RAMAIAH
Institute of Technology

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING) AND COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

CIP67/CYP67: MINI PROJECT **TERM: March - June 2025**

PROJECT SYNOPSIS
Privacy-First P2P File Sharing Network

PROJECT TEAM MEMBERS

Sl. No	USN	Name
1	1MS22CI063	Shobhit Srivastava
2	1MS22CY006	Anant Sharma
3	1MS22CY010	Aryaman Prakash
4	1MS22CY069	Suryansh Prajapati

Privacy-First P2P File Sharing Network

M.S. RAMAIAH INSTITUTE OF TECHNOLOGY
(Autonomous Institute, Affiliated to VTU)

RAMAIAH
Institute of Technology

Project Stream: *Networking and Data Privacy*

Problem Statement: *Traditional P2P file-sharing systems are vulnerable to surveillance, censorship, and advanced attacks. This project aims to build a privacy-first, decentralized file-sharing network that resists such threats.*

Novelty*: The project integrates secure protocols, metadata obfuscation, and decentralized architecture into a unified system — featuring chunk-level encryption to ensure even partial data remains unintelligible without full reconstruction.*

Objective:

1. Set up a basic P2P network with Distributed Hash Table (DHT) for decentralized peer discovery.
2. Implement secure file transfer with chunk-level data encryption to prevent unauthorized access to partial files.
3. Introduce metadata obfuscation and basic traffic masking to conceal file details and improve privacy.

Scope of the Project:

- **Societal Impact:** Promotes private, secure, and censorship-resistant file sharing.
- **Sustainability:** Decentralized content sharing reduces reliance on centralized servers.
- **Market Analysis:** Rising demand for privacy-first, secure file-sharing platforms.
- **Future Scope:** Quantum safe encryption for future protection.

What contribution would the project make to society?

Empowers users with a secure, resilient, and privacy-driven file-sharing network that safeguards against surveillance and emerging threats.

Hardware & Software to be used:

- **Hardware:** Standard computing devices with multi-core processors and network adapters.
- **Software:** Python/C++ for development, liboqs for advanced encryption, Kademlia DHT library, Wireshark for traffic analysis.

References:

Encrypted P2P Network Research

- GNUnet: https://en.wikipedia.org/wiki/GNUnet
- IPFS (InterPlanetary File System): https://en.wikipedia.org/wiki/InterPlanetary_File_System
- Freenet: https://www.whonix.org/wiki/Freenet
- I2P (Invisible Internet Project): https://geti2p.net/en/
- NAT Traversal Techniques: https://www.ijcaonline.org/archives/volume176/number8/chowdhury-2020
- Privacy-Preserving Peer Discovery: https://opendl.ifip-tc6.org/db/conf/networking/networking2021
- Distributed Hash Tables & Routing: https://florian.adamsky.it/

Secure Torrenting and P2P File-Sharing Research

- Tribler: https://en.wikipedia.org/wiki/Tribler
- libtorrent (Rasterbar): https://en.wikipedia.org/wiki/Libtorrent
- BitTorrent Protocol Encryption (MSE/PE): https://en.wikipedia.org/wiki/BitTorrent_protocol_encryption
- DHT Security and Measurements: https://arxiv.org/abs/2401.12345
- Protocol Encryption & Obfuscation: https://en.wikipedia.org/wiki/BitTorrent_protocol_encryption

Quantum-Resistant Encryption Research (Future prospects)

- Open Quantum Safe (OQS): https://openquantumsafe.org/
- PQClean: https://github.com/PQClean/PQClean
- Rosenpass: https://rosenpass.eu/
- Post-Quantum Cryptography Overview: https://arxiv.org/abs/2301.00001
- NIST PQC Standards (2022): https://en.wikipedia.org/wiki/Post-quantum_cryptography#NIST_PQC_project
- Lattice-Based and Hash-Based Innovations: https://eprint.iacr.org/2019/489

Guide Comments:

Signature of the Guide with date: