



Secure Cloud-Based Media Sharing: Scalable Access Control And Privacy-Preserving Deduplication

Dhiraj Shinde, Sanket Navthar, Jayesh Udavant, Rushikesh Jadhav

B.E. Students,

Department of Computer Engineering

Sinhgad Institute of Technology, Lonavala, India

Prof. K.S.Mulani

Assistant Professor,

Department of Computer Engineering

Sinhgad Institute of Technology, Lonavala, India

Abstract— This development aims to contribute treatments (medicines) that are either fresh or stale in nature. The new treatments can be handed to a poor individual who will be able to use them in the future. This programme assists the user in donating or selling any unused medicines to a non-profit organisation. There are three people that make up this body: the administrator, the non-governmental organisation, and the user. A system administrator will log in and manage users, including deleting and barring users who are giving incorrect or expired drugs. In addition, the administration has a consultant, similar to the appointment requested by the NGO. The administration receives a monthly noise of remedies that have been contributed. Authorizations are used to register and login for non-profit organisations. They can promote a request for an appointment, which will be added to a more appropriate and comprehensive list by the administrator. The standard is managed by an NGO, which aids in the preservation of the history of the current medicines. In the event of a safety issue, an NGO can also modify their PIN. Authorizations are used to allow users to register and log in. They can provide remedies by providing remedy details and generating demand; once this has been agreed upon by the administration and the NGO, they will plan a date for the donation to take place. Also available to consumers is a history of their previous remedial transactions.

Keywords: Scalable Access Control, Privacy-Preserving Deduplication, Cloud-based Media Sharing, Data Privacy

I. INTRODUCTION

A. Overview

It is network based computing system and it is the large storage space area where the authorized user can access the platform from anywhere and anytime with the good internet or network connectivity. Due to the explosive growth of media contents, secure deduplication schemes have been proposed to save the storage space in cloud. firstly introduced the AES encryption scheme which utilizes a message derived key to encrypt the message. Hence, identical plaintexts produce the same ciphertexts. proposed AES, which subsumes convergent encryption and gives detailed security definitions. The cloud computing is the advancement to shared volume of information through the network. There are lots of techniques that are used to providing security for data in cloud. But current techniques are as better related to the ciphertext. So here, we propose information gathering, sharing and restrictive distribution plan with multi-owner privacy preserving in cloud. Here, data owner can impart private information to group of clients through cloud in secure.

II. MOTIVATION

- ▶ To the proposed system we use AES Algorithm For The Encryption and Decryption and Provide Data Security and Secure access control
- ▶ To use MD 5 Algorithm For The Avoid Deduplication On the data.
- ▶ Developing a system focused on data deduplication to optimize storage efficiency and tackle data redundancy challenges.
- ▶ Providers meet diverse needs, offering cost-effective data storage, transfer, and backup, along with access to various cloud resources.

III. GOAL AND OBJECTIVES

- ▶ Goal: Enhance Cloud Storage Efficiency
- ▶ Objective: Implement a secure deduplication system to minimize redundant data, optimizing storage space and reducing communication overhead.
- ▶ Goal: Ensure Privacy in Cloud Data Deduplication

- ▶ Objective: Develop an encryption-based deduplication scheme with efficient re-encryption, safeguarding sensitive user data and addressing vulnerabilities.
- ▶ Goal: Improve Performance of Data Deduplication in Cloud Data Centers
- ▶ Objective: Propose and implement a block-level deduplication approach, comparing and demonstrating superior results over conventional file-level deduplication.

IV. OPEN ISSUES

A lot of work has been done in this field thanks to its extensive use and applications. This section mentions some of the approaches that have been implemented to achieve the same purpose. These works are mainly differentiated from the techniques for unused medicine systems.

V. LITERATURE SURVEY

LEVER: Secure Deduplicated Cloud Storage with Encrypted Two-Party Interactions in Cyber-Physical Systems

Author: Sahil Garg

Publisher: IEEE Region 10 Humanitarian Technology Conference

Year: 2020

Summary: This study presents a secure deduplicated cloud storage system with encrypted interactions, focusing on cyber-physical systems. It emphasizes data confidentiality, tag consistency, access control, and resistance to brute-force attacks, highlighting the importance of secure interactions in deduplicated storage.

2. Secure Block-level Data Deduplication Approach for Cloud Data Centers

Author: Arslan Rafi

Publisher: IEEE Region 10 Humanitarian Technology Conference

Year: 2020

Summary: This paper proposes a block-level deduplication method for cloud data centers, which is more efficient than traditional file-level deduplication. It focuses on optimizing storage efficiency and improving data confidentiality through secure deduplication techniques.

3. Privacy-Preserving Media Sharing with Scalable Access Control and Secure Deduplication in Mobile Cloud Computing

Author: Zhicheng Zhang, Yixian Yang

Publisher: IEEE Region 10 Humanitarian Technology Conference

Year: 2019

Summary: This research addresses privacy-preserving media sharing in mobile cloud computing. It introduces scalable access control mechanisms combined with secure deduplication to enhance storage efficiency while maintaining user privacy.

4. Secure and Efficient Data Deduplication in JointCloud Storage

Author: Nankun Mu

Publisher: IEEE Region 10 Humanitarian Technology Conference

Year: 2021

Summary: This study introduces a deduplication scheme for JointCloud storage, focusing on security and efficiency. It explores dynamic ownership management and secure Proof-of-Ownership to handle changes in data ownership effectively, enhancing deduplication performance.

Summary of Key Findings

Data Confidentiality and Security: All studies emphasize the importance of data confidentiality and security in deduplication schemes. Techniques like encrypted interactions and secure Proof-of-Ownership are critical.

Deduplication Efficiency: Block-level deduplication is shown to be more efficient than file-level deduplication, optimizing storage and reducing redundancy.

Privacy Preservation: Scalable access control mechanisms are crucial for maintaining user privacy, especially in mobile and cloud computing environments.

