xyz 云盘系统
设计文档

	人员	日期
拟制	宋小牛 陈泳舟 金泽文	2018-05-20
评审人	•	yyyy-mm-dd
批准	•	yyyy-mm-dd
签发	•	yyyy-mm-dd

摘　要

本文档是 xyz 云盘系统需求规格分析文档，由宋小牛、陈泳州和金泽文共同创建，

本文档主要分析了该软件的任务概述、总体设计、接口设计、数据结构设计、数据库设计、界面设计、出错处理设计和安全保密设计、维护设计、等关于软件多个方面的设计。

关键词：云盘　分布式存储　文件共享　版本更新　网络　隐私　安全　p2p　存储冗余　内容审核　数据结构　算法

表 1　缩略词清单

缩略语	英文全名	中文解释
CentOS	Community Enterprise Operating Syste	社区事业版操作系统
CSS	Cascading Style Sheets	层叠样式表
HTML	HyperText Markup Language	超文本标记语言
HTTP	HyperText Transfer Protocol	超文本传输协议
HTTPS	Hypertext Transfer Protocol Secure	超文本传输安全协议
IOPS	Input/Output Operations Per Second	每秒读写操作的次数
IP	Internet Protocol	网际协议
MD5	Message-Digest Algorithm 5	讯息摘要演算法 5
TCP	Transmission Control Protocol	传输控制协议

目　录

图目录

表目录

第 1 章　引言

1.1　编写目的

在本项目的前一阶段，也就是需求分析阶段，已经将系统用户对本系统的需求做了详细的阐述，这些用户需求已经在上一阶段中对不同用户所提出的不同功能，实现的各种效果做了调研工作，并在需求规格说明书中得到详尽得叙述及阐明。

本阶段已在系统的需求分析的基础上，对 xyz 云盘系统进行设计。主要解决了实现该系统需求的程序模块设计问题。包括如何把该系统划分成若干个模块、决定各个模块之间的接口、模块之间传递的信息，以及数据结构、模块结构的设计等。在以下的概要设计报告中将对在本阶段中对系统所做的所有概要设计进行详细的说明，在设计过程中起到了提纲挈领的作用。

在下一阶段的详细设计中，程序设计员可参考此概要设计报告，在概要设计即时聊天工具所做的模块结构设计的基础上，对系统进行详细设计。在以后的软件测试以及软件维护阶段也可参考此说明书，以便于了解在概要设计过程中所完成的各模块设计结构，或在修改时找出在本阶段设计的不足或错误。

1.2　项目背景

随着互联网技术的飞速发展以及广泛应用，云计算这一技术也随之普及。云存储，是近几年在云计算的发展潮流之中诞生的，一项新兴的网络存储技术。云存储集成了网络技术和分布式文件系统等功能，是通过对不同的物理存储设备进行虚拟化映射，以形成逻辑层面统一的大存储空间的应用。

云盘系统，就是利用云存储技术，面向广大的有存储需求的客户，提供数据文件存储服务的第三方托管系统。

我们的 xyz 云盘系统，是基于分布式文件系统来设计和开发的云盘系统，是一个独立的项目。它的命名来自三位开发者名字的首字母（Xiaoniu，Yongzhou，Zewen），表明这将是由三位开发者开发的完全不同于其他云盘系统的新兴的云盘系统。

1.3 术语

表 1.1 术语表

缩写、术语	解释
CentOS	Community Enterprise Operating Syste , 社区事业版操作系统
CSS	Cascading Style Sheets , 层叠样式表
HTML	HyperText Markup Language , 超文本标记语言
HTTP	HyperText Transfer Protocol , 超文本传输协议
HTTPS	Hypertext Transfer Protocol Secure , 超文本传输安全协议
IOPS	Input/Output Operations Per Second , 每秒读写操作的次数
IP	Internet Protocol , 网际协议
MD5	Message-Digest Algorithm 5 , 讯息摘要演算法 5
TCP	Transmission Control Protocol , 传输控制协议

第 2 章　任务概述

本系统的目标是实现一个 xyz 云盘系统，包括客户端、服务器端两个部分。

客户端面向 xyz 云盘用户，为用户提供 p2p 下载、上传、分享、加密、在线解压缩等服务。

2.1　目标

实现 xyz 云盘系统，实现需求规格说明书中所描述的 p2p 下载、上传、分享、备份、加密、审核、在线解压缩和预览等功能，并且保证系统的健壮性、高可用性和数据安全。

2.2　开发与运行环境

2.2.1　开发环境的配置

如表 2.1 开发环境的配置所示。

2.2.2　测试环境的配置

如表 2.2 测试环境的配置所示。

2.2.3　运行环境的配置

如表 2.3 运行环境的配置所示。

2.3　需求概述

功能需求包括:

用户的注册、登陆、退出、忘记密码。

文件的上传、下载、重命名、移动、加密、分享、搜索、在线解压缩、审核、共享文件夹等。

2.4　条件与限制

为了完成这个项目，xyz 云盘系统的的开发应该在以下条件下展开:

表 2.1　开发环境的配置

类别	标准配置	最低配置
计算机硬件	基于 x86 结构的 CPU 内存 >=8G 硬盘 >=250G 主频 >=2.4GHz 网络带宽 >=100MBps	基于 x86 结构的 CPU 内存 >=4G 硬盘 >= 100G 主频 >=1.0GHz 网络带宽 >=10MBps
计算机软件	服务器端:CentOS (version>=7.4) 客户端:Win10(version>=1709)	服务器端:CentOS (version>=7.1) 客户端:Win10(version>=1703)
其他	Java HotSpot VM 18.3 Tomcat (version>=9) Mysql(version>=5.7) Google Chrome(version>=61) 等浏览器 Ceph(version>=12.2)	Java HotSpot VM 18.3 Tomcat (version>=9) Mysql(version>=5.6) Google Chrome(version>=61) 等浏览器 Ceph(version>=12.0)

• 开发者掌握足够的开发 xyz 云盘系统的能力，比如前后端代码编写的能力、UI 设计的能力、与客户进行有效沟通的能力等。

• 开发者掌握足够的需要开发 xyz 云盘系统的软硬件环境配置，尤其是开发过程中的软硬件资源、以及运行时的足够的服务器资源。

• 开发者有足够的精力与时间进行 xyz 云盘系统的开发。

• 开发者能够负责后续的项目更新、bug 修复等事宜。

同时，xyz 云盘系统的开发具有如下的限制因素：

• 硬件资源：开发者没有足够的经费以维持足够的服务器硬件开销，尤其是庞大的硬盘开销以及网络带宽开销。

• 开发经验：开发者没有足够的相关应用的开发经验。

• 人力资源：没有足够的人员数量以及开发的时间精力。

• 用户隐私：xyz 云盘系统为了在中国能够合法的运营下去，必须遵守中国的相关法律规定，包括存储必要的用户数据以允许相关部门的合法审查，而这必然会限制用户隐私的绝对保护。

• 安全性依赖：xyz 云盘系统依赖于 Windows、Java、CentOS、Mysql、Ceph、Tomcat、Chrome 等多个第三方开源产品，所以其安全性受到这些第三方产品的

表 2.2　测试环境的配置

类别	标准配置	最低配置
计算机硬件 (服务器端)	内存 >=8G 硬盘 >=250G 主频 >=2.4GHz 网络带宽 >=1GBps	内存 >=4G 硬盘 >= 100G 主频 >=1.0GHz 网络带宽 >=10MBps
计算机硬件 (客户端)	内存 >=2G 硬盘剩余空间 >=1G 主频 >=2.4GHz 网络带宽 >=100MBps	内存 >=1G 硬盘剩余空间 >= 100M 主频 >=1.0GHz 网络带宽 >=10MBps
计算机软件	服务器端:CentOS (version>=7.4) 客户端:Win10(version>=1709)	服务器端:CentOS (version>=7.1) 客户端:Win10(version>=1703)
其他	Java HotSpot VM 18.3 Tomcat (version>=9) Mysql(version>=5.7) Google Chrome(version>=61) 等浏览器 Ceph(version>=12.2)	Java HotSpot VM 18.3 Tomcat (version>=9) Mysql(version>=5.6) Google Chrome(version>=61) 等浏览器 Ceph(version>=12.0)

