A

Mini-Project Report on

## WEB BASED SECURE FILE SHARING

Submitted in partial fulfillment of the requirements for the degree of

BACHELOR OF ENGINEERING

IN

### Computer Science & Engineering

### Artificial Intelligence & Machine Learning

by

Akash Singh (22106065)

Vedant Vethekar (22106090)

Dhruv Wesavkar (22106016)

Mohit Rajput (22106126)

Under the guidance of

## Prof. Monali korde



### Department of Computer Science & Engineering

### (Artificial Intelligence & Machine Learning)

**A. P. Shah Institute of Technology**

**G. B. Road, Kasarvadavali, Thane (W)-400615**

**University Of Mumbai**

**2023-2024**

## 

## A. P. SHAH INSTITUTE OF TECHNOLOGY

## CERTIFICATE

This is to certify that the project entitled “**web based secure file sharing”** is a bonafide work of Akash Singh (22106065), Vedant Vethekar (22106090), Dhruv Wesavkar (22106016), Mohit Rajput (22106123) submitted to the University of Mumbai in partial fulfillment of the requirement for the award of **Bachelor of Engineering** in **Computer Science & Engineering (Artificial Intelligence & Machine Learning).**

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Prof. Monali Korde | Dr. Jaya Gupta |
| Mini Project Guide | Head of Department |

## 

## A. P. SHAH INSTITUTE OF TECHNOLOGY

## Project Report Approval

This Mini project report entitled “**Web based secure file sharing*”*** by **Akash Singh, Dhruv Wesavkar, Vedant Vethekar and Mohit Rajput**is approved for the degree of ***Bachelor of Engineering*** in ***Computer Science &Engineering***, (AIML) ***2023-24***.

##### External Examiner:

##### Internal Examiner:

Place: APSIT, Thane

Date:

**Declaration**

##### We declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

|  |  |  |  |
| --- | --- | --- | --- |
| Akash singh | Dhruv Wesavkar | Vedant Vethekar | Mohit Rajput |
| (22106065) | (22106016) | (22106090) | (22106126) |

#### ABSTRACT

This project proposes the development of a robust file-sharing website with a hierarchical access structure. Designed for secure collaboration, the system appoints an administrator responsible for creating user accounts. Each user account is equipped with unique login credentials, ensuring authentication and access control. Once registered, users gain the capability to securely upload various files and documents onto the platform. Emphasizing data security, the system restricts access solely to authenticated users, safeguarding confidentiality and integrity. Users can seamlessly share and utilize uploaded documents, promoting efficient collaboration and information exchange. Through its user-friendly interface and stringent security measures, the platform facilitates enhanced file management and sharing experiences. This project addresses the need for a reliable and secure environment for collaborative work, offering a comprehensive solution for efficient and protected file sharing among users

**Index**

|  |  |  |  |
| --- | --- | --- | --- |
| Index | | | Page no. |
| Chapter-1 | | |  |
|  | Introduction | | 1 |
|  |  |  |  |
| Chapter-2 | | |  |
|  | Literature Survey | |  |
|  | 2.1 | History | 4 |
|  | 2.1 | Review | 4 |
|  |  |  |  |
| Chapter-3 | | |  |
|  | Problem Statement | | 7 |
|  |  |  |  |
| Chapter-4 | | |  |
|  | Experimental Setup | |  |
|  | 4.1 | Hardware setup | 9 |
|  | 4.2 | Software Setup | 9 |
|  |  |  |  |
| Chapter-5 | | |  |
|  | Proposed system and Implementation | |  |
|  | 5.1 | Block Diagram of proposed system | 12 |
|  | 5.2 | Description of Block diagram | 12 |
|  | 5.3 | Implementation | 13 |
|  |  |  |  |
| Chapter-6 | | |  |
|  | Conclusion | | 15 |
|  |  |  |  |
| References | | | 16 |
|  |  |  |  |

**Table of Figures:**

|  |  |  |
| --- | --- | --- |
| Figures no. | Figures name | Page no. |
| 5.1.1 | User Authentication | 12 |
| 5.1.2 | File Download WorkFlow | 12 |
| 5.1.3 | Login Page. | 13 |
| 5.1.4 | Dashboard | 13 |
| 5.1.5 | New user page | 14 |
| 5.1.6 | User list | 14 |
| 5.1.7 | Document list | 14 |
| 5.1.8 | View Document | 15 |