Dynamic Ownership Management: Effective management of dynamic data ownership is necessary to maintain security and efficiency in deduplication systems.

Challenges: Current challenges include addressing scalability for large data volumes, managing dynamic ownership securely, countering side-channel attacks, and improving re-encryption schemes.

Name of the paper	Author Name	Publisher	Year
LEVER : Secure Deduplicated Cloud Storage with Encrypted Two-Party International in Cyber-Physical Systems	Sahil Garg	7 JEEE Region 10 Humanitarian Technology Conference	2020

Secure Block-Level Data Deduplication approach for Cloud Data Centers	Arslan Rafi	IEEE Region 10 Humanitarian Technology Conference	2020
Privacy- Preserving Media Sharing with Scalable Access Control and Secure Deduplication in Mobile Cloud Computing	Zhicheng Zhang, and Yixian Yang	IEEE Region 10 Humanitarian Technology Conference	2019
Secure and Efficient Data Deduplication in Joint Cloud Storage	Nankun Mu	IEEE Region 10 Humanitarian Technology Conference	2021

VI. SYSTEM ARCHITECTURE

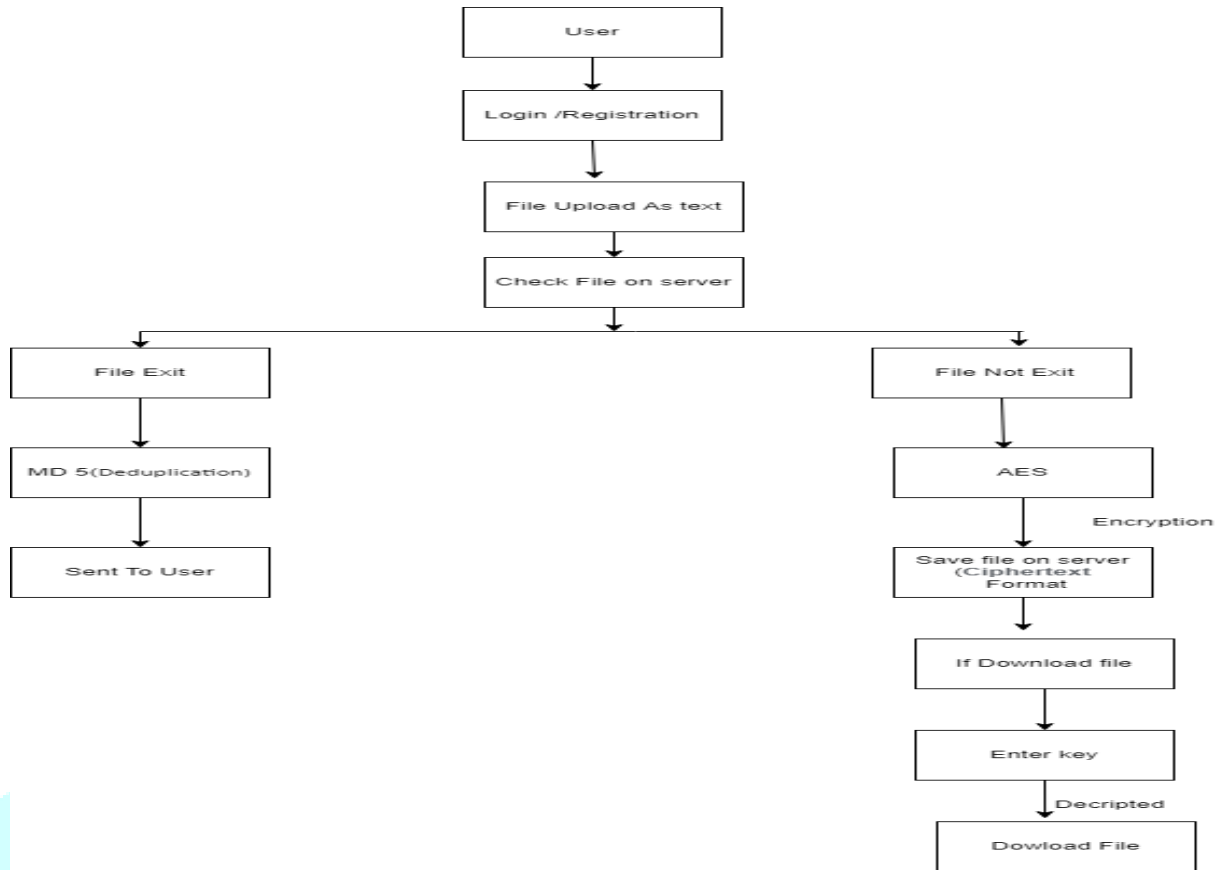
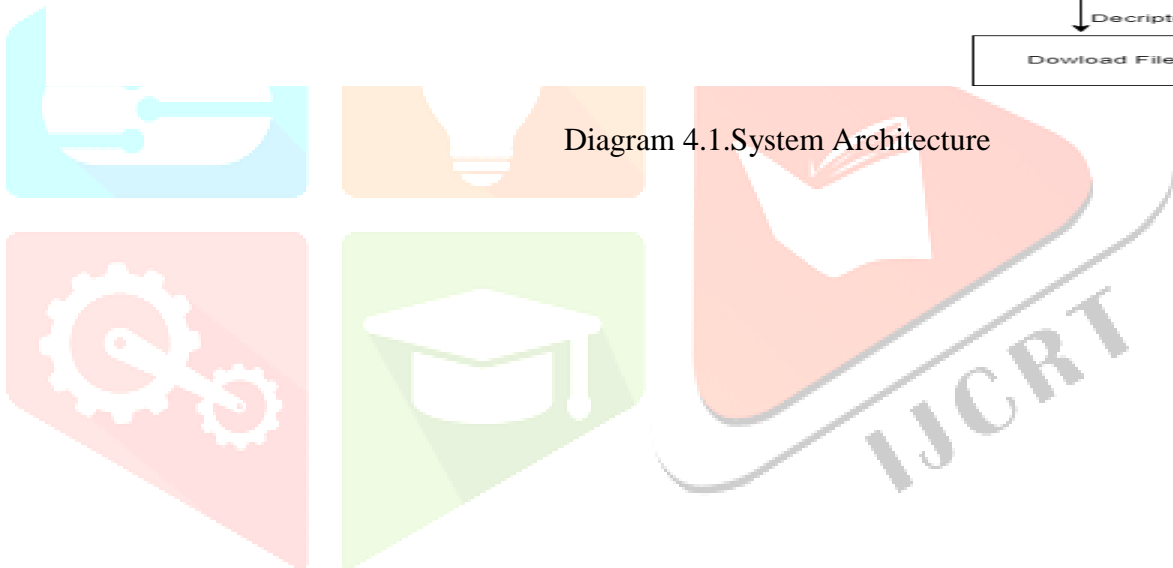