表 2.3　运行环境的配置

类别	标准配置	最低配置
计算机硬件 (服务器端)	内存 >=8G 硬盘 >=250G 主频 >=2.4GHz 网络带宽 >=1GBps	内存 >=4G 硬盘 >= 100G 主频 >=1.0GHz 网络带宽 >=10MBps
计算机硬件 (客户端)	内存 >=2G 硬盘剩余空间 >=1G 主频 >=2.4GHz 网络带宽 >=100MBps	内存 >=1G 硬盘剩余空间 >= 100M 主频 >=1.0GHz 网络带宽 >=500KBps
计算机软件	服务器端:CentOS (version>=7.4) 客户端:Win10(version>=1709)	服务器端:CentOS (version>=7.1) 客户端:Win10(version>=1703)
其他	Java HotSpot VM 18.3 Tomcat (version>=9) Mysql(version>=5.7) Google Chrome(version>=61) 等浏览器 Ceph(version>=12.2)	Java HotSpot VM 18.3 Tomcat (version>=9) Mysql(version>=5.6) Google Chrome(version>=61) 等浏览器 Ceph(version>=12.0)

限制。

• 性能依赖：xyz 云盘系统由于是网盘软件，所以其下载、上传等功能会极大地受到用户自身硬件资源等的限制，所以性能与用户硬件的相关性极大。

• 浏览器依赖：xyz 云盘系统的客户端部署在用户的浏览器中，所以根据浏览器对 Http、Https 等协议的实现不同，其兼容性可能也会有些许偏差。

第 3 章　总体设计

3.1　软件描述

系统包括前台和后台两个部分。

前台主要功能是：初始化界面的显示、关操作的请求（如输入用户名密码等）、用户的文件相关操作的请求（如选中文件并上传、下载、分享等操作）的控制信息的发送以及数据文件的发送、用户操作的结果显示等。

后台主要功能是：处理用户的输入，判断其权限、其操作是否合法；对于相应的文件操作，进行相应的判断与处理，比如：对于上传以及分享的文件，进行内容审核处理；对文件进行存储冗余处理；并且将处理结果 (包括操作的结果以及下载操作对应的数据文件的发送等) 返回到客户端。

3.2　处理流程

3.2.1　总体流程

总体流程图如图 3.1 所示。总体上来说，客户端将用户的请求通过网络发送到服务器端，服务器端对该请求进行检查，审核等处理之后，再执行相关操作，并最终将操作的结果返回到客户端。

3.2.2　系统基本流程

系统基本流程如图 3.2 所示。

3.2.3　客户端基本流程

客户端基本流程如图 3.3 所示。

3.2.4　服务器端基本流程

服务器端基本流程如图 3.4 所示。

3.2.5　功能 1-用户登录的具体流程

用户在初始登录界面输入用户名和密码。

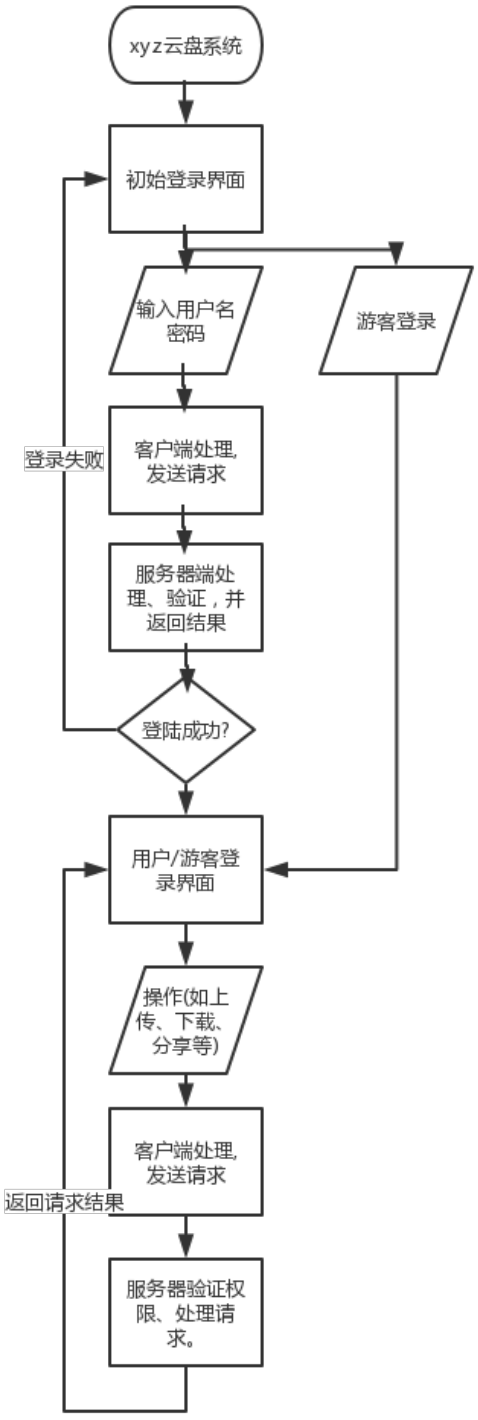

图 3.1　总体流程图

在点击登录按钮之后，客户端检测用户名和密码的长度以及字符是否符合要求，如果不合法则弹出“用户名和密码违法”的界面；否则客户端将用户名和密码结合时间戳进行密码学处理并发送到服务器端。

