**A PEER-TO-PEER DISTRIBUTED ENCRYPTED FILE SYSTEM**

*CMSC 626 – PRINCIPLES OF COMPUTER SECURITY*

**CONTENTS**

1. ABSTRACT
2. PURPOSE OF A DISTRIBUTED FILE SYSTEM
3. WORKING OF A DISTRIBUTED FILE SYSTEM
4. REQUEST FLOWS
   1. Single Request Flow
   2. Multiple Request Flow
5. ENCRYPTION
6. PERMISSION MANAGEMENT SYSTEM
7. UML DIAGRAM
8. PLAN OF ACTION
9. REFERENCES

**TEAM – 03**

Anjani Lingamallu

Varunpal Gopidi DW89091 [vgopidi1@umbc.edu](mailto:vgopidi1@umbc.edu)

Seetaram Oruganti QL21570 [seetaro1@umbc.edu](mailto:seetaro1@umbc.edu)

Sai Teja Challa JA52979 [*schalla4@umbc.edu*](mailto:schalla4@umbc.edu)

Kavya Vellanki PI66332 [*kavyapv1@umbc.edu*](mailto:kavyapv1@umbc.edu)

***Under the guidance of,***

***Professor***

Gerald S. Tompkins

***Teaching Assistant***

Ran Liu

* + 1. **ABSTRACT:**

Modern digital communication needs advanced file-sharing services that prioritize privacy and integrity. This project presents a P2P distributed file system that allows users to store and transfer files on untrusted remote servers. This file system is intended to assure user confidentiality, data integrity, and real-time access to the most recent version of files. By adding advanced security mechanisms, permission-based user roles, encrypted communications, and an integrated log mechanism to detect malicious activity, we hope to overcome traditional P2P restrictions. The goal of this project is to develop the next phase of the P2P file system that combines the efficiency of distributed networks with enhanced security features. Our solution focuses on user privacy, data integrity, and system stability, resulting in a platform that is streamlined, secure, and user-friendly for all file storage and sharing requirements.

* + 1. **MOTIVATION:**

A notable motivation for adopting P2P DFS is its inherent scalability, as it can easily scale without the need for reconfiguration. In a P2P distributed file system data is stored across multiple nodes, even if one node goes offline, the data can be accessed from remaining nodes. The files in this distributed system are encrypted using encryption techniques, hence these are always secure. When a client sends many requests, the jobs are distributed among multiple servers, and the system improves performance by reducing the workload on a single server. Thus, P2P DFS provides a robust environment for developing a secure file-sharing system.

* + 1. **WORKING OF P2P FILE SYSTEM:**

A distributed file system is a collection of systems also called peers that are connected

to other peers to share files and resources. Here every peer act as both client and server,

sharing Their resources within the network. We should make sure all the users can see and

are getting the most updated version of documents and able to create, write, read, and delete

files.

-----

Diagram

---------

There will be special permissions and access restrictions to users for security purposes' grants permissions to users by allowing or preventing a user from unauthorized access. A user can share a file with other users in the P2P Distributed File System network by adding it to their local file system. The user's P2P Distributed File System client software breaks down the file into smaller segments and encrypts them as a security measure against unauthorized access. Afterward, the client program disperses these file segments among different nodes within the network. Other nodes on the network can request specific file portions from these distributed nodes, enabling them to reconstruct the complete file on their respective systems.

**5)** **ENCRYPTION:**

Encryption is to be implemented to secure the data while communication or file sharing in the file system. We will be implementing the RSA algorithm as it is asymmetric and through that we could achieve both Confidentiality and Integrity with the help of digital signatures. The RSA algorithm would be the best choice for implementing a basic encrypted file system.