Diagram 4.1. System Architecture



VIII. USE CASE DIAGRAM

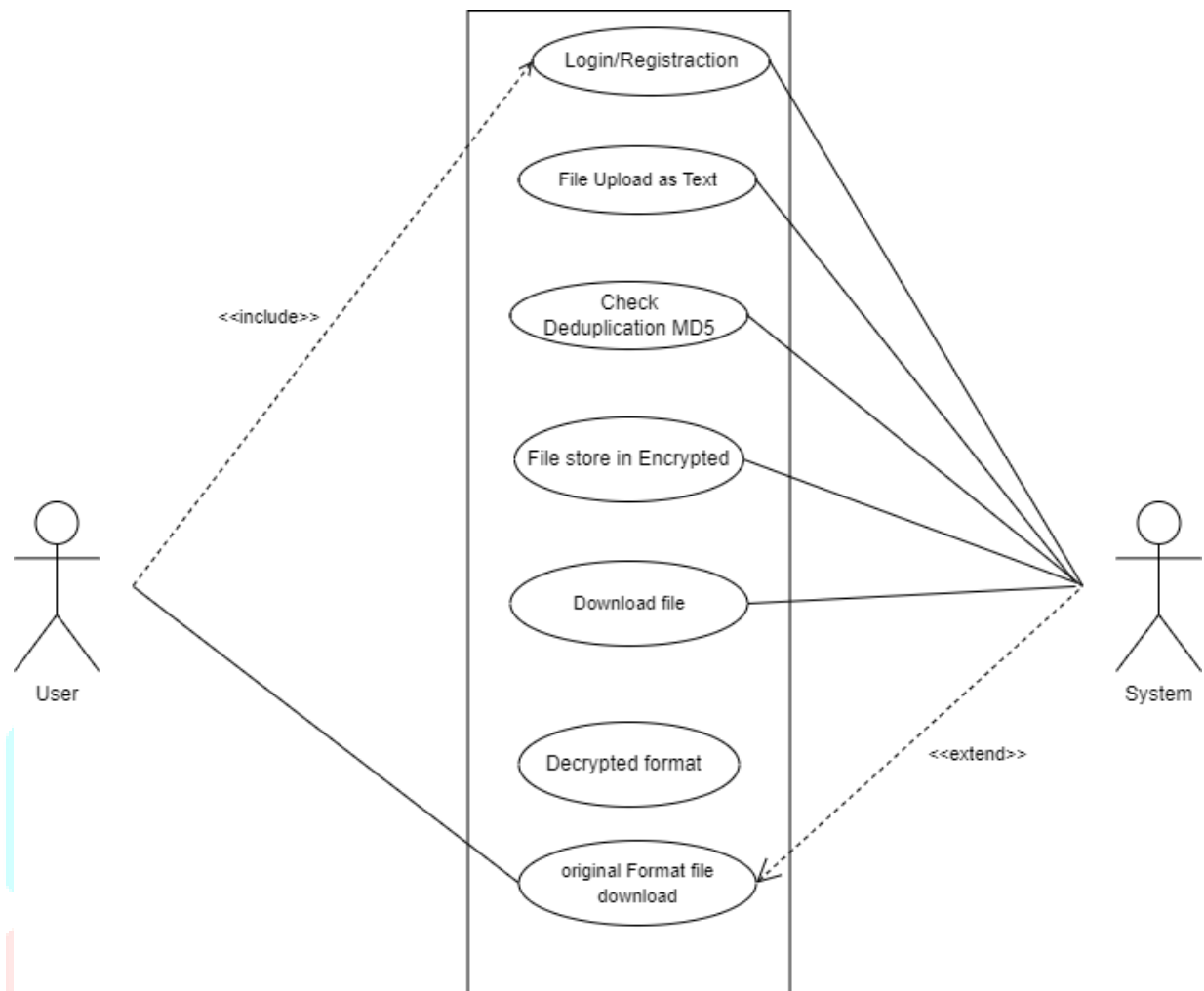
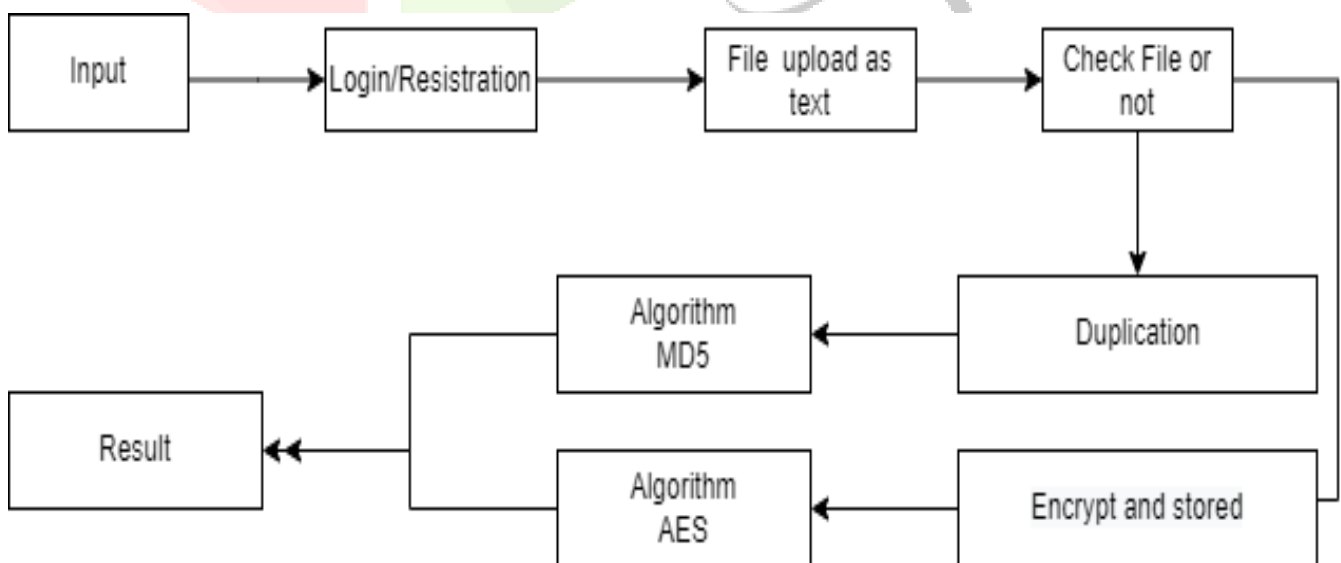