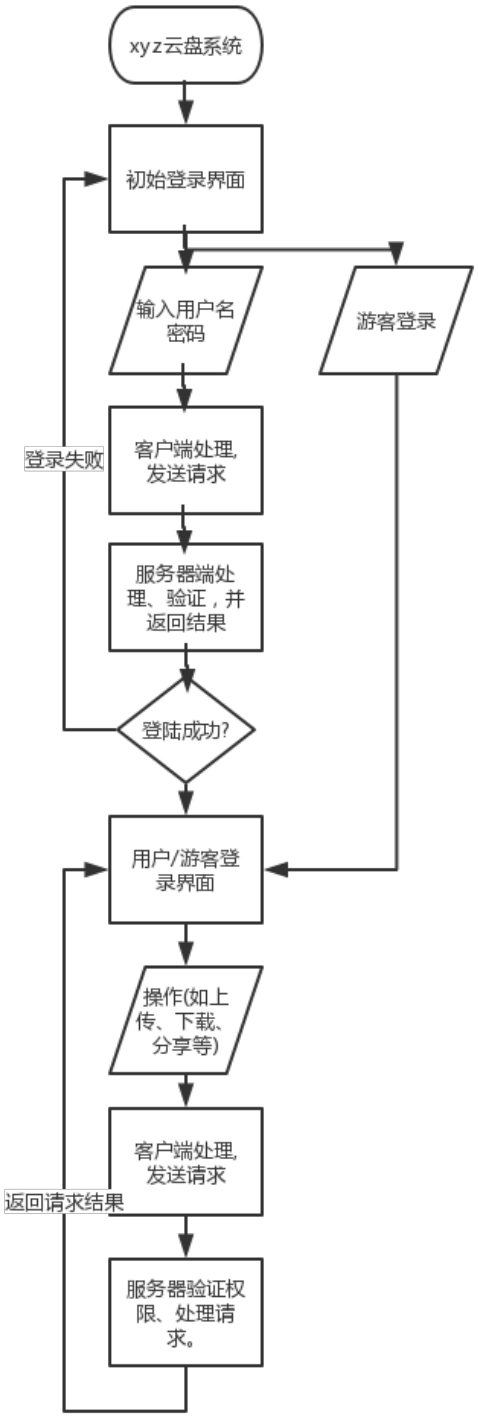

图 3.2　系统基本流程图

服务器端通过密码学处理比对数据库中的用户信息，如果密码正确，返回带有时间戳的 cookie 给客户端。

客户端收到之后, 如果密码正确，生成 HTML 页面，显示用户的根文件夹；

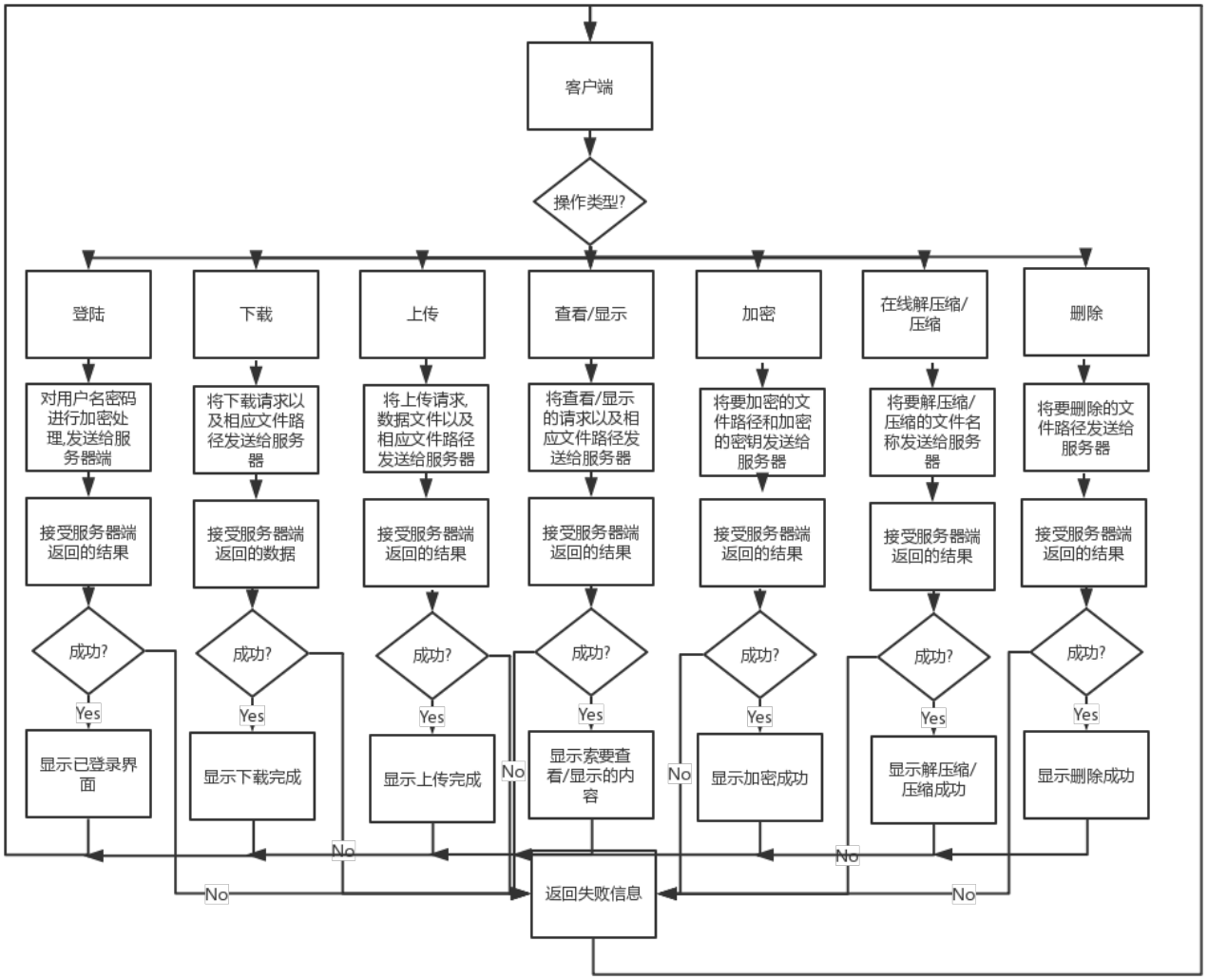

图 3.3　客户端基本流程图

如果密码错误，生成 HTML 页面，显示“密码错误”，以及错误次数，进行警告。

3.2.6　功能 2-用户注册的具体流程

在看到登陆界面之后，用户可以点击“注册”键。客户端生成 HTML 页面，跳转到注册页面。之后在新的页面中用户输入用户名和绑定邮箱以及密码，点击“确认”键。

客户端检查用户名密码的字符以及长度是否符合要求，如果不符合要求，则生成 HTML 页面，提示“不符合要求”；否则将用户名密码以及绑定邮箱，结合时间戳进行密码学处理之后打包，通过 POST 发送给服务器端。

服务器端通过密码学手段验证用户名和邮箱是否有效。如果无冲突且有效，

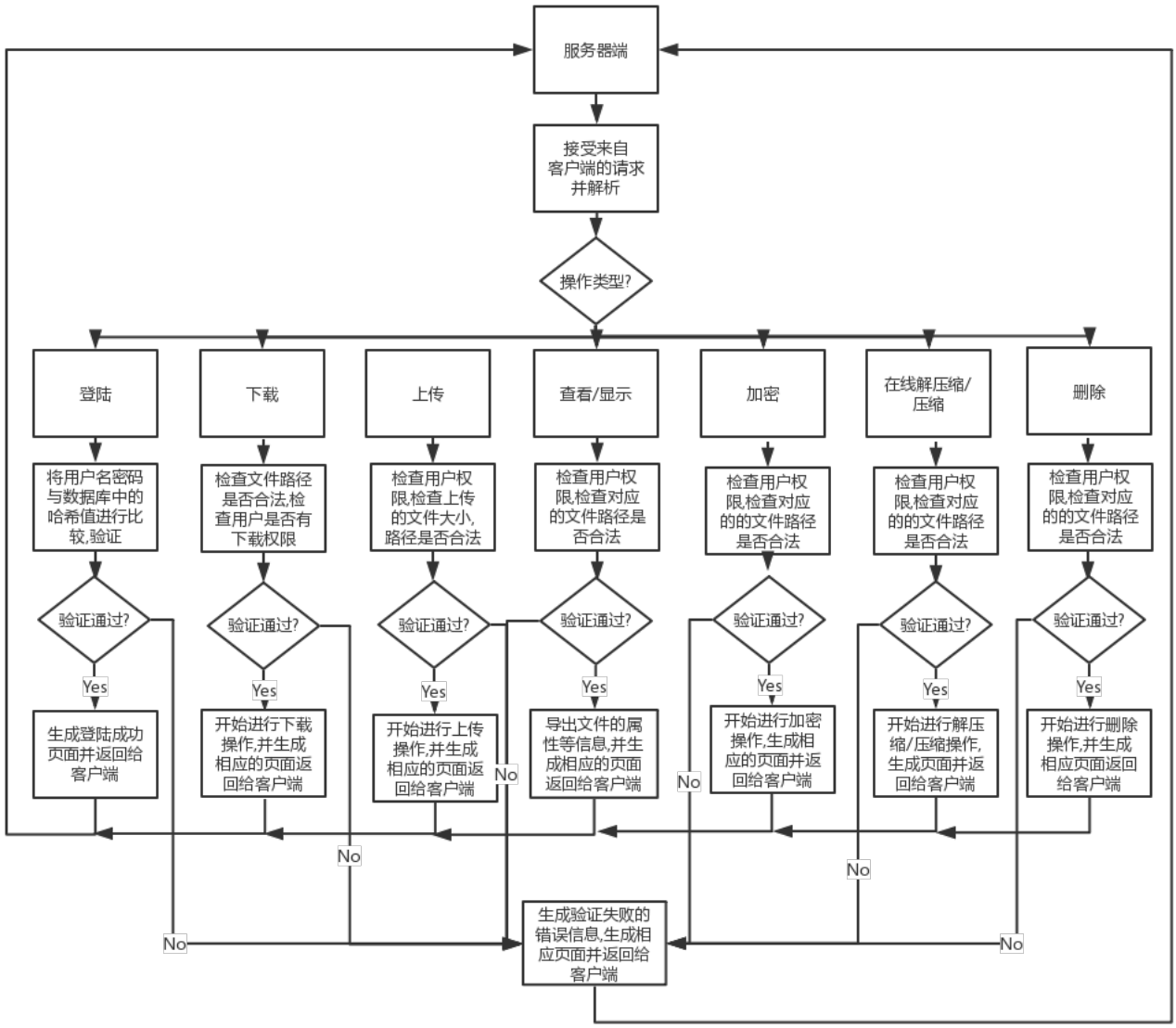

图 3.4　服务器端基本流程图

在服务器端创建新用户，并设置对应的邮箱一直处理后的密码。如果冲突或者无效，则返回错误信息给客户端。

如果注册成功，客户端生成 HTML 页面，提示成功；如果用户名或邮箱冲突或无效，则生成 HTML 页面，显示相应信息。

3.2.7　功能 3-用户忘记密码的具体流程

在看到登陆界面之后，用户可以点击“忘记密码”键，客户端生成 HTML 页面，，跳转到新页面。之后在新的页面中输入绑定邮箱以及新的密码，点击“确认”键。

客户端将密码和邮箱，结合时间戳进行密码学处理之后打包，通过 POST 发送给服务器端。

服务器端检查邮箱是否有效。如果邮箱对应的用户存在，则生成随机链接到对应邮箱中，以便重置密码，并返回“邮箱已发送”信息给客户端。如果不存在用户，则返回“邮箱不存在”给客户端。

