OOAD MINI PROJECT SYNOPSIS

TITLE: SECURE FILE SHARING SYSTEM

Team Members:

PES1UG20CS583: S NIHARIKA

PES1UG20CS588: SAHANA RAO

PES1UG20CS591: SHREYA

ABSTRACT

The aim of the project is to build an end-to-end secure file sharing system which mimics the P2P architecture. Files are securely shared via a room which is created by the client through Advanced encryption algorithm. The invite link of the sharing platform which in this case is a room is created for the peers who want to access and download files. The link has to be submitted by each peer to join the network to send or receive the files.

.

INTRODUCTION

The secure file sharing system is an advanced solution that uses Advanced encryption algorithms and secure communication protocols to safeguard files against unauthorized access. The system ensures that files are shared only with authorized parties and are protected from any breaches or attacks.

On the sender side the file is encrypted using the secret key before sending the file. The encrypted files are decrypted on the receiving end using the secret key available in the room to validate the file. After the decryption the file is

downloaded on the receiving end. In order to account for the file not being corrupted, the concept of checksum is used to verify the integrity of the file. The encrypted file here is being sent to the peers in the room using different sockets in the local system presently.

All the files being sent/transmitted in the room are stored in the mongodb database for future reference of the ongoing session. Each user is assigned a database to keep track of his files used in the session

MOTIVATION

To address the growing concerns about the security of online data sharing. With the increasing reliance on digital communication and the sharing of sensitive information online, there is a growing need for secure and reliable methods of file sharing.

Existing file sharing solutions are often limited in their security features, leaving them vulnerable to cyber threats such as data breaches, hacking, and identity theft.

WHY THIS PROJECT?

Protects Sensitive Information: A secure file sharing system ensures that sensitive information, such as personal or financial data, intellectual property, or confidential business information, is protected from unauthorized access or data breaches.

Control: With a secure file sharing system, users have more control over the information they share, who they share it with, and how it is accessed. This allows organizations to implement access controls and permission levels, ensuring that files are only accessed by authorized parties.

OBJECTIVES AND GOALS

1. Develop a secure and reliable file sharing system that utilizes advanced encryption algorithms, user authentication, access control to ensure the confidentiality, integrity, and availability of shared files.

2. Provide a user-friendly experience that enables users to easily and securely share files with authorized parties.

3. Implement access controls and permission levels that allow organizations to control who can access and share files, and provide detailed logs and audit trails of file access and sharing activity.

4. Provides user control where user can control over the information they share and who they share it with

BACKGROUND:

Secure file sharing is an essential aspect of modern-day communication and collaboration. With the increasing reliance on digital communication, there is a growing need for secure file sharing tools that enable users to exchange information safely and efficiently. Secure file sharing tools ensure that files are transmitted and stored securely, protecting them from unauthorized access and theft.

TOOLS and PLATFORM

HARDWARE REQUIREMENTS:

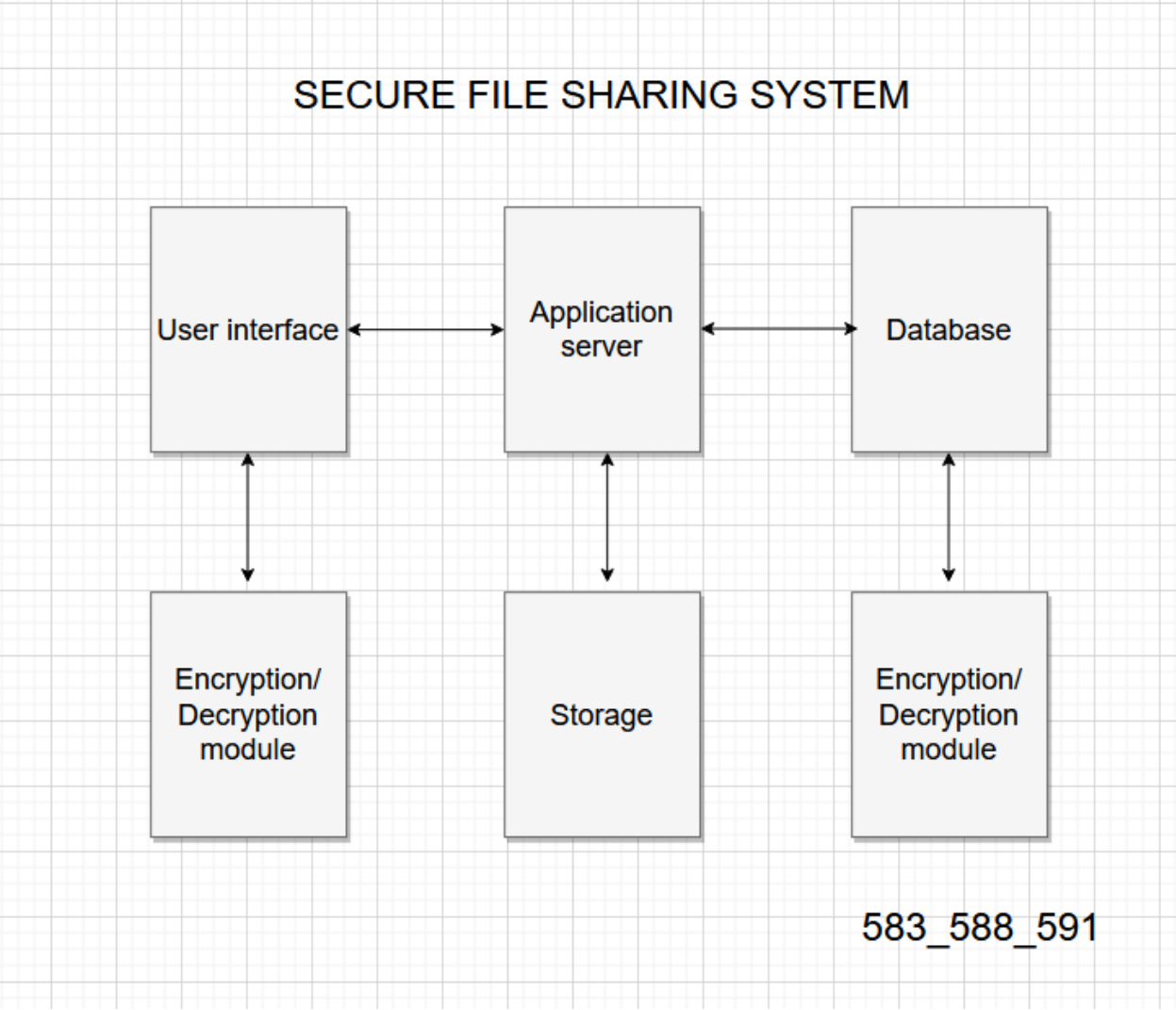
1. Computer
2. Storage

3. Internet Connectivity
4. Peripheral devices

SOFTWARE PLATFORMS:

1. Java Development Kit (JDK)
2. Integrated Development Environment
3. Java Cryptography Extension (JCE)
4. Web Application Server

BLOCK DIAGRAM:



APPLICATIONS:

Domains such as healthcare, finance and government

1. Collaboration: To collaborate on projects and share files with team members securely.
2. Document management: Secure file sharing systems can be used for document management, where users can store and manage sensitive documents securely.
3. Backup and disaster recovery: Secure file sharing systems can be used to back up important files and data and restore them in case of a disaster.

FUTURE SCOPE:

Advancements in encryption technologies and cloud computing such as,

1. Blockchain based secure file sharing: using Blockchain technology to provide high levels of security and data integrity
2. Artificial intelligence-based security: AI based security systems that can detect and prevent security breaches in real time