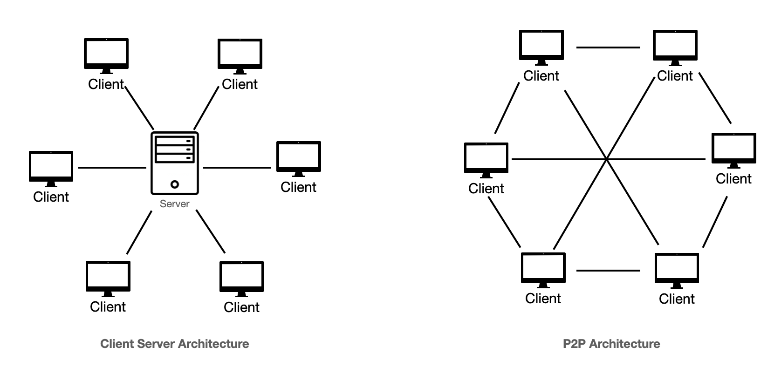
*Eitan Coronel 315468132*

*Elyashiv Newman 206387177*

1. **Explain the problem space**:

Our project addresses privacy concerns in peer-to-peer (P2P) file-sharing networks. In traditional P2P systems, users share and download file segments across a decentralized network where each peer acts as both a client and a server. Files are split into chunks, and peers download these chunks from multiple sources simultaneously, often with the help of a Distributed Hash Table (DHT) that tracks file availability.



As we can see in this picture, the P2P network (right) differs significantly from a traditional client-server network (left). In a client-server model, all clients connect to a centralized server to download or upload data. This means that the server is the sole distributor of files, creating a potential bottleneck and single point of failure. In contrast, in a P2P network, all peers communicate and exchange data directly with each other without relying on a central server. Each peer can download file chunks from multiple other peers, increasing efficiency and resilience.

While this decentralized approach makes file sharing faster and more robust, it also exposes users to privacy risks, as adversaries can observe network traffic and track which files or file segments are being requested and downloaded by specific peers.

1. **Motivate the importance of the problem you’re targeting:**

The need for privacy in digital communication and file-sharing is critical in today's data-driven world. P2P networks are widely used for various applications, including money transfers (through cryptocurrencies like Bitcoin), sharing large files via platforms like BitTorrent, and even use to power streaming services such as Spotify (which previously used P2P technology to distribute music).  
However, without privacy protections, users in these networks are vulnerable to surveillance and tracking by malicious actors. This exposure allows adversaries to monitor and analyse which files users are downloading, which could lead to potential risks, especially in regions where internet usage is closely monitored, or for users accessing politically sensitive or copyrighted content. The ability to observe user behaviour in P2P networks can result in privacy breaches, data mining, or even legal consequences for individuals who unintentionally expose their downloading activity to the public or adversaries.  
The significance of this project can be encapsulated by Stewart Baker’s statement: “metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content.”

1. **Describe your solution and how it compares to the state of the art:**
   1. **What is the attacker model? What assumptions does it make?**

In our project, the attacker model assumes that adversaries can monitor network traffic within the peer-to-peer (P2P) network. These adversaries could be other peers in the network, a network observer, or a malicious entity with access to the P2P communications. The goal of the attacker is to track and infer which files a particular user is downloading or uploading. The attacker is considered to have the capability to observe all communications between peers, including the frequency, size, and timing of the data packets exchanged. This allows the attacker to identify patterns and potentially deduce which files or file segments are being requested, even if the content itself is encrypted.

The model assumes that while the attacker cannot decrypt encrypted data, they can still see the encrypted packets being exchanged, giving them visibility into communication patterns. Additionally, the attacker could be strategically positioned within the network to correlate requests over time, making it easier to identify consistent downloaders of particular files or content.

Their overall aim is to use this gathered information to profile users, determine their download behaviours, or even attempt to uncover sensitive information based on their observed activity.

* 1. **Motivate your design given the attacker model:**

1. **Evaluate your solution**