如果服务器在规定时间（15min）内收到该链接下的新的密码，则修改该用户的密码为新密码。

如果客户端收到“邮箱已发送”，则显示“邮箱已发送”；如果客户端收到“邮箱不存在”，则显示“优先不存在”。

3.2.8 功能 4-上传文件的具体流程

用户点击“上传”按钮，在弹出的对话框中选择所要上传的文件或文件夹，并点击“上传”按钮。

客户端在用户第一次点击“上传”按钮时，显示小型资源管理器以便查找。在用户第二次点击“上传”按钮之后，客户端与服务器建立 tcp 链接，开始上传。上传时根据传输情况，计算速度，剩余时间，进度，剩余文件大小等信息。

客户端在用户第一次点击“上传”按钮时，弹出小型资源管理器。在用户第二次点击“上传”按钮之后，显示开始上传。上传时显示速度，剩余时间，进度，剩余文件大小等信息。

3.2.9 功能 5-下载文件的具体流程

用户选中所要下载的文件以及文件夹，点击“下载”按钮，在弹出的对话框中选择所要存储的文件夹，并点击“下载”按钮。

客户端在用户第一次点击“下载”按钮时，显示小型资源管理器以便设置下载路径。在用户第二次点击“下载”按钮之后，客户端与服务器建立 tcp 链接，开始下载。下载时根据传输情况，计算速度，剩余时间，进度，剩余文件大小等信息。

客户端在用户第一次点击“下载”按钮时，弹出小型资源管理器。在用户第二次点击“下载”按钮之后，显示开始下载。下载时显示速度，剩余时间，进度，剩余文件大小等信息。

3.2.10 功能 6-新建文件夹的具体流程

用户在当前目录空白处右键点击新建文件夹，或在点击新建文件夹的功能按钮，在窗口输入名称并点击确认

客户端将新建文件夹的指令与名称打包发给服务端，服务端首先检查名字是否有效，否则提示非法名称，是则判断文件夹是否已经存在，是则创建，否则返回名称冲突的错误。

若创建成功，则刷新当前目录，否则输出错误信息

3.2.11 功能 7-打开文件夹的具体流程

用户双击文件夹，或者选中文件夹之后点击打开选项。

客户端将打开文件夹的指令打包，发送到服务器，服务器传回文件夹内容。客户端接收之后，切换路径到所选中的文件夹，并展示其所包含的文件及文件夹。

若无异常发生，客户端显示文件夹中的文件以及子文件夹。

3.2.12 功能 8-重命名的具体流程

用户选中文件或文件名，右键，选中“重命名”选项。

客户端将重命名的原名字和新名字打包发给服务器端。

服务器检查该重命名是否合法不冲突，是则返回“成功”的信息，否则，返回“失败”的信息。

如果成功，则刷新当前目录，显示最新的名字。如果失败，则提示失败。

3.2.13 功能 9-复制、粘贴、剪切的具体流程

复制：用户选中需要操作的文件和文件夹，右键，选中“复制”选项。客户端将用户选中要复制的项的完全名字（包括路径）存储到 cache 中。

剪切：用户选中需要操作的文件和文件夹，右键，选中“剪切”选项。客户端将用户选中要剪切的项的完全名字（包括路径）存储到 cache 中。

粘贴：用户在所要粘贴的文件夹中，右键，选中“粘贴”选项。需要注意的是，必须有之前“复制”或“剪切”的操作记录，“粘贴”选项才可选。客户端将执行粘贴的文件夹的路径，以及之前复制或者剪切的类型一起打包，发给服务器端。服务器接收之后检查命名是否冲突。如果冲突就返回“命名冲突”信息；如果不冲突，

如果是复制，则复制到目标文件夹，如果是剪切，则先复制，再删除。最后返回“成功”给客户端

如果粘贴成功，则刷新当前文件夹，显示最新结果。如果粘贴失败，则弹窗提示粘贴失败。

3.2.14 功能 10-移入回收站、移出回收站、彻底删除的具体流程

移入回收站：

用户选中文件或文件夹，右键，选中“移入回收站”选项。客户端将该文件或文件夹名字（包括路径）打包发送到服务器端。服务器将该文件或文件夹移入“回收站”中并返回“成功”。客户端收到信息后，刷新当前文件夹。

移出回收站：

用户在回收站中选中文件或文件夹，右键，选中“移出回收站”选项。客户端将该文件或文件夹名字（包括路径）打包发送到服务器端。服务器端检查该文件或文件夹复原之后是否有命名冲突等。如果无冲突则移出“回收站”中并返回“成功”，否则返回“失败”。客户端收到信息后，如果成功，则刷新回收站；如果失败，则弹窗提示。

彻底删除：

用户在回收站中选中文件或文件夹，右键，选中“彻底删除”。客户端将该文件或文件夹名字（包括路径）打包发送到服务器端。服务器从回收站中删除。返回“成功”。客户端收到信息后，如果成功，则刷新回收站；如果失败，则弹窗提示。

3.2.15 功能 11-加入收藏夹、移出收藏夹的具体流程

加入收藏夹：

用户选中文件或文件名，右键，选中“加入收藏夹”选项。客户端将用户选中的文件名打包发给服务器端，服务器将该文件或文件夹加入所维护的收藏夹数据结构中。返回成功。

移出收藏夹：

用户在收藏夹中选中文件或文件名，右键，选中“移出收藏夹”选项。客户端将用户选中的文件名打包发给服务器端，服务器将该文件或文件夹从所维护的收藏夹数据结构中删除。返回成功。

3.2.16 功能 12-加密的具体流程

用户选中所要加密的文件或文件夹，右键，选中“加密”选项。在接下来弹出的对话框中写入不同于登录密码的密钥。

客户端将用户输入的密钥进行密码学处理，和对应的文件以及文件夹名称一起打包，发给服务器。服务器端用对该文件及文件夹设置加密标记，并保存经密码学处理的密钥，以便后面比对。最后服务器将陈工信息返回给客户端。

如果成功，则提示加密成功。否则弹窗提示失败。

3.2.17 功能 13-分享的具体流程

用户选中所要分享的文件或文件夹，右键，如果选中“分享”选项。接下来会生成带有随机字符串的链接。用户将该字符串发送给其他用户。

用户在客户端点击“导入分享”按钮，在弹出的对话框中输入链接；也可以直接用该链接用其他软件下载。

客户端在用户点击“分享”之后，将文件或文件夹的名字（包括路径）打包，标记“分享”发通过 POST 送给服务器端。服务器收到后根据路径名生成带有随机字符串的链接，发送给客户端。服务器维护文件名字到链接的映射，以便分享，以及在规定时间之后（如七天）取消该链接有效性。

在其他用户点击”导入分享“之后，客户端将该链接发送到服务器端。服务器检查该串是否有效，如果无效则返回”无效“给客户端；否则在服务器中将该文件或文件夹复制到该用户空间中，返回”成功“给客户端。

客户端在用户点击“分享”之后，如果成功，则提示成功，并显示该链接；否则提示失败。

其他用户在导入时，如果链接无效则提示无效，否则提示成功，并刷新页面，显示该文件或文件夹的位置。

3.2.18 功能 14-搜索的具体流程

用户在当前目录上方的搜索框输入关键字，点击搜索

客户端将当前目录与关键字打包发送到服务器，服务器对当前目录与子目录的文件、文件夹列表以及可见的共享文件夹进行匹配，返回匹配成功的列表。

客户端像进入一个新的文件夹一样显示搜索结果

3.2.19 功能 15-预览的具体流程

用户不做显式的操作

服务器将当前目录的文件进行格式匹配:

1. 文档，在大图标模式下，返回第一页的图片；在小图标模式下，返回对应格式的图标

2. 视频：在大图标模式下，返回随机帧的秃瓢；在小图标模式下，返回对应格式的图标

3. 其他文件：返回该文件附带的图标，若无则返回对应格式的图标

显示文件列表时显示对应的图标或预览

3.2.20 功能 16-在线解压/压缩的具体流程

解压:

