In a typical file-sharing application, the supported file types for upload and download can vary depending on the system's design and implementation. Common file types that we are going to developed include:

1. Documents: .pdf, .docx, .xlsx, .pptx, .txt
2. Images: .jpg, .png, .gif
3. Audio: .mp3, .wav
4. Video: .mp4, .mov, .avi
5. Compressed files: .zip, .rar

The maximum file size limits can also vary depending on the system's configuration and requirements. It is common for file-sharing applications to set a maximum file size to ensure efficient storage and transfer. Typical limits can range from a few megabytes (MB) to several gigabytes (GB).

Regarding security requirements, some common practices for file-sharing applications include:

1. Virus Scanning: Implementing a virus scanning mechanism to scan uploaded files for malware or viruses to prevent the spread of malicious content.
2. File Encryption: Encrypting files during storage and transmission to protect sensitive information and prevent unauthorized access.
3. Access Control: Implementing user authentication and authorization mechanisms to ensure that only authorized individuals can upload, download, and access files.
4. Data Privacy: Ensuring compliance with data privacy regulations and implementing measures to protect user data and maintain confidentiality.
5. Secure Storage: Storing files in secure storage systems, such as encrypted databases or file servers, to prevent unauthorized access or data breaches.