# CHAPTER 1 INTRODUCTION

### INTRODUCTION

|  |
| --- |
| This project endeavors to create a comprehensive and secure file-sharing website tailored for collaborative work environments. In addition to robust user management features, the platform offers advanced functionalities such as document listing, detailed file descriptions, and customizable access controls.  At the heart of the system is a hierarchical access structure, empowering an appointed administrator to oversee user management tasks. Administrators hold the exclusive privilege to add new users, granting them access by providing essential user details including name, contact number, role, email address, physical address, and a password. Additionally, each user is assigned a unique character for identification and access purposes, enhancing security measures.  Once registered, users gain access to a myriad of features aimed at streamlining file sharing and collaboration. Users can upload files along with descriptive titles and descriptions, facilitating easy organization and retrieval. Furthermore, the platform supports actions such as downloading files and document deletion, allowing users to manage shared content effectively.  The system emphasizes security and confidentiality by restricting access to authenticated users only. Administrators possess the authority to monitor and regulate user activities, ensuring compliance with security protocols and organizational policies. Through its intuitive interface and robust security measures, the platform fosters efficient collaboration and information exchange among users.  Overall, this project seeks to address the growing need for a reliable, user-friendly, and secure platform for collaborative file sharing. By combining advanced features with stringent security measures, the platform aims to provide a comprehensive solution for modern workplace collaboration needs. |

# CHAPTER 2 LITERATURE SURVEY

#### LITERATURE SURVEY

###### 2.1-HISTORY

|  |
| --- |
| File-sharing systems have evolved significantly over the years, adapting to the changing needs of users and advancements in technology. The history of file sharing can be traced back to the early days of the internet when users relied on primitive methods such as FTP (File Transfer Protocol) to exchange files. However, these methods lacked robust security features and were cumbersome to use.  The emergence of peer-to-peer (P2P) file-sharing networks in the late 1990s revolutionized the way files were shared online. P2P networks such as Napster, Kazaa, and BitTorrent allowed users to share files directly with each other, bypassing centralized servers. While these platforms offered greater efficiency and scalability, they also raised concerns about copyright infringement and security vulnerabilities.  In response to these challenges, modern file-sharing systems have incorporated advanced security measures and user management features. Cloud-based file-sharing platforms such as Dropbox, Google Drive, and Microsoft OneDrive have gained popularity due to their ease of use and robust security features. These platforms offer centralized storage and collaboration tools, allowing users to securely share files with others while maintaining control over access permissions. |

#### 2.2-LITERATURE REVIEW

|  |
| --- |
| Numerous studies have explored various aspects of file-sharing systems, ranging from user behavior and security concerns to system design and implementation. A study by Li et al. (2018) investigated the security vulnerabilities of popular cloud-based file-sharing platforms and proposed mitigation strategies to address these vulnerabilities. The study highlighted the importance of encryption, access control, and secure authentication mechanisms in ensuring the confidentiality and integrity of shared files.  In a review by Gupta et al. (2020), different file-sharing protocols and technologies were compared, highlighting their strengths and weaknesses. The review emphasized the need for a balance between usability and security in file-sharing systems, as well as the importance of user education and awareness in mitigating security risks.  Furthermore, research by Smith et al. (2019) explored the impact of file-sharing on collaborative work environments, examining how different sharing mechanisms influence productivity and collaboration among users. The study identified key factors that contribute to the effectiveness of file-sharing systems, such as ease of use, access control, and integration with existing workflows. |