用户在一个压缩文件上右击，点击在线解压

客户端将文件路径与解压指令发送给服务端，服务器查找文件是否存在且为压缩文件：1. 查找成功，尝试解压。若成功，则解压到同名文件夹（若同名文件夹已存在，则解压入内），否则生成 HTML 页面，提示解压失败 2. 查找不成功，生成 HTML 页面，提示文件不存在

压缩:

用户在当前文件夹复选多个文件、文件夹，单机压缩功能按钮或右键选择压缩，点击确认或更改默认压缩文件名后点击确认。

客户端提示的默认压缩包名为：若只选择了一个文件、文件夹，则压缩包名称默认为它的名字。若选择了多个文件、文件夹，则压缩包名称默认为当前目录的名字（若当前目录为用户网盘根目录，则为用户名称）。

客户端将复选的文件与压缩指令、压缩包名称发送给服务端。服务端确认这些文件的存在，并根据压缩包名称创建压缩文件：若名称冲突，则在其后增加”（1）”（若仍冲突则改为”（2）”，类推）压缩成功后，生成 HTML 页面，提示压缩成功

3.2.21 功能 17-举报的具体流程

用户选中所要举报的文件以及文件夹，右键，选择“举报”选项。在接下来弹出的对话框中选择举报的分类。

客户端在用户点击“举报”选项之后，生成对话框，之后将用户所选择的文件

以及文件夹的名字以及举报类型打包，发给服务器端。

服务器接收之后记录文件名，及其 md5 值，并在所维护的举报库中找到相应 md5，如果找到了，就增加举报次数，如果没有找到则将 md5 值与文件信息加入，并设置举报次数为 1。最后服务器端返回成功信息给客户端。

运维人员定期检查举报库，判断文件是否应被屏蔽。若是，则将举报库中该条文件设为已审核，屏蔽。否则，将该条文件设为已审核，放行。

客户端生成 HTML 页面，显示”感谢您的举报“窗口。

3.2.22 功能 18-审核的具体流程

用户对网盘文件进行正常的修改操作

服务器对每次目录的更新（重命名，添加文件/文件夹）进行匹配文件名，若关键字匹配成功，则使该次修改操作失败，并返回错误信息：敏感关键字。

服务器对文件的更新（上传，粘贴移动）进行 md5 匹配，若在举报库中匹配 md5 成功且该文件未屏蔽状态，则使该次操作失败生成 HTML 页面，并返回错误信息：该文件已被举报。

3.2.23 功能 19-标签页创建/关闭的具体流程

创建:

用户点击标签页旁边的创建按钮。

客户端打包指令发送给服务端，服务端返回与当前目录相同的一个子页面作为新的标签页。

用户在标签页栏看到与当前标签页在同一目录的新标签页。

关闭:

