CMSC 626 PRINCIPLES OF COMPUTER SECURITY

PROJECT REPORT

Encrypted and Distributed File System

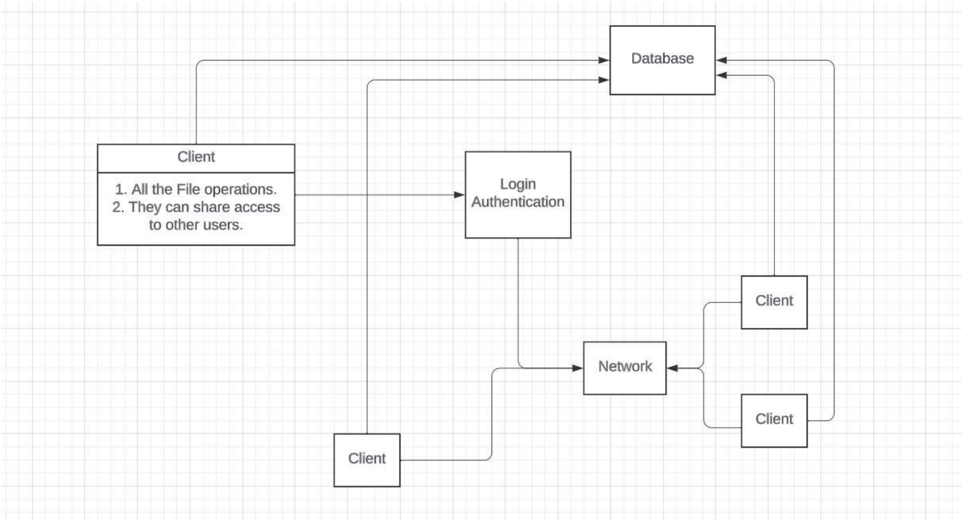
Team 7
Surya Theja Dokka - SL67413
Sathvik Reddy Musku - SX77250
Vishwanth Reddy Jakka - ZJ06092
Lakshmi Vivek Jagabathina - TN20930

ABSTRACT:

The popularity of distributed file systems continues to grow. Reasons they are preferred over traditional centralized file systems include fault tolerance, availability, scalability and performance. In addition, peer-to-peer (P2P) system concepts and scalable functions are being incorporated into the domain of file systems.

INTRODUCTION:

The File System supports the all the file operations that other systems do, like creating, reading, deleting, Updating retrieving files, Etc. The File system encrypts all the data from unauthorized users and attackers, so that only the authorized users are having access to the files. The file access can be shared to other users. Updated data will be visible whenever the user wants to access the files.


Database
Client
1. All the File operations.
2. They can share access to other users.
Login Authentication
Client
Network
Client
Client

FILE SYSTEM DESIGN:

We have used python Programming language for this project for the Peer-to-Peer distributed system which is both secure and encrypted. We have 2 servers so if the main server got failed the backup server will be used for the connection. We have used tkinter GUI toolkit for the good user experience. After running the client.py the user can choose the login or register process. If the user clicks on the Login the login GUI will be coming, on the login the user can give the username and password to login into the system. If the user is new, they can create a new account by clicking on the Create Account, where they need to fill the username, email, password and confirm password. They can even click on the forgot password and enter the new username and password to update the password.

The Connection between the peers and the files are encrypted with AES and base64 Algorithms are used for the encryption and encoding of the data.

Once the User logins they can perform few actions

- Creating Directory.
- Create File.
- Read File
- Delete File.
- Upload File.
- Write File.
- Restore File.
- Available Files.
- Share Access.
- Logs.

1. **Creating Directory:**
    a. This function will allow the user to create a new Directory in the system.
    b. Only the Authorized users can create a directory and will be owner of that directory.
2. **Create File:**
    a. This function will allow the user to create a new file.
    b. The owner will be having the write and delete access to that file.
3. **Read File:**
    a. This Function will allow the user to read the data from the existing file.
    b. The user can only read the file does not update it.

4. **Delete File:**
    a. This Function is used to Delete the File.
    b. The owner of the file can only delete it.
5. **Upload File:**
    a. The user can Upload the file to the file directory.
6. **Write File:**
    a. This Functionality will help the user to write data into a new or existing file.
7. **Restore File:**

    a. This Functionality will help the user to restore the deleted file.