Diagram 6.1. Use Case Diagram



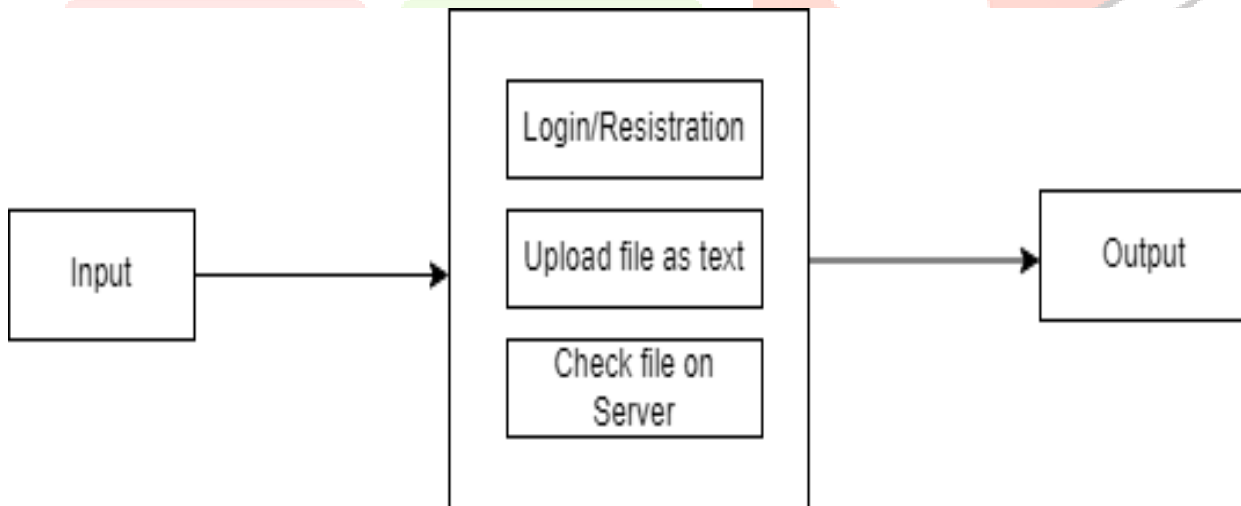
IX. SOFTWARE REQUIREMENTS

- Operating System - Windows 7/8/10
- Front End - HTML, CSS, Bootstrap
- Database - MySQL
- IDE - VS Code
- Language - java

X. HARDWARE REQUIREMENTS

- Processor - Intel i3/i5/i7
- Speed - 3.1 GHz
- RAM - 4 GB(min)
- Hard Disk - 40 GB
- Keyboard - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