用户点击标签页上的关闭按钮。

客户端打包指令发送给服务端并删除该子页，服务端返结束该会话记录。

该标签页被关闭，从标签栏中消失。

3.2.24 功能 20-创建共享文件夹的具体流程

用户点击“创建共享文件夹”按钮，输入想要创建的共享文件夹的名称，选择想要对其可见的用户列表，并对其分配权限：管理，读，写

用户点击创建并输入文件夹名后，客户端将相关指令信息打包发送给服务端

服务端在专门设置的放置共享文件夹的位置创建该文件夹。若创建失败，则返回错误信息。若创建成功，则根据用户设置的权限对文件夹的属性进行修改。

客户端收到创建成功或失败，显示提示信息。

3.2.25 功能 21-进入共享文件夹的具体流程

用户点击共享文件夹按钮，客户端将此命令打包发送到服务器。

服务器传回所有对用户可见的共享文件夹（看起来就像此时进入了一个文件夹一样）。

用户点击想要进入的共享文件夹，客户端将指令打包发送到服务器

服务器传回该共享文件夹内的所有对该用户的可见文件，从而进入了该文件夹。之后的操作与普通文件夹一样，但多了一个额外限制：只返回对改用户可见的文件。

用户选择进入一个共享文件夹，之后对其的操作与普通文件夹一样

3.2.26 功能 22-共享文件夹的权限匹配的具体流程

用户对共享文件夹/其中的文件夹、文件进行像普通文件（夹）一样的操作：修改权限，创建文件夹、文件，下载，上传，重命名，删除，移动，复制粘贴，预览

客户端的行为与普通文件夹下的行为一致，但在服务端需要判断用户的权限是否允许客户进行该操作：

用户需要有该文件的读权限：

1. 下载
2. 复制、移动到用户个人网盘
3. 预览

用户需要有该文件的写权限：

1. 删除
2. 重命名
3. 移动
4. 上传对其进行覆盖
5. 删除的文件夹内包含这个文件

用户需要拥有该文件夹的读权限：

1. 进入该文件夹

2. 下载该文件夹

3. 复制、移动到用户个人网盘

4. 预览

用户需要有该文件夹的写权限：

1. 向其中上传文件（夹）

2. 在其中删除文件（夹）

3. 重命名该文件夹

4. 移动该文件夹

5. 上传文件夹对其进行合并

6. 删除该文件夹

7. 删除该文件夹所属的文件夹

用户需要有该共享文件夹的管理权限：

1. 修改其内文件、文件夹的权限分配

2. 移除该共享文件夹

若服务端发现用户指令与其权限不匹配，返回权限不匹配的信息，否则正常进行操作并返回正常操作的返回信息

3.2.27 功能 23-共享文件夹的权限管理的具体流程

用户对共享文件夹中的文件夹/文件或共享文件夹本身点击管理按钮，选择指定的用户并修改其对应的各个权限，点击确认

点击确认按钮后，客户端将指令打包发给服务端

服务端判断用户是否有管理权，若有则修改指令中的对应权限，并提示修改成功，否则，返回没有权限的错误信息

客户端根据返回信息提示修改是否成功

3.3 功能结构设计

3.3.1 整体结构

整体模块的结构如图 3.5 所示。整体结构由客户端的 4 个内部模块、1 个外部模块，和服务器端的 11 个内部模块、1 个外部模块组成。

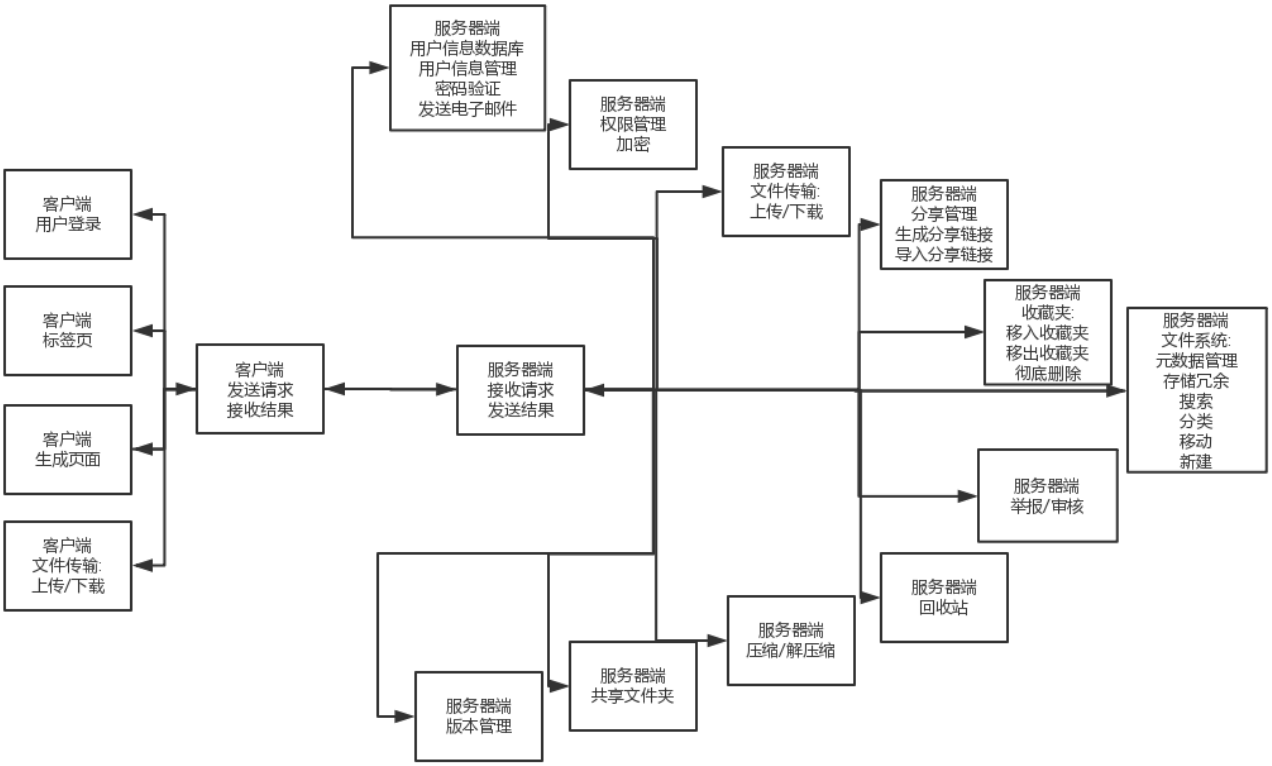

图 3.5　整体结构模块图

3.3.2　用户端结构

用户端的模块结构如图 3.6 所示，分成负责用户登录、注册、忘记密码的登陆模块，负责标签页的创建与关闭操作的标签页模块，负责生成页面，显示内容，弹出错误提示信息的显示模块，负责上传文件、下载文件的传输模块，以及与这些模块通信、与服务器端模块通信的通信模块一共 5 个模块构成。

3.3.2.1　MODULE.CLIENT.1: 通信模块

将其他模块产生的输入打包为 http 请求，向服务器端发送，并将返回的内容传给该模块

3.3.2.2　MODULE.CLIENT.2: 登陆模块

产生登陆页面。

若用户登陆，检查其用户名与密码合法性，将用户名与密码散列值传给通信模块，并解析返回的结果

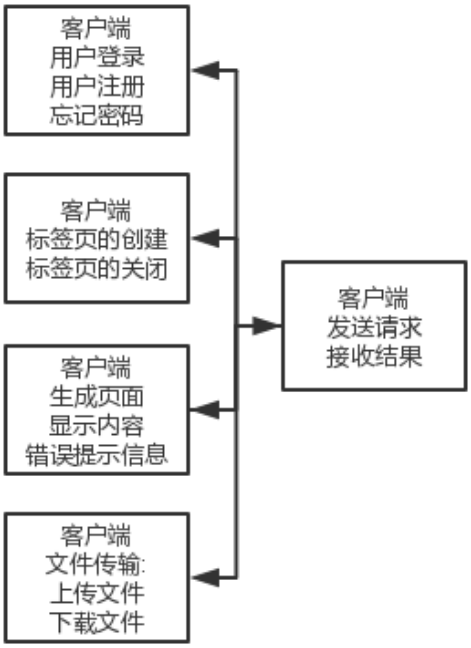

图 3.6　用户端模块结构图

若用户注册，则检查用户信息的合法性，并将其打包传给通信模块，解析返回的结果

若用户忘记密码，则检查用户信息的合法性，打包传给通信模块，解析传回的结果

3.3.2.3　MODULE.CLIENT.3: 标签页模块

管理用户同时打开的多个标签页，对每个标签页有一个子页面。

将用户对标签的操作打包传给通信模块，解析传回的结果

3.3.2.4　MODULE.CLIENT.4: 显示模块

绘制页面内容，包括文件列表、功能按钮、

3.3.2.5　MODULE.CLIENT.5: 传输模块

t

3.3.3 服务器端结构

服务器端的模块结构如图 3.6 所示，分成负责用户信息管理、密码验证、发送电子邮件等操作的用户信息数据库模块，负责权限管理、文件加密的权限模块，负责上传文件、下载文件的文件传输模块，负责生成分享链接、导入分享链接的分享管理模块，负责移入收藏夹、移出收藏夹的收藏夹模块，负责文件元数据管理（如存储冗余、搜索、分类、新建、移动等）的元数据管理模块，负责举办和审核的审核模块, 负责移入回收站、移出回收站、彻底删除的回收站模块，负责压缩、解压缩的压缩模块，负责共享文件夹操作的共享文件夹模块，负责版本更新的版本管理模块，以及负责与这些模块通信，与客户端模块通信的通信模块，一共 12 个模块。

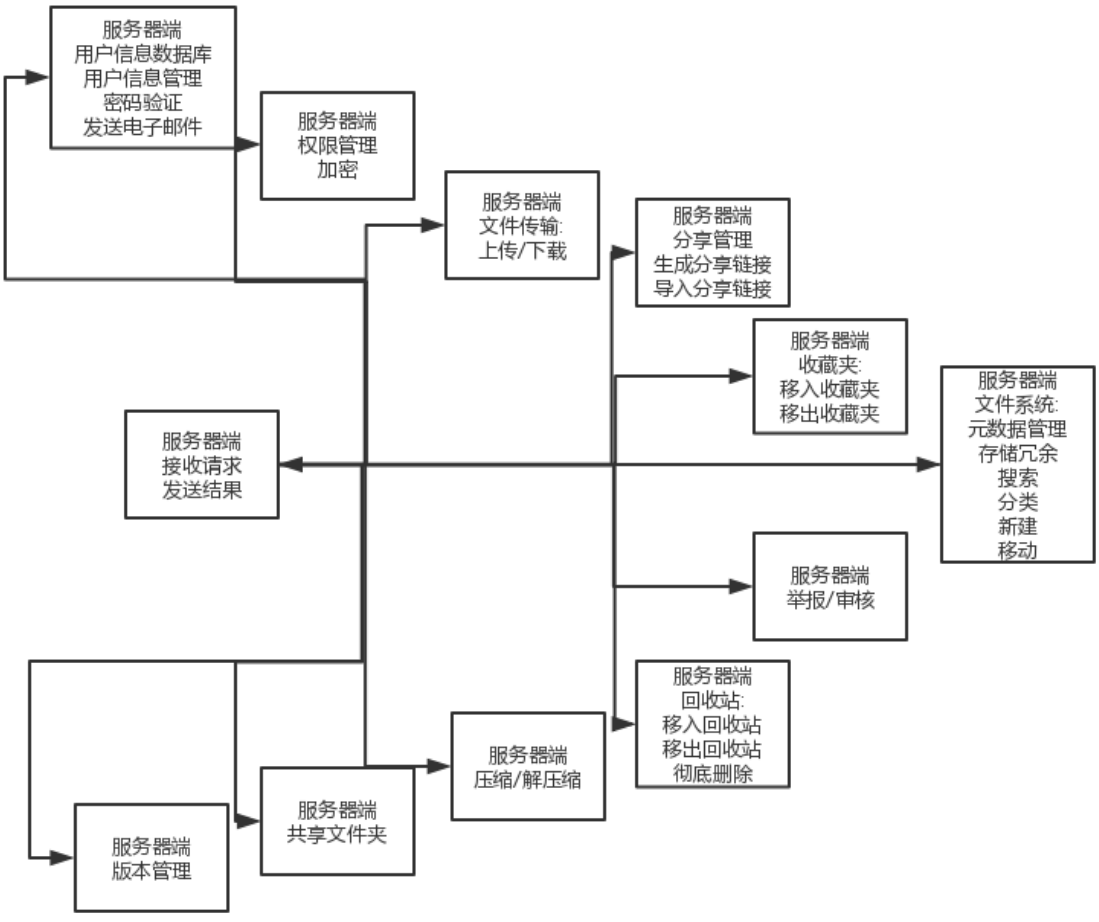

图 3.7　服务器端模块结构图

3.3.3.1 MODULE.SERVER.1: 通信模块

t

3.3.3.2 MODULE.SERVER.2: 用户信息数据库模块

t

3.3.3.3 MODULE.SERVER.3: 权限模块

t

3.3.3.4 MODULE.SERVER.4: 文件传输模块

t

3.3.3.5 MODULE.SERVER.5: 分享管理模块

t

3.3.3.6 MODULE.SERVER.6: 收藏夹模块

t

3.3.3.7 MODULE.SERVER.7: 元数据管理模块

t

3.3.3.8 MODULE.SERVER.8: 审核模块

t

3.3.3.9 MODULE.SERVER.9: 回收站模块

t

3.3.3.10 MODULE.SERVER.10: 压缩模块

t

3.3.3.11 MODULE.SERVER.11: 共享文件夹模块

t

3.3.3.12 MODULE.SERVER.12: 版本管理模块

t

3.4 功能需求与程序代码的关系

这一小节分为功能需求与用户端代码的关系和功能需求与服务器端代码的关系两个部分。其中，与用户端代码的关系如表 3.1，表 3.2 所示；与服务器端的代码的关系如表 3.3，表 3.4 所示。