|  |
| --- |
| **[1]** **Kallahalla, Mahesh, Erik Riedel, Ram Swaminathan, Qian Wang, and Kevin Fu. "Plutus: Scalable secure file sharing on untrusted storage." In 2nd USENIX Conference on File and Storage Technologies . 2003**  Plutus is a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. In particular, it makes novel use of cryptographic primitives to protect and share files. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. We explain the mechanisms in Plutus to reduce the number of cryptographic keys exchanged between users by using filegroups, distinguish file read and write access, handle user revocation efficiently, and allow an untrusted server to authorize file writes. We have built a prototype of Plutus on OpenAFS. Measurements of this prototype show that Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic.  **[2] Castiglione, A., Catuogno, L., Del Sorbo, A., Fiore, U. and Palmieri, F., 2014. A secure file sharing service for distributed computing environments. The Journal of Supercomputing, 67, pp.691-710**  Distributed cryptographic file systems enable file sharing among their users and need the adoption of a key management scheme for the distribution of the cryptographic keys to authorized users according to their specific degree of trust. In this paper we describe the architecture of a basic secure file sharing facility relying on a multi-party threshold-based key-sharing scheme that can be overlaid on top of the existing stackable networked file systems, and discuss its application to the implementation of distributed cryptographic file systems. It provides flexible access control policies supporting multiple combination of roles and trust profiles. A proof of concept prototype implementation within the Linux operating system framework demonstrated its effectiveness in terms of performance and security robustness  **[3]Seeland, Josh, Sarah Elaine Eaton, and Brenda M. Stoesz. "Leveraging college copyright ownership against file-sharing and contract cheating websites." *Contract Cheating in Higher Education: Global Perspectives on Theory, Practice, and Policy*. Cham: Springer International Publishing, 2022. 61-76**.  To engage with the complex world of academic integrity, an institution will require a veritable arsenal of cumulative strategies. Academic file-sharing is “…the transfer and trading of lecture materials, notes, assessment tasks, answers, and responses with others, including Internet-based sites, for a fee, for free, or to barter” (Rogerson & Basanta, *Handbook of academic integrity*. Springer, 2016, p. 274). Academic file-sharing can take place on the same platforms as contract cheating, yet there are major differences between these two behaviours. Copyright ownership is a factor that effects the ease of having files removed from these sites, and varies among institutions. By framing academic file-sharing as both a copyright issue and an academic integrity violation, academic misconduct could be reduced, and possibly set a precedent for other colleges and universities to leverage copyright ownership.  [4] **Oberholzer-Gee, Felix, and Koleman Strumpf. "The effect of file sharing on record sales: An empirical analysis." *Journal of political economy* 115.1 (2007): 1-42.**  For industries ranging from software to pharmaceuticals and entertainment, there is an intense debate about the appropriate level of protection for intellectual property. The Internet provides a natural crucible to assess the implications of reduced protection because it drastically lowers the cost of copying information. In this paper, we analyze whether file sharing has reduced the legal sales of music. While this question is receiving considerable attention in academia, industry, and Congress, we are the first to study the phenomenon employing data on actual downloads of music files. We match an extensive sample of downloads to U.S. sales data for a large number of albums. To establish causality, we instrument for downloads using data on international school holidays. Downloads have an effect on sales that is statistically indistinguishable from zero. |

# CHAPTER 3

# Problem Statement

#### 3.Problem Statement

|  |
| --- |
| Contemporary collaboration demands efficient and secure file-sharing platforms that strike a delicate balance between user accessibility and data protection. Existing solutions often fall short, presenting challenges in usability and security. Usability concerns arise from complex interfaces, hindering seamless collaboration, while security issues stem from the increasing vulnerability of shared data to unauthorized access and privacy breaches. Traditional file-sharing services may lack versatility, offering limited options for diverse collaboration needs. Furthermore, the authentication-centric approach of many platforms introduces friction in collaborative endeavors, as users are compelled to create accounts or log in, impeding spontaneous information exchange.  In this landscape, there is a pressing need for a comprehensive and user-friendly file-sharing platform that addresses these challenges. The platform should facilitate public file sharing, text collaboration, and private rooms with password protection, catering to a spectrum of collaborative scenarios. Ensuring a seamless user experience while prioritizing robust security measures is paramount. This problem statement encapsulates the demand for a novel file-sharing solution capable of meeting the diverse collaboration needs of users, fostering a collaborative environment that is both accessible and secure. The challenge lies in creating a platform that aligns with contemporary collaboration expectations, streamlining file-sharing processes while safeguarding sensitive information.  Top of Form |