XI. PROJECT FLOW



XII. RESULTS

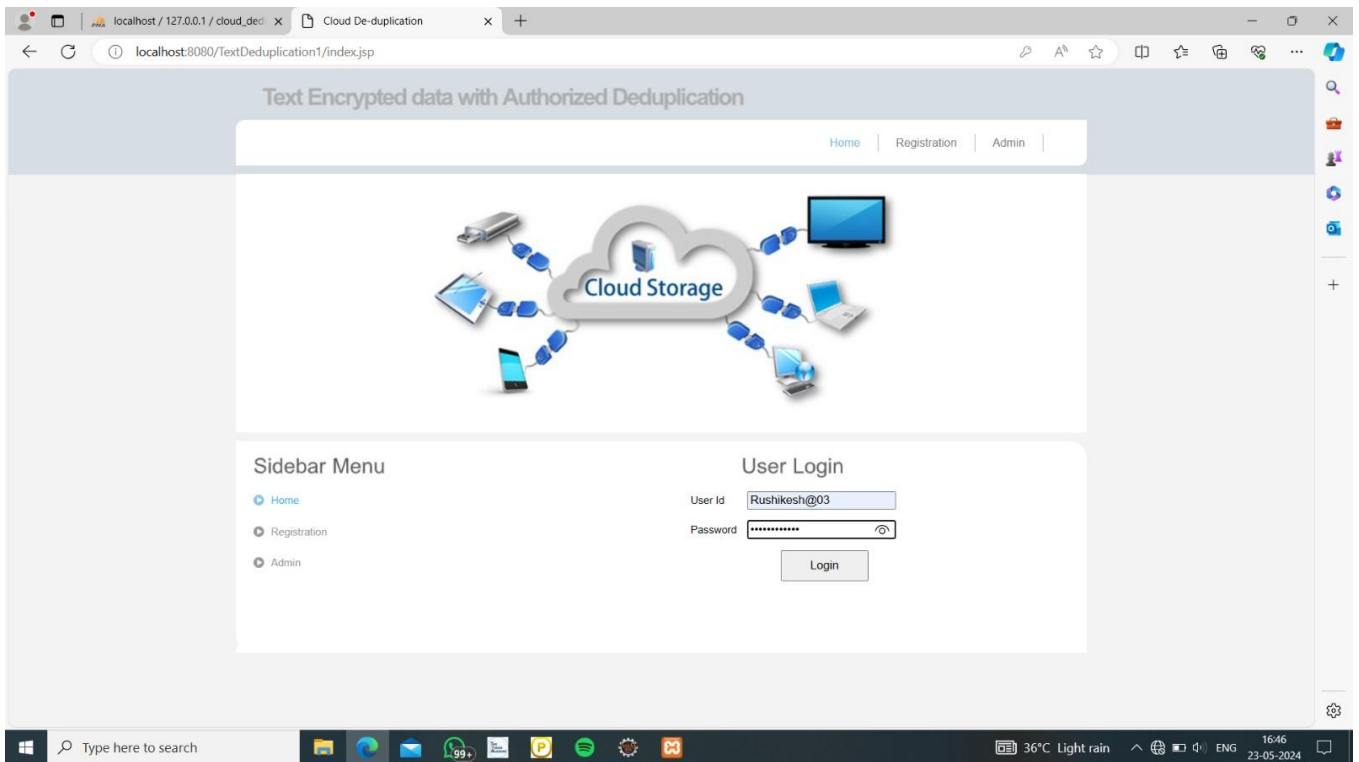


Fig .Dashboard

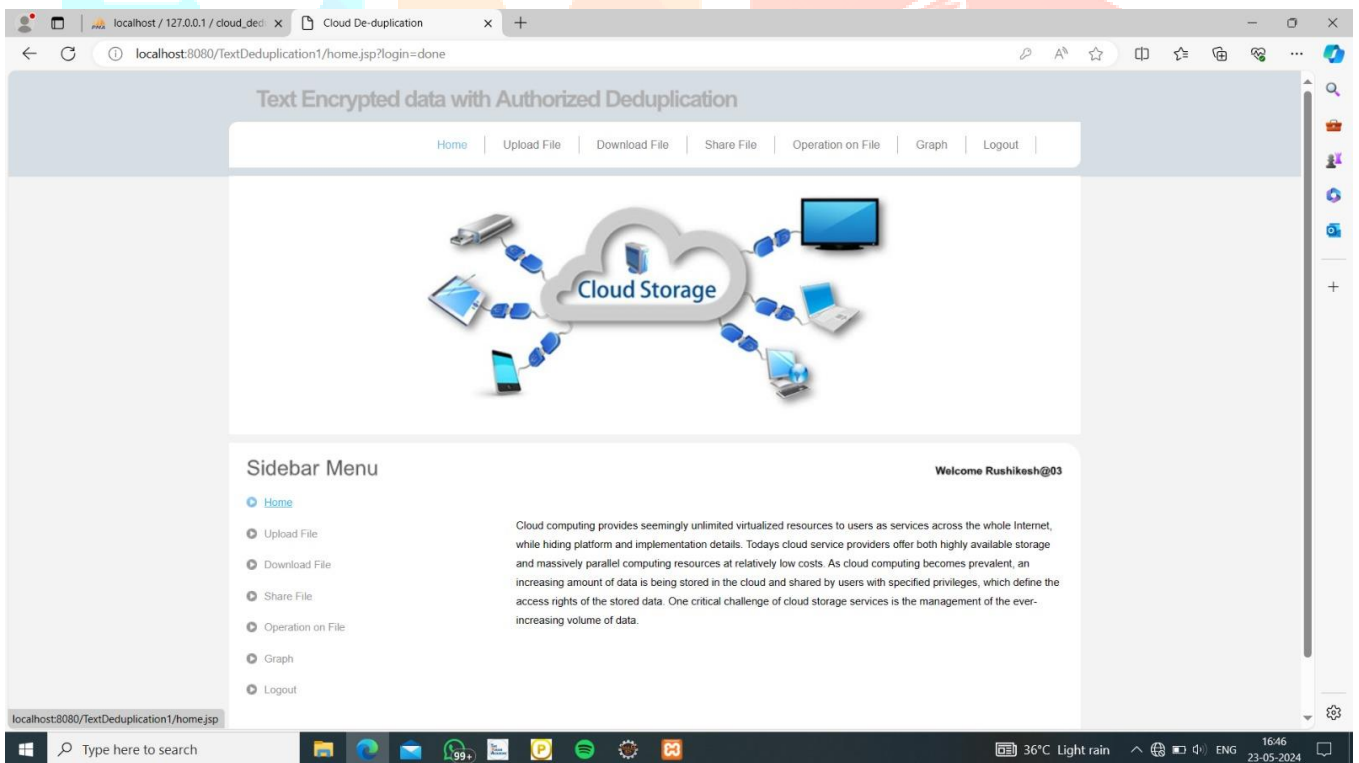