表 3.1　功能需求与程序代码的关系表 1-用户端模块第 1 部分

需求 ID	MD.CL.1	MD.CL.2	MD.CL.3	MD.CL.4	MD.CL.5
R..USER.LOGIN.001	·	·	·	Y	·
R..USER.LOGIN.002	Y	Y	Y	·	·
R..USER.LOGIN.003	Y	Y	Y	·	·
R..USER.LOGIN.004	Y	Y	Y	·	·
R..USER.LOGIN.005	·	·	·	Y	·
R..FILE.BASIC.001	Y	·	·	Y	Y
R..FILE.BASIC.002	Y	·	·	Y	Y
R..FILE.BASIC.003	Y	·	·	Y	·
R..FILE.BASIC.004	Y	·	·	Y	·
R..FILE.BASIC.005	Y	·	·	Y	·
R..FILE.BASIC.006	Y	·	·	Y	·
R..FILE.BASIC.007	Y	·	·	Y	·
R..FILE.BASIC.008	Y	·	·	Y	·
R..FILE.BASIC.009	Y	·	·	Y	·
R..FILE.BASIC.010	·	·	Y	Y	·
R..FILE.HIGH.001	Y	·	·	Y	·
R..FILE.HIGH.002	Y	·	·	Y	·
R..FILE.HIGH.003	Y	·	·	Y	·
R..FILE.HIGH.004	Y	·	·	Y	·
R..FILE.HIGH.005	Y	·	·	Y	·

注：表中的 R..XXX 等均指 R.XYZ.CLOUDSTORAGE.XXX。MD.CL 指 MODULE.CLIENT

表 3.2　功能需求与程序代码的关系表 1-用户端模块第 2 部分

需求 ID	MD.CL.1	MD.CL.2	MD.CL.3	MD.CL.4	MD.CL.5
R..FILE.HIGH.006	Y	·	·	Y	·
R..FILE.HIGH.007	Y	·	·	Y	·
R..FILE.HIGH.008	Y	·	·	Y	·
R..FILE.HIGH.009	Y	·	·	Y	·
R..FILE.HIGH.010	Y	·	·	Y	·
R..FILE.HIGH.011	Y	·	·	Y	·
R..TAB.001	·	·	Y	Y	·
R..TAB.002	·	Y	·	Y	·
R..SHAREFOLDER.001	Y	·	·	Y	·
R..SHAREFOLDER.002	Y	·	·	Y	·
R..SHAREFOLDER.003	Y	·	·	Y	·
R..SHAREFOLDER.004	Y	·	·	Y	·
R..VERSION.001	Y	·	·	Y	·

注：表中的 R..XXX 等均指 R.XYZ.CLOUDSTORAGE.XXX。MD.CL 指 MODULE.CLIENT

表 3.3　功能需求与程序代码的关系表 2-服务器端模块第 1 部分

需求 ID	1	2	3	4	5	6	7	8	9	10	11	12
R..USER.LOGIN.001	·	·	·	·	·	·	·	·	·	·	·	Y
R..USER.LOGIN.002	Y	Y	·	·	·	·	·	·	·	·	·	·
R..USER.LOGIN.003	Y	Y	·	·	·	·	·	·	·	·	·	·
R..USER.LOGIN.004	Y	Y	·	·	·	·	·	·	·	·	·	·
R..USER.LOGIN.005	·	·	·	·	·	·	·	·	·	·	·	·
R..FILE.BASIC.001	Y	·	Y	Y	·	·	Y	Y	·	·	·	·
R..FILE.BASIC.002	Y	·	Y	Y	·	·	Y	Y	·	·	·	·
R..FILE.BASIC.003	Y	·	Y	·	·	·	Y	·	·	·	·	·
R..FILE.BASIC.004	Y	·	Y	·	·	·	Y	·	·	·	·	·
R..FILE.BASIC.005	Y	·	Y	·	·	·	Y	·	·	·	·	·
R..FILE.BASIC.006	Y	·	Y	·	·	·	Y	·	·	·	·	·
R..FILE.BASIC.007	Y	·	Y	·	·	·	Y	·	·	·	·	·
R..FILE.BASIC.008	Y	·	Y	·	·	·	Y	·	·	Y	·	·
R..FILE.BASIC.009	Y	·	Y	·	·	·	Y	·	·	Y	·	·
R..FILE.BASIC.010	·	·	·	·	·	·	·	·	·	·	·	·
R..FILE.HIGH.001	Y	·	Y	·	·	·	Y	·	Y	·	·	·
R..FILE.HIGH.002	Y	·	Y	·	·	Y	Y	·	·	·	·	·
R..FILE.HIGH.003	Y	·	Y	·	·	·	Y	·	·	·	·	·
R..FILE.HIGH.004	Y	·	Y	·	Y	·	Y	Y	·	·	·	·
R..FILE.HIGH.005	Y	·	Y	·	·	·	Y	·	·	·	·	·

注：表中的 R..XXX 等均指 R.XYZ.CLOUDSTORAGE.XXX。第一行的 1 12 表示指 MODULE.SERVER.1 12

表 3.4　功能需求与程序代码的关系表 2-服务器端模块第 2 部分

需求 ID	1	2	3	4	5	6	7	8	9	10	11	12
R..FILE.HIGH.006	Y	·	Y	·	·	·	Y	·	·	·	·	·
R..FILE.HIGH.007	Y	·	Y	·	·	·	Y	·	·	·	·	·
R..FILE.HIGH.008	Y	·	Y	·	·	·	Y	·	·	·	·	·
R..FILE.HIGH.009	Y	·	Y	·	·	·	Y	·	·	·	·	·
R..FILE.HIGH.010	Y	·	Y	·	·	·	Y	Y	·	·	·	·
R..FILE.HIGH.011	Y	·	Y	·	·	·	Y	Y	·	·	·	·
R..TAB.001	·	·	·	·	·	·	·	·	·	·	·	·
R..TAB.002	·	·	·	·	·	·	·	·	·	·	·	·
R..SHAREFOLDER.001	Y	·	Y	·	·	·	Y	·	·	·	Y	·
R..SHAREFOLDER.002	Y	·	Y	·	·	·	Y	·	·	·	Y	·
R..SHAREFOLDER.003	Y	·	Y	·	·	·	Y	·	·	·	Y	·
R..SHAREFOLDER.004	Y	·	Y	·	·	·	Y	·	·	·	Y	·
R..VERSION.001	Y	·	·	·	·	·	·	·	·	·	·	Y

注：表中的 R..XXX 等均指 R.XYZ.CLOUDSTORAGE.XXX。第一行的 1 12 表示指 MODULE.SERVER.1 12

第 4 章　接口设计

4.1　外部接口

4.1.1　HTTP 接口

xyz 云盘系统通过 HTTP 请求的方式实现 API 调用。

4.1.1.1　初始界面接口

URL：/api/index

请求类型：GET

参数：无参数

返回值: 返回初始页面

4.1.1.2　登录接口

URL：/api/login

请求类型：POST

参数：

• username: 用户名/邮箱

• pass: 密码经过密码学处理之后的字符串

返回值:bool 类型, 表示是否成功, 同时设置 cookie

4.1.1.3　注册接口

URL：/api/register

请求类型：POST

参数：

• username: 用户名

• email: 邮箱

• 密码: 密码经过密码学处理之后得到的字符串

返回值:bool 类型, 表示是否注册成功.

4.1.1.4 忘记密码接口

URL：/api/forget

请求类型：POST

参数：

• username: 用户名/邮箱

返回值: 不返回. 如果用户存在, 则服务器向该邮箱发送重设密码的链接.