8. **Available File:**
    a. This functionality will allow users to check all the files that user can access.
9. **Share Access:**
    a. The user will be able to share the file to the other users.
10. **Logs:**
    a. This Functionality will help the users to check what all activity are happening on the system on the files.

KEY ARCHITECTURE:

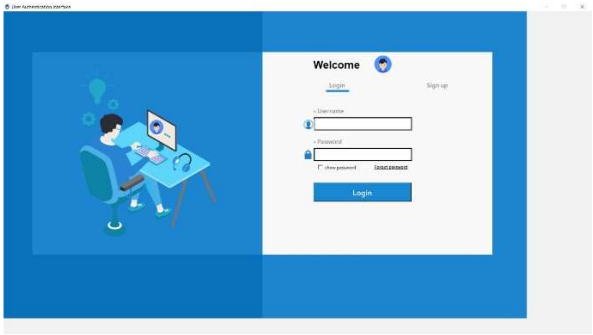
Our main goal is on giving users with access and security. Everything has been encrypted with AES encryption algorithm so that unauthorized users cannot access the system. The users can give access of the files to the other users. The user permissions will determine how the peer grant access to the keys.

IMPLEMENTATION:

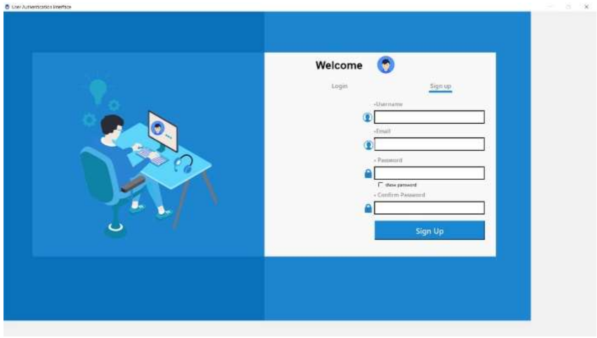
To store the user permissions, we are storing the permissions in MYSQL, where the access_mode is stored. Every time the server starts it will retrieve the data from the files. The peer will continuously monitor the file system to find any malicious activity like creating or deleting the files. When the user selects one of the options from the menu, it performs the operation and simultaneously it sends the operation request to all the peers and the peers will continuously monitor the socket to receive the request from their peers and perform that operation.

EXPIREMENT and RESULTS:

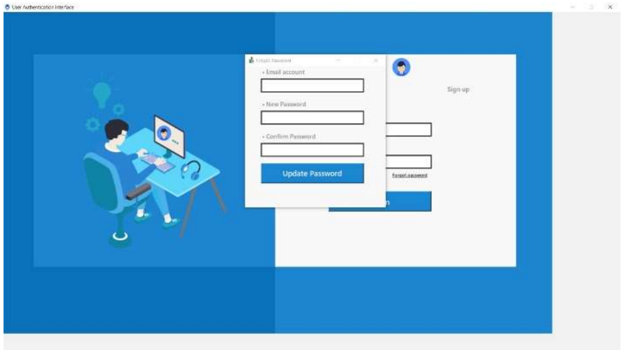
Login Page



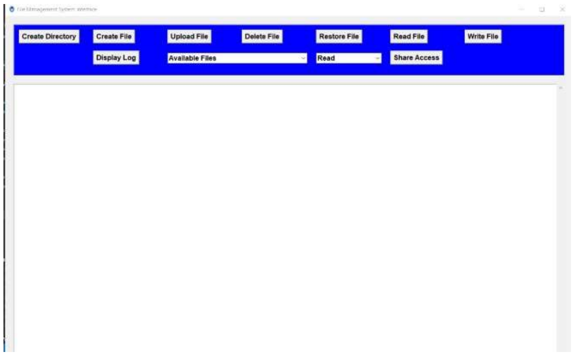
Sign Up Page:



