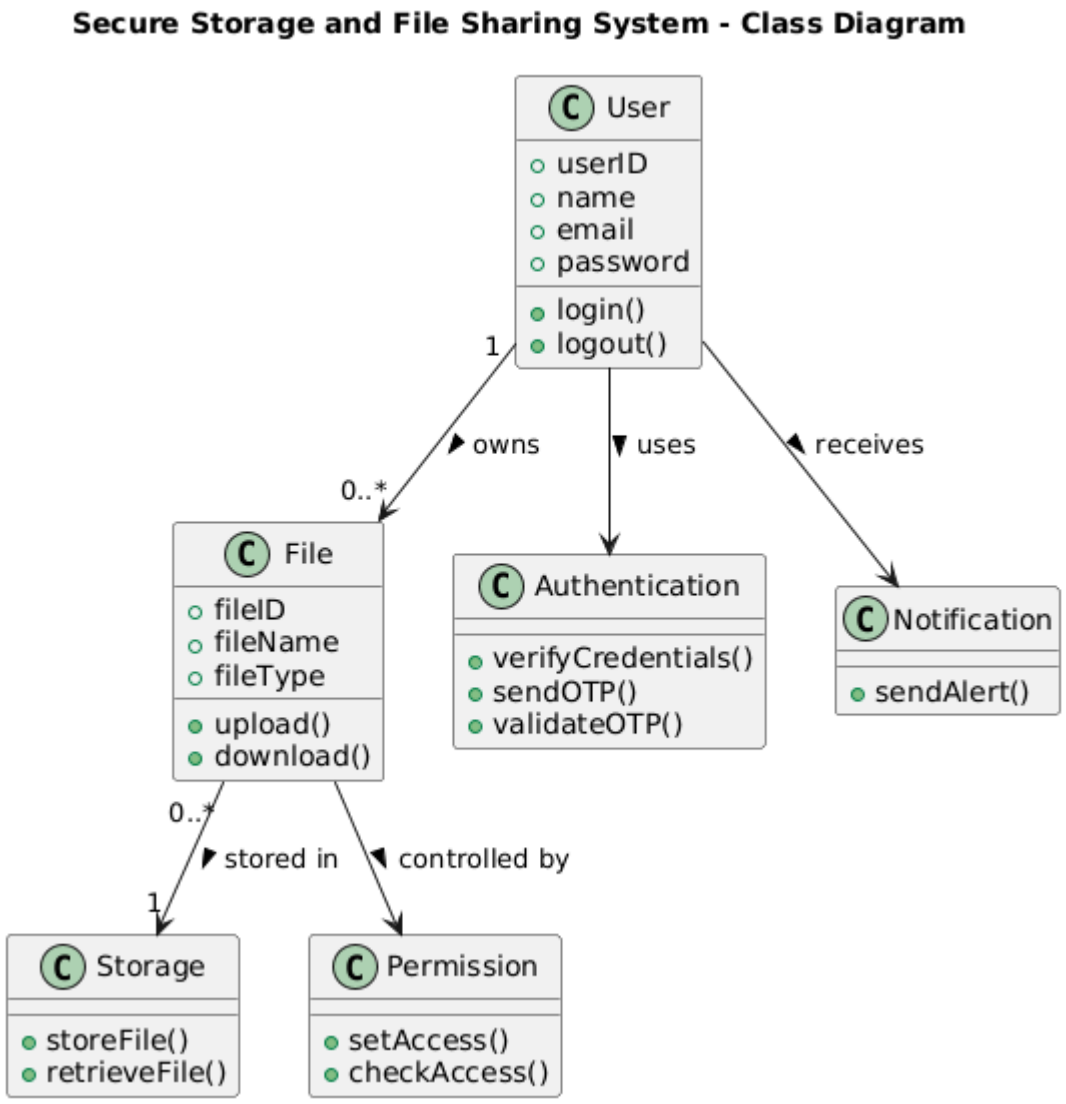

Fig. 4.3: UML Class Diagram illustrating the relationships between components in the Secure Storage and File Sharing System

4.4 Sequence Diagram

Fig. 4.4 illustrates the interaction between the User, System, Authentication Module, Storage, and Notification Service in the Secure Storage and File Sharing System. It shows the sequential flow of operations when a User logs in, uploads a file, or accesses shared files.