# CHAPTER 4

# Experimental Setup

#### 4. Experimental Setup

|  |
| --- |
| **4.1 Hardware Setup:**  1. Server: A dedicated server or cloud-based server with sufficient processing power, memory, and storage capacity to host the file-sharing platform and manage user accounts and file storage.  2. Networking Equipment: Routers, switches, and firewalls to establish and secure network connections between users and the server.  3. Storage Devices: High-capacity storage devices such as hard disk drives (HDDs) or solid-state drives (SSDs) to store uploaded files securely.  4. Backup Systems: Backup servers or cloud backup services to ensure data redundancy and disaster recovery in case of hardware failures or data loss.  **4.2 Software Setup:**  The software setup encompasses the configuration and deployment of the necessary software components to enable the file-sharing platform's functionality. This involves the installation and configuration of the operating system, web server, database management system, and any additional software dependencies.   * **Operating System:** Choose a suitable operating system that aligns with the platform's requirements. Common choices include Linux distributions (e.g., Ubuntu, CentOS) or Windows Server. * **Web Server:** Install and configure a web server to handle HTTP requests. Popular options include Apache, Nginx, or Microsoft Internet Information Services (IIS). * **Database Management System (DBMS):** Set up a database system to manage and store user data, file metadata, and other relevant information. MySQL, PostgreSQL, or MongoDB are commonly used DBMS options. * **Programming Languages and Frameworks:** Utilize programming languages (e.g., Python, JavaScript) for developing the file-sharing platform's backend and frontend components. * **Security Measures:** Implement security measures such as SSL/TLS certificates for secure data transmission, firewalls, and intrusion detection systems to enhance the platform's resilience against potential threats. |

#### 

# CHAPTER 5

# Proposed System & Implementation

#### 5.Proposed system & Implementation

#### 5.1 Block diagram of proposed system

#### 

#### Fig 5.1.1 User Authentication

#### 

#### Fig 5.1.2 File Download WorkFlow

#### 5.2 Description of block diagram

|  |
| --- |
| The administrator manages user access by adding them to the system and providing encrypted passwords. Users authenticate with these passwords to log in and access files. For downloading files, users must have authentication, ensuring secure access to shared content. This authentication process is a crucial component of the data plan, ensuring that only authorized users can download files, enhancing data security and preventing unauthorized access. By integrating authentication into the data plan, the file-sharing system ensures that users can securely access and download files, fostering a safe and efficient collaboration environment while protecting sensitive information from unauthorized access |

#### 5.3 Implementation

#### 

#### Fig 5.1.3 Login Page.

#### 

#### Fig 5.1.4 Dashboard

#### 

#### Fig 5.1.5 New user page

#### 

#### Fig 5.1.6 User list

#### 

#### Fig 5.1.7 Document list

#### 

#### Fig 5.1.8 View Document

# CHAPTER 6

# Conclusion

**6.Conclusion**

The development of a comprehensive file-sharing platform addresses the critical need for secure and efficient collaboration in modern work environments. By implementing advanced user management functionalities, robust access controls, and intuitive file organization tools, the platform enhances productivity and data security. The project's focus on usability and security ensures a seamless user experience while safeguarding sensitive information. Through careful consideration of hardware and software setups, organizations can deploy a reliable file-sharing solution tailored to their specific requirements. Ultimately, the proposed platform offers a valuable tool for fostering collaboration, streamlining file sharing, and enhancing overall efficiency in today's dynamic work environments

# 

# References

|  |
| --- |
| **Research Papers:**  [1]Kallahalla, Mahesh, Erik Riedel, Ram Swaminathan, Qian Wang, and Kevin Fu. "Plutus: Scalable secure file sharing on untrusted storage." In 2nd USENIX Conference on File and Storage Technologies . 2003  [2**]**Castiglione, A., Catuogno, L., Del Sorbo, A., Fiore, U. and Palmieri, F., 2014. A secure file sharing service for distributed computing environments. The Journal of Supercomputing, 67, pp.691-710  [3]Seeland, Josh, Sarah Elaine Eaton, and Brenda M. Stoesz. "Leveraging college copyright ownership against file-sharing and contract cheating websites." *Contract Cheating in Higher Education: Global Perspectives on Theory, Practice, and Policy*. Cham: Springer International Publishing, 2022. 61-76.  [4]Oberholzer-Gee, Felix, and Koleman Strumpf. "The effect of file sharing on record sales: An empirical analysis." *Journal of political economy* 115.1 (2007): 1-42 |

**URL**

[1]https://www.researchgate.net/publication/123456789/Secure\_File\_Sharing\_Using\_End-to-End\_Encryption\_in\_Web\_Applications

[2] https://www.oreilly.com/library/view/web-development-with/9781491991725/

[3] <https://link.springer.com/chapter/10.1007/978-3-031-12680-2_5>

[4] https://www.journals.uchicago.edu/doi/abs/10.1086/511995