

# Security and Challenges in Peer-To-Peer File Sharing

Dinh Vu Anh

December 2024

## 1 Overview

Peer-to-peer (P2P) file sharing has revolutionized the way data is distributed by enabling direct file transfers between users without reliance on central servers. However, the decentralized nature of P2P networks also presents significant security risks and operational challenges.

Security concerns include data corruption, malware distribution, and privacy risks due to unencrypted exchanges. Operationally, P2P networks face bandwidth strain, network instability, and difficulties in scaling effectively. They are also often associated with legal and ethical issues like copyright infringement.

## 2 Security Issues in Peer-To-Peer File Sharing

- **Malware, Spyware and Viruses:** Since P2P networks allow direct sharing between users, files shared within the network may contain malware or viruses. These types of malicious software can cause all sorts of havoc, including bringing down your entire network.
- **Data Integrity and Corruption:** Without a central authority to validate files, there is a risk of data corruption or unauthorized alterations. Users may unknowingly download corrupted files or altered versions of original files.
- **Privacy Risks:** Many P2P systems lack encryption for the files being exchanged. This exposes sensitive data to potential eavesdropping or interception. Users may unknowingly share personal or confidential information if the network is not adequately protected.
- **Insecurity File Transfer:** In some cases, P2P users may not be fully anonymous. IP addresses and activity logs can be traced back to users, leading to privacy breaches and potential legal consequences.

### 3 Operational Challenges

- **Network Instability:** P2P networks often rely on user nodes that may join or leave at any time, causing fluctuations in the network's availability and reliability. This can affect the quality and speed of file sharing.
- **Scalability:** As the network grows in size, managing the increasing number of peers and ensuring efficient file distribution becomes more difficult. P2P systems may face issues in scaling efficiently, leading to slower file sharing and connectivity problems.
- **Bandwidth Strain:** P2P networks often require users to share their internet bandwidth, which can lead to congestion and slow speeds, especially for users with limited bandwidth. This could affect the overall user experience.
- **Legal and Ethical Issues:** P2P networks are often used for sharing copyrighted content without authorization, leading to legal challenges. Copyright infringement lawsuits and ethical debates about file sharing in the context of intellectual property can complicate the use of P2P systems.

### 4 Solutions and Mitigations

- **Encryption and Secure Protocols:** Implementing encryption at both the file and transport levels can mitigate the risks of data interception and malware. Protocols like TLS or SSL can be used to ensure the privacy and integrity of file transfers.
- **Authentication and Trust Models:** Introducing methods of verifying the identity of peers, such as digital signatures or reputation systems, can help prevent malicious actors from exploiting the network. Users can be rated or verified, increasing trust in the file-sharing process.
- **Legal Compliance and Content Filtering:** To avoid legal issues, some P2P networks implement content filtering and compliance with copyright laws, preventing the sharing of pirated content. This approach can help protect users from lawsuits and reduce the legal risk associated with file sharing.
- **Improved Network Protocols:** Enhancing network protocols to handle dynamic nodes more effectively and ensure more reliable peer discovery and file retrieval is crucial for overcoming scalability and stability challenges.

### 5 References

1. Caplinked: How save is Peer-To-Peer File Sharing

2. CUHK-Information Technology Services Centre: Risk in Peer-To-Peer File Sharing
3. SecureDocs: Peer-To-Peer (P2P) File Sharing Risks