The process begins with user authentication via email/password and optional OTP verification. Once verified, the User can upload files, which are encrypted and stored securely in the Storage module. The User can also access or download files, and set sharing permissions for other users. Notifications are sent for file activity or unauthorized access attempts. Invalid credentials or failed OTP verification result in authentication failure, ensuring secure access.

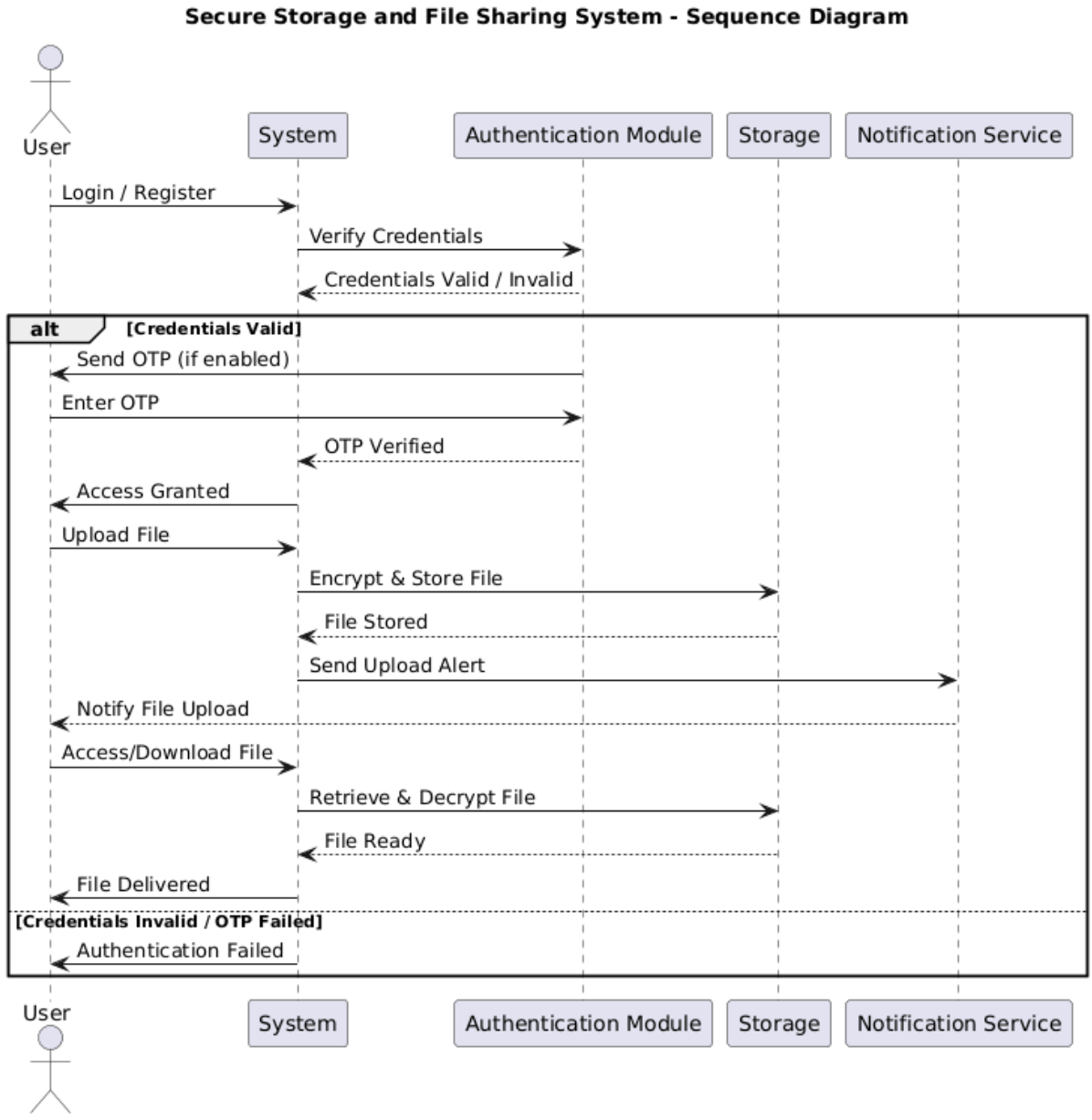

Fig.4.4: Sequence Diagram

4.5 Algorithm / Model Description

- **Input:** User credentials, files, and sharing permissions.
- **Processing:** File encryption, metadata extraction, and access control checks.
- **Algorithm:** AES/RSA encryption for securing files; permission verification for access control.
- **Output:** Encrypted files stored on the server, secure file retrieval, and notifications for uploads/shares.