Fig. HomePage

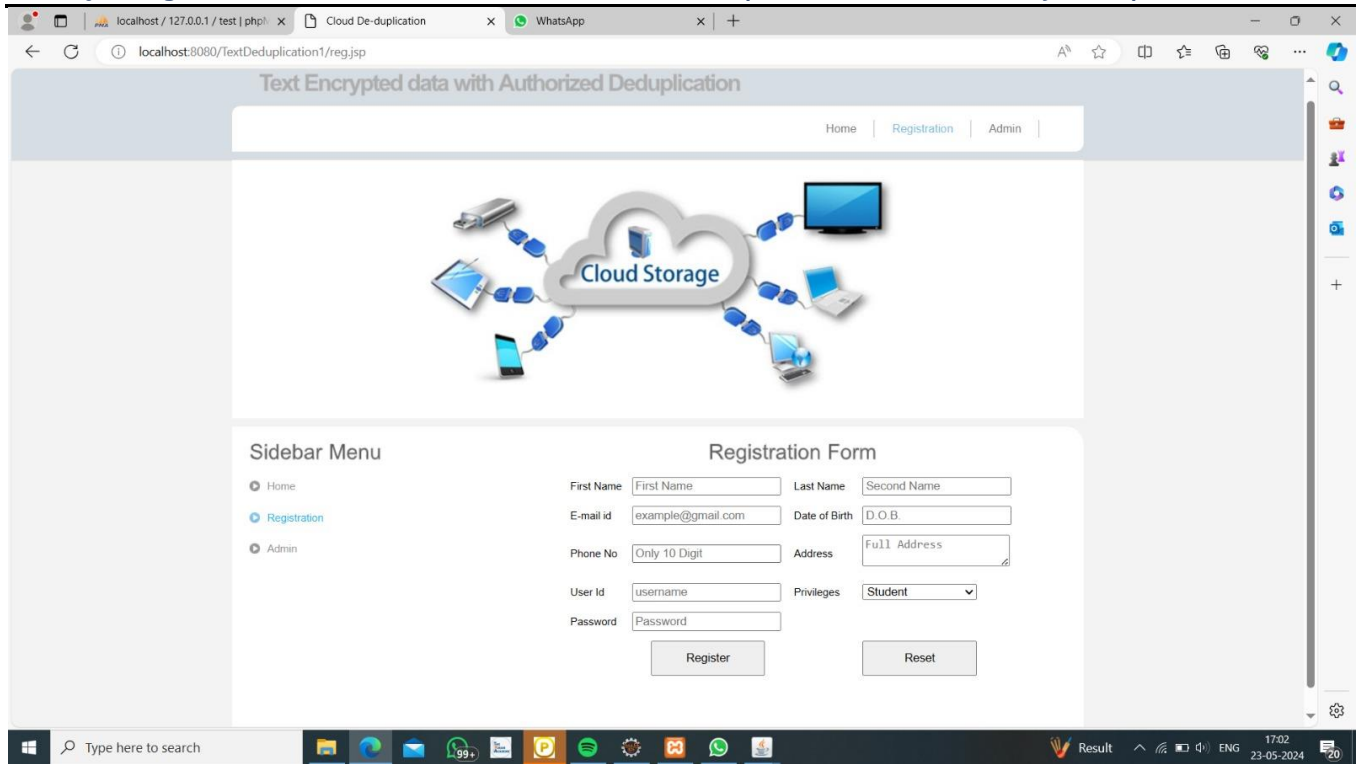


Fig. Registration Form

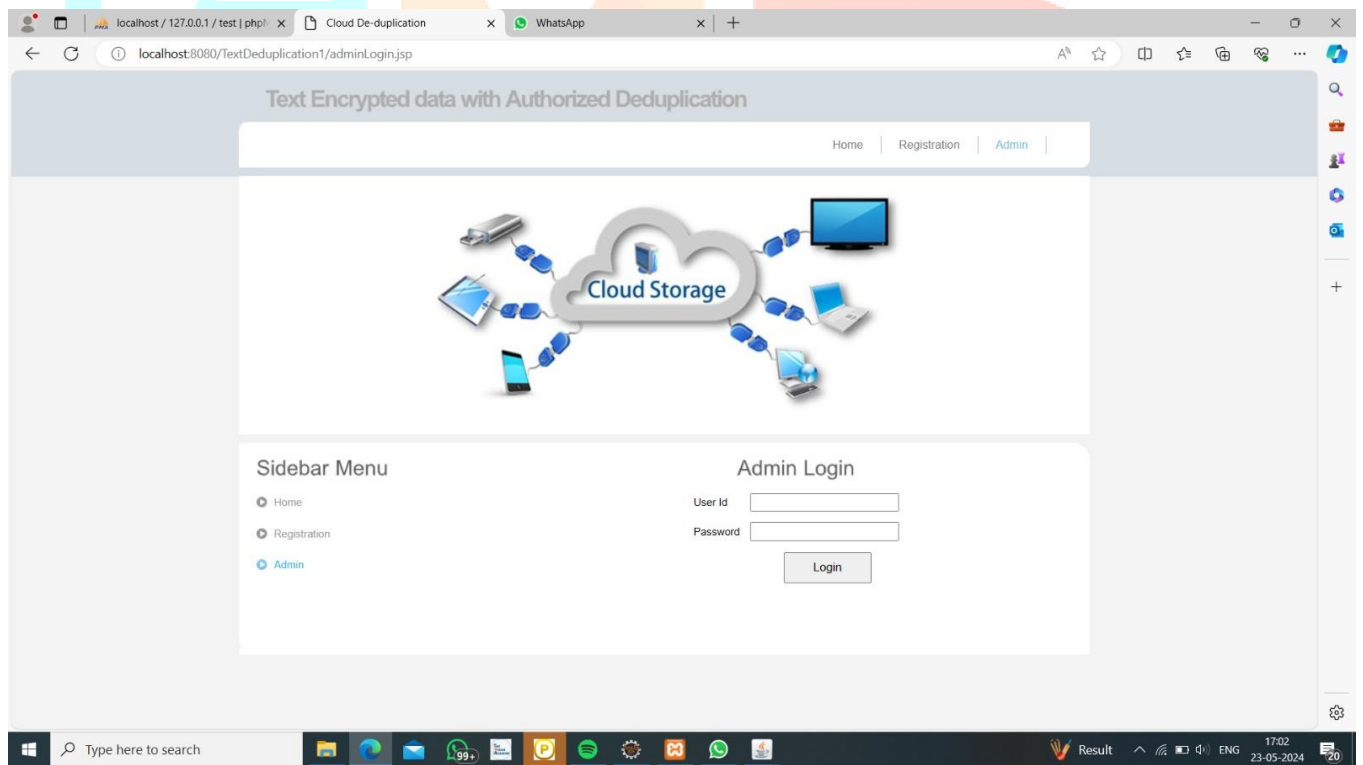