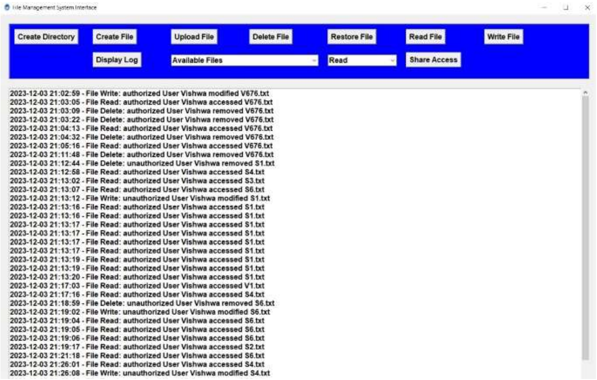
Forgot Password Page:



File Operations Page:

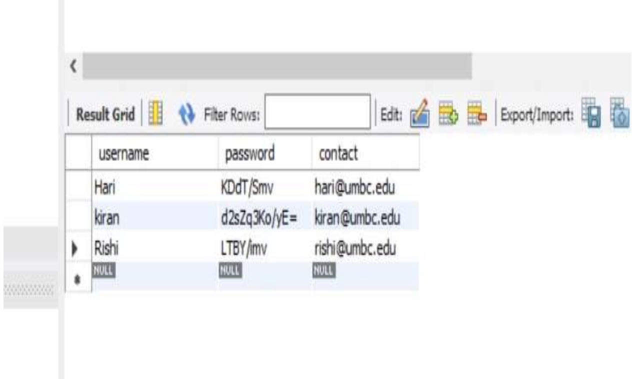


Logs of the Files:



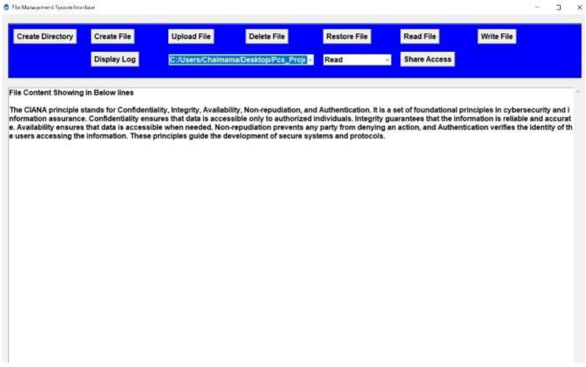
```
2023-12-03 21:02:59 - File Write: authorized User Vishwa modified V676.txt
2023-12-03 21:03:05 - File Read: authorized User Vishwa accessed V676.txt
2023-12-03 21:03:09 - File Delete: authorized User Vishwa removed V676.txt
2023-12-03 21:03:22 - File Delete: authorized User Vishwa removed V676.txt
2023-12-03 21:04:13 - File Read: authorized User Vishwa accessed V676.txt
2023-12-03 21:04:32 - File Delete: authorized User Vishwa removed V676.txt
2023-12-03 21:05:16 - File Read: authorized User Vishwa accessed V676.txt
2023-12-03 21:11:48 - File Delete: authorized User Vishwa removed V676.txt
2023-12-03 21:12:44 - File Delete: unauthorized User Vishwa removed S1.txt
2023-12-03 21:12:58 - File Read: authorized User Vishwa accessed S4.txt
2023-12-03 21:13:02 - File Read: authorized User Vishwa accessed S3.txt
2023-12-03 21:13:07 - File Read: authorized User Vishwa accessed S6.txt
2023-12-03 21:13:12 - File Write: unauthorized User Vishwa modified S1.txt
2023-12-03 21:13:16 - File Read: authorized User Vishwa accessed S1.txt
2023-12-03 21:13:16 - File Read: authorized User Vishwa accessed S1.txt
2023-12-03 21:13:17 - File Read: authorized User Vishwa accessed S1.txt
2023-12-03 21:13:17 - File Read: authorized User Vishwa accessed S1.txt
2023-12-03 21:13:17 - File Read: authorized User Vishwa accessed S1.txt
2023-12-03 21:13:17 - File Read: authorized User Vishwa accessed S1.txt
2023-12-03 21:13:19 - File Read: authorized User Vishwa accessed S1.txt
2023-12-03 21:13:19 - File Read: authorized User Vishwa accessed S1.txt
2023-12-03 21:13:20 - File Read: authorized User Vishwa accessed S1.txt
2023-12-03 21:17:03 - File Read: authorized User Vishwa accessed V1.txt
2023-12-03 21:17:16 - File Read: authorized User Vishwa accessed S4.txt
2023-12-03 21:18:59 - File Delete: unauthorized User Vishwa removed S6.txt
2023-12-03 21:19:02 - File Write: unauthorized User Vishwa modified S6.txt
2023-12-03 21:19:04 - File Read: authorized User Vishwa accessed S6.txt
2023-12-03 21:19:05 - File Read: authorized User Vishwa accessed S6.txt
2023-12-03 21:19:06 - File Read: authorized User Vishwa accessed S6.txt
2023-12-03 21:19:17 - File Read: authorized User Vishwa accessed S2.txt
2023-12-03 21:21:18 - File Read: authorized User Vishwa accessed S6.txt
2023-12-03 21:26:01 - File Read: authorized User Vishwa accessed S4.txt
2023-12-03 21:26:08 - File Write: unauthorized User Vishwa modified S4.txt
```