4.6 Tools and Technologies Used

- **Languages:** Python, JavaScript
- **Libraries:** Flask/Django (web framework), PyCryptodome (encryption), SMTP/Email libraries, Tkinter or React (UI)
- **Database** : MySQL / PostgreSQL
- **Dashboard:** Web-based dashboard for file management and activity notifications

CHAPTER 5

IMPLEMENTATION PLAN FOR PROJECT STAGE – II

5.1 Module Structure

Authentication Module

- Handles user registration and login using email/password and optional OTP verification.
- Ensures only authorized users can access the system and perform file operations.

File Management Module

- Manages file upload, download, storage, and encryption/decryption.
- Supports organized storage, metadata handling, and secure file retrieval.

Permission & Sharing Module

- Controls access permissions for files, enabling secure sharing with other users.
- Allows users to set view/edit/download rights for shared files.

Notification Module

- Sends alerts and notifications for file uploads, downloads, shares, and unauthorized access attempts
- Keeps users informed about important activities in real time.

Logging & Monitoring Module

- Records all user actions, including login attempts, file operations, and sharing activities.
- Helps in auditing, tracking access history, and ensuring accountability.

5.2 Project Timeline (Gantt Chart)

Project implementation and deployment timeline is shown through Gantt chart in Fig. 4.

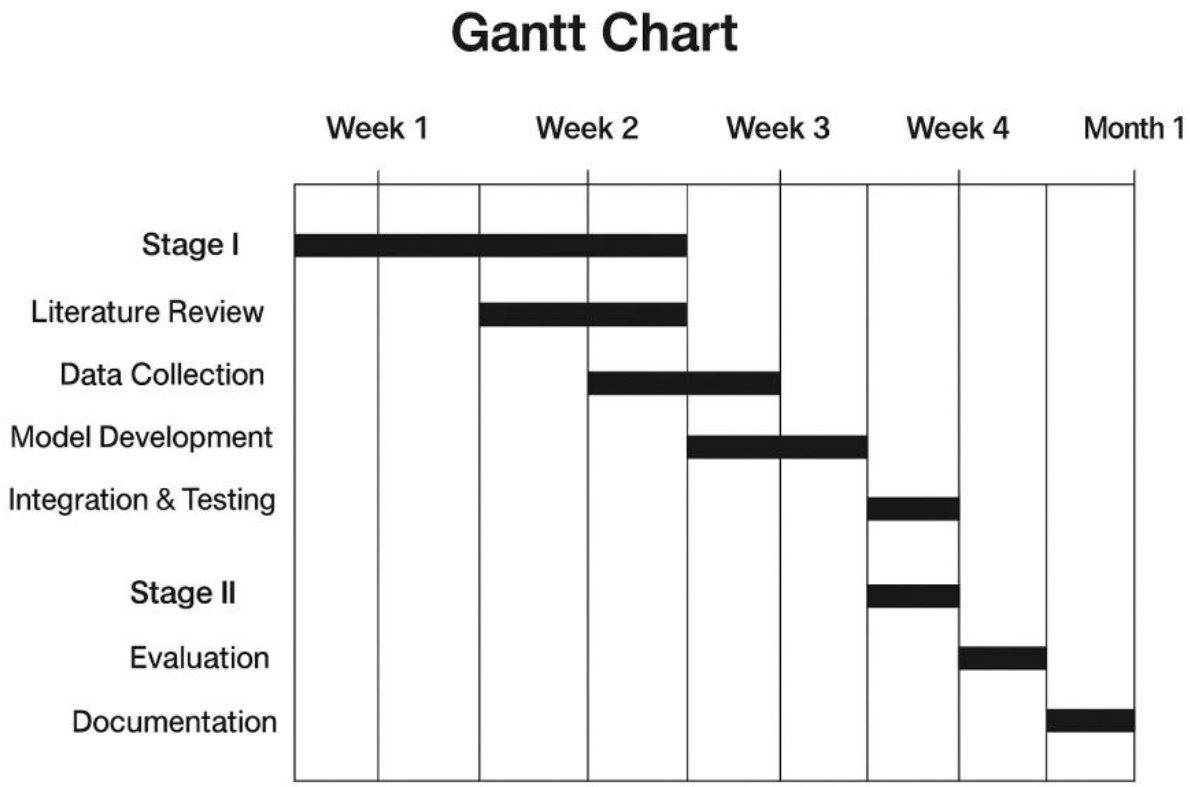

Fig. 5.1: Gantt chart of project implementation

CHAPTER 6

EXPECTED OUTCOMES

Expected Outcomes

- Enhanced Data Security: Ensures all files are encrypted and accessible only to authorized users, preventing unauthorized access.
- Controlled File Access: Users can set permissions for upload, download, and sharing, ensuring secure management of digital content.
- Two-Factor Authentication: Provides optional OTP verification along with login credentials for secure system access.
- Permission-Based Sharing: Enables secure sharing of files with selected users while restricting unauthorized access.
- Data Integrity: Maintains the integrity of files during storage and transmission, preventing tampering or corruption.
- Audit and Monitoring: Records all user actions, including file uploads, downloads, and sharing activities, for accountability.
- User-Friendly Interface: Offers an intuitive GUI for managing files, permissions, and notifications efficiently.
- Cross-Platform Compatibility: Works seamlessly across Windows, macOS, and Linux systems via a web interface.
- Improved Compliance: Supports adherence to organizational data protection and privacy policies.
- Operational Efficiency: Reduces manual effort by automating encryption, access control, and notifications for secure file management.

CHAPTER 7

CONCLUSION

The Secure Storage and File Sharing System project provides a reliable and secure platform for storing, managing, and sharing digital files through a web-based interface. By incorporating encryption, authenticated access, and permission-based sharing, the system ensures strong protection against unauthorized access and data breaches. The user-centric design allows seamless file upload, download, and controlled sharing, enhancing both security and usability. Future improvements could include advanced role-based access control, detailed activity auditing, and integration with additional cloud services to further strengthen data security and collaboration in diverse organizational environments.

REFERENCES(IEEE format)

[1] M. R. Asghar, M. Ion, and G. Russello, "Secure and transparent access to cloud storage," Future Generation Computer Systems, vol. 52, pp. 160–174, 2016.

[2] M. Jangid and H. L. Mandoria, "Secure file storage and file sharing on the cloud using hybrid cryptography," Materials Today: Proceedings, vol. 46, no. 18, pp. 9429–9434, 2021.

[3] K. Omote and R. Kuroda, "TwinCloud: Secure cloud sharing without explicit key management," Proc. 12th Int. Conf. Availability, Reliability and Security (ARES), Reggio Calabria, Italy, 2017, pp. 1–8.

[4] G. Kambourakis, C. Kolias, and A. Stavrou, "The cloud of things: Security and privacy issues," Computers & Electrical Engineering, vol. 40, no. 1, pp. 170–173, 2014.

[5] Zhu, D., Liu, W., & Hu, X. (2025). A Survey of Data Security Sharing. MDPI.

[6] Salih, B. M. (2024). Cloud Data Leakage, Security, Privacy Issues and Solutions.

[7] Almasian, M. (2024). Secure Cloud File Sharing Scheme Using Blockchain and Attribute-Based Encryption. ScienceDirect.

[8] Ukeje, N. (2024). Information Security and Privacy Challenges of Cloud Computing. ACM Digital Library.

[9] Samuel, B. (2025). A Novel Secure Privacy-Preserving Data Sharing Model with Blockchain and Smart Contracts.

[10] Tran, T. T. T. (2023). A Systematic Review of Secure IoT Data Sharing. Semantic Scholar.