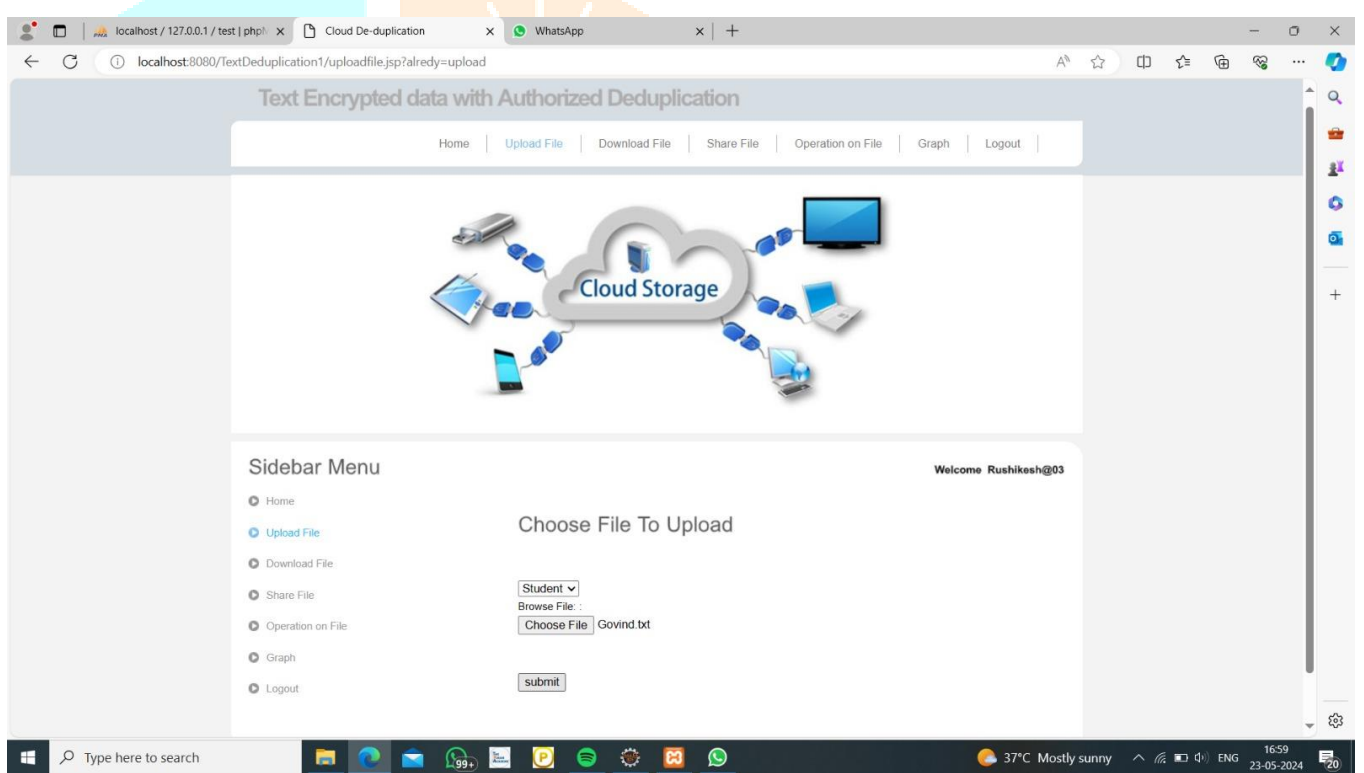
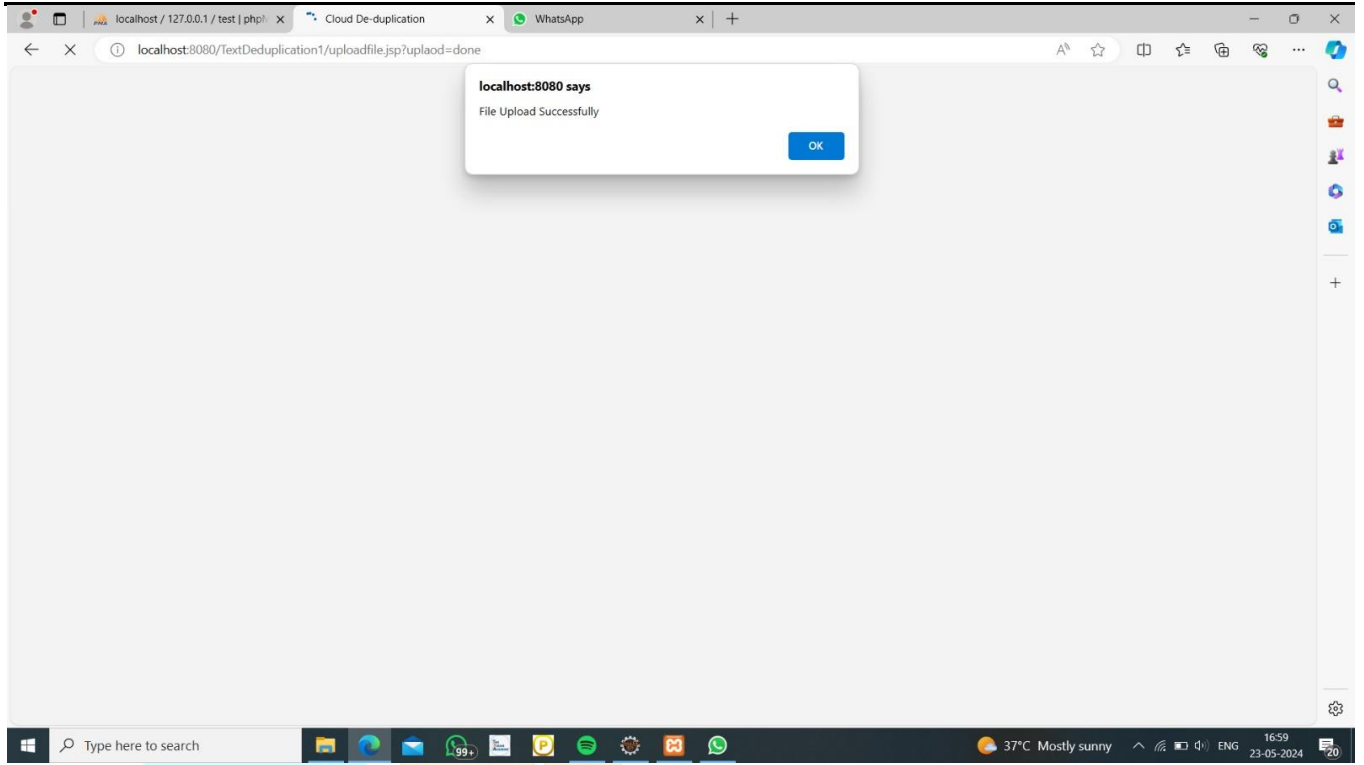
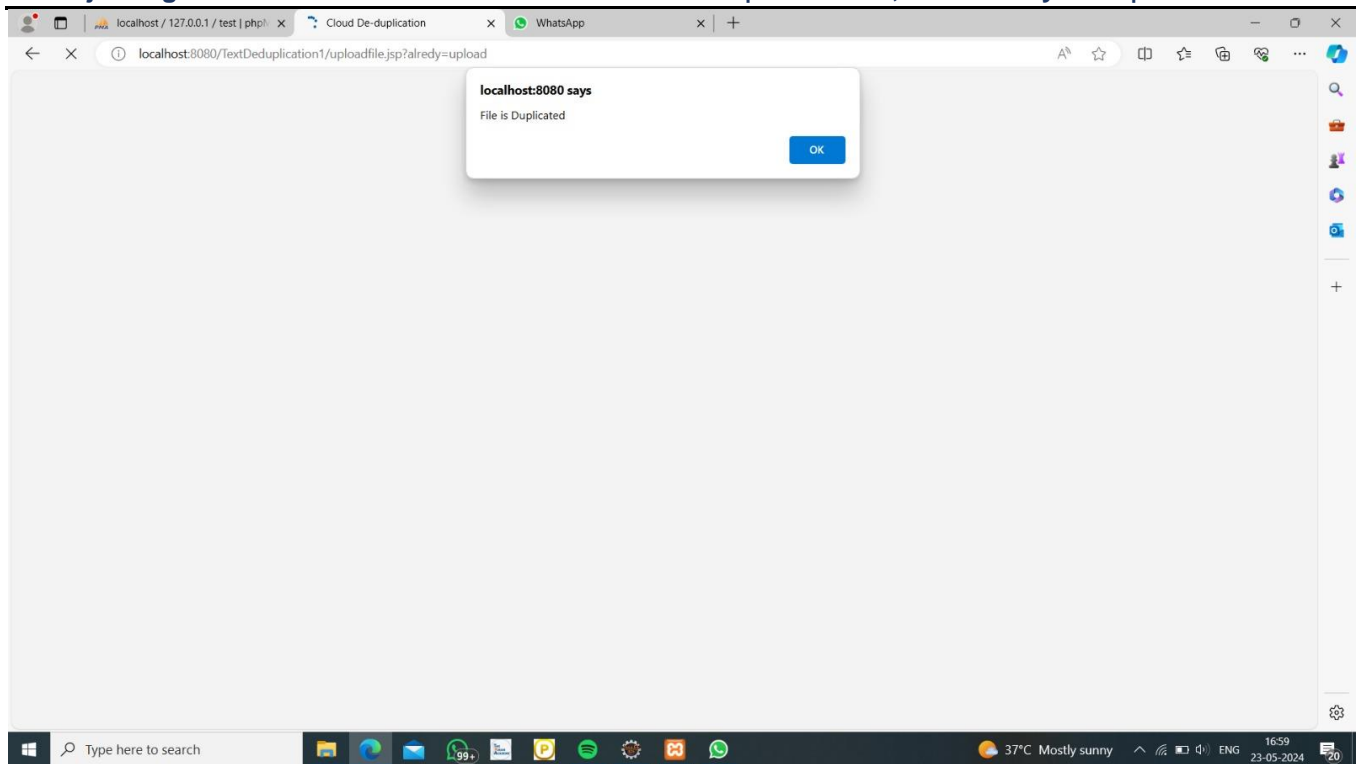