Password stored in cipher text.



username	password	contact
Hari	KDdT/Smv	hari@umbc.edu
kiran	d2sZq3Ko/yE=	kiran@umbc.edu
Rishi	LTBY/imv	rishi@umbc.edu
NULL	NULL	NULL

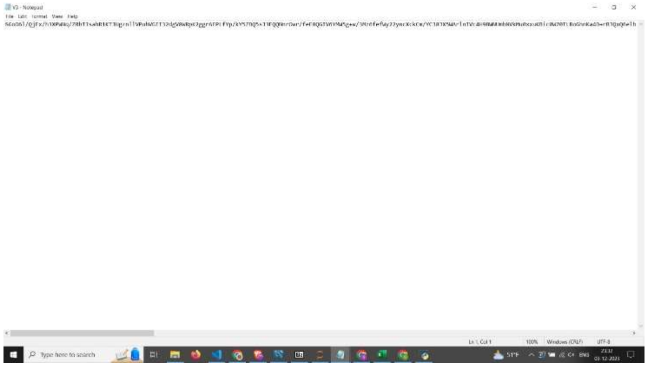
File Data



File Content Showing in Below lines

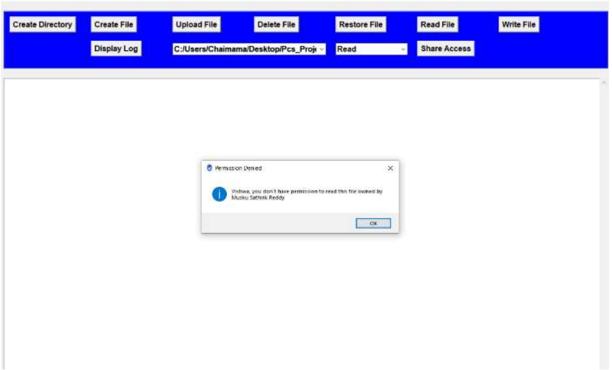
The CIANA principle stands for Confidentiality, Integrity, Availability, Non-repudiation, and Authentication. It is a set of foundational principles in cybersecurity and information assurance. Confidentiality ensures that data is accessible only to authorized individuals. Integrity guarantees that the information is reliable and accurate. Availability ensures that data is accessible when needed. Non-repudiation prevents any party from denying an action, and Authentication verifies the identity of the users accessing the information. These principles guide the development of secure systems and protocols.

Encrypted File Data



[illegible]

Access is denied if the user is accessing others data without permission



C:/Users/Chaimama/Desktop/Pcs_Proj

Read

Permission Denied

Vishwa, you don't have permission to read this file owned by Musku Sathvik Reddy

CONCLUSION:

The main idea of our project is to provide users a safe and secure way to access files. We have Developed a Peer-to-Peer Encrypted file system by using the python language. The File system has a security as there will be user authentication and encryption. The Encryption Algorithms will help in preventing the attackers from unauthorized users.

REFERENCES:

[1] Robert Tracey, Mobayode O. Akinsolu, Vadim Elisseev “pyp2pcluster: A cluster discovery tool”

[2] J. Sen, "Peer-to-peer networks," 2012 3rd National Conference on Emerging Trends and Applications in Computer Science, Shillong, 2012, pp.

GitHub Link:

https://github.com/Msathvik007/PCS_PROJECT_TEAM7