Fig. Login Form





XIII. APPLICATIONS

- Optimize storage, reduce costs, ensure data security.
- SECURE STORAGE AND SHARING OF PATIENT RECORDS, COMPLIANCE WITH REGULATIONS.

XIV. CONCLUSION

- secure cloud data deduplication plays a pivotal role in optimizing storage space and communication overhead while ensuring data confidentiality and access control. The surveyed literature reveals diverse approaches addressing challenges such as privacy, efficiency, ownership management, and resilience against attacks. While significant progress has been made, open issues remain in enhancing scalability, countering side-channel attacks, and improving interoperability. Future research should focus on refining existing schemes, developing efficient re-encryption methods, and addressing emerging issues to further enhance the security and efficiency of cloud data deduplication systems.

XV. REFERENCES

- [1] LEVER: Secure Deduplicated Cloud Storage with Encrypted Two-Party Interactions in Cyber-Physical Systems, 2020 . [Online]. Available:<http://www.who.int/workforcealliance/countries/bgd/en/> .
- [2] Secure Block-level Data Deduplication approach for Cloud Data Centers [Online].
- [3] Privacy-Preserving Media Sharing with Scalable Access Control and Secure Deduplication in Mobile Cloud Computing
- [4] Secure and Efficient Data Deduplication in JointCloud Storage