4.1.1.5 登陆后接口

URL：/api/home

请求类型：GET

参数：

• cookie, 无需用户手动输入

返回值: 显示登陆后的页面。

4.1.1.6 上传接口

URL：/api/upload

请求类型：POST

参数：

• path：文件的路径

• cookie, 无需用户手动输入

返回值:bool 类型，表示是否成功。

4.1.1.7 下载接口

URL：/api/download

请求类型：GET

参数：

• path：文件路径

• cookie：无需用户手动输入

返回值:

4.1.1.8 登录接口

URL：/api/

请求类型：POST

参数：

-
-

返回值:

4.1.1.9 登录接口

URL：/api/

请求类型：POST

参数：

-
-

返回值:

4.1.1.10 登录接口

URL：/api/

请求类型：POST

参数：

-
-

返回值:

4.1.1.11 登录接口

URL：/api/

请求类型：POST

参数：

-
-

返回值:

4.1.1.12 登录接口

URL：/api/

请求类型：POST

参数:

-
-

返回值:

4.2 内部接口

内部模块/系统之间的交互的接口。

第 5 章　数据结构设计

5.1　逻辑结构设计

使用伪代码来表示数据结构的设计

5.1.1　文件数据结构

```
1  class File:
2      str file_name
3      str file_mode
4      int owner_id
5      int num_bytes
6      time last_updated
7      list right_list
```

说明：此类包含了云盘上文件的相关信息

5.1.2　用户信息数据结构

```
1  class User:
2      str name
3      str password
4      str email
5      list files_own
```

说明：此类包含了用户的基本信息

5.1.3　链接数据结构

```
1  class Link:
2      int owner_id
3      str link_url
4      str link_password
5      time due_time
```

说明：此类包含了分享云盘资源所需要的信息

5.1.4　举报信息数据结构

```
1  class Report:
2      int file_id
3      int report_type
4      str report_detail
5      bin report_fig
```

说明：此类包含了举报文件的信息

5.2 物理结构设计

各数据结构无特殊物理结构要求。

5.3 数据结构与程序模块的关系

表 5.1 数据结构与程序代码的关表

·	用户结构	文件结构	链接结构	举报结构
客户端登录模块	Y	·	·	·
客户端标签页模块	Y	·	·	·
客户端生成模块	Y	Y	·	·
文件传输模块	Y	·	Y	·
服务器用户管理模块	Y	·	·	·
服务器权限加密模块	Y	Y	·	·
分享模块	Y	Y	Y	·
收藏夹模块	Y	Y	·	·
举报模块	Y	Y	·	Y
回收站模块	Y	Y	·	·
解压压缩模块	·	Y	·	·
版本管理模块	Y	Y	·	·
共享文件夹模块	Y	Y	·	·

注：各项数据结构的实现与各个程序模块的分配关系

第 6 章　数据库设计

6.1　数据库环境说明

本系统的数据系统采用 MySQL 数据库系统。

6.2　数据库的命名规则

只有标识符“ID”可以缩写，其他有意义的名词不允许缩写
表名统一用单数。命名最大字节数为 100，关联表用该表”ID” 作为外键
统一所有表无前缀

6.3　逻辑设计

数据库设计应满足 BCNF 范式
实体的逻辑关系图如图 6.1 所示。

6.4　物理设计

6.4.1　数据库产品

数据库采用 MySql 数据库。由于文件本身是存储在 ceph 中的，数据库只存储控制信息，因此不需要分布式数据库。数据库所在的服务器应使用 1TB 以上的 SSD 硬盘并使用 32G 以上内存

6.4.2　实体属性、类型、精度

6.4.2.1　文件数据表设计

文件数据表设计如表 6.1 所示。

6.4.2.2　用户数据表设计

用户数据表设计如表 6.2 所示。

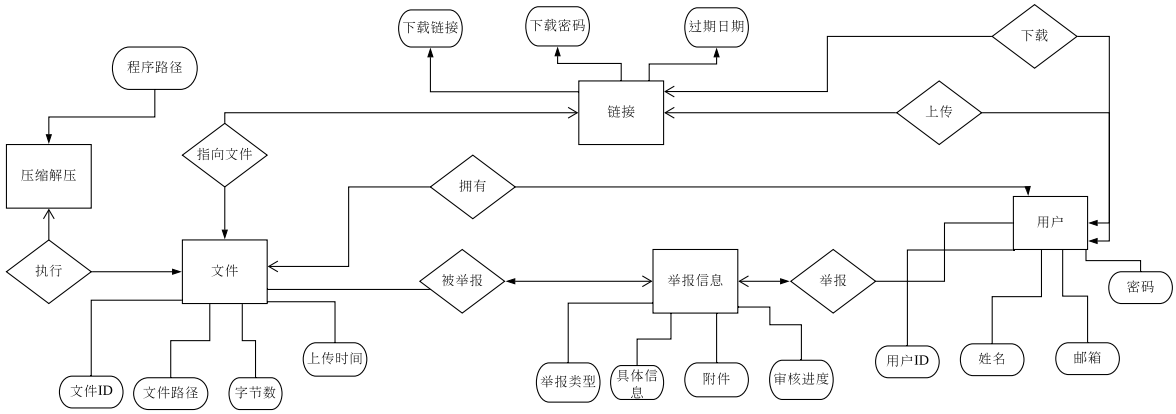

图 6.1　ER1 关系图

表 6.1　文件数据表 Files 设计

字段名	类型	大小	说明	备注
文件 ID	char	64	文件的唯一标识符	主键
文件路径	char	512	文件在用户目录下路径	
文件模式	char	20	文件的信息	
用户 ID	char	64	该文件拥有者的 ID	外键，来自 Users 表
收藏夹 ID	char	64	该文件所在收藏夹	外键，来自 BookMarks 表
压缩/解压 ID	char	64	解压或压缩该文件的程序	外键，来自 Presses 表
字节数	int	1	文件大小	
更新时间	char	64	上次上传文件更新的时间	

注：文件数据表 Files 设计

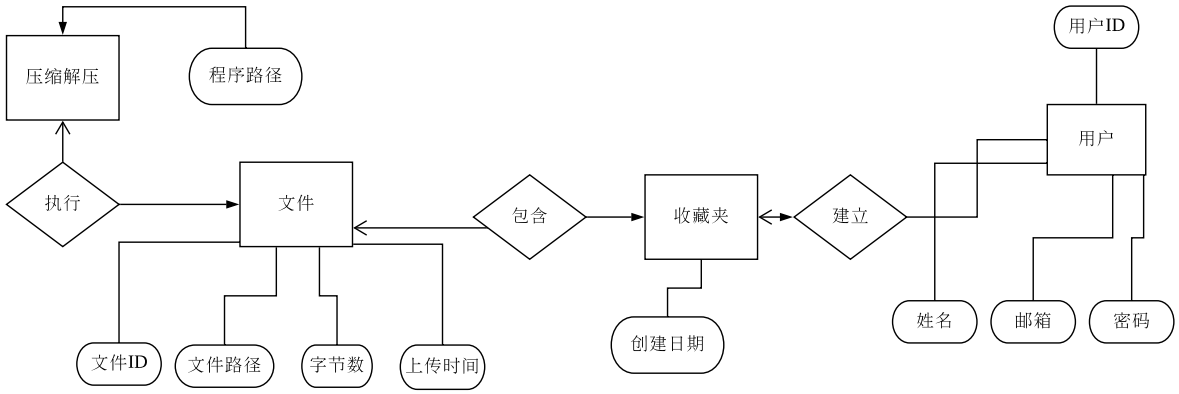

图 6.2　ER2 关系图

表 6.2　用户数据表 Users 设计

字段名	类型	大小	说明	备注
用户 ID	char	64	用户的唯一标识符	主键
用户名	char	64	对应用户	
密码	char	64	用户登录的密码	
邮箱地址	char	64	用户的邮箱	

注：用户数据表 Users 设计

6.4.2.3 链接数据表设计

链接数据表设计如表 6.3 所示。

表 6.3 链接数据表 Users 设计

字段名	类型	大小	说明	备注
用户 ID	char	64	对应用户	主键；外键，来自 Users 表
文件 ID	char	64	对应文件	主键；外键，来自 Files 表
链接网址	char	64	本链接的 URL	
下载密码	char	64	输入密码下载资源	
过期日期	char	128	链接失效的日期时间	

注：链接数据表 Links 设计

6.4.2.4 收藏夹数据表设计

表 6.4 收藏夹数据表 BookMarks 设计

字段名	类型	大小	说明	备注
收藏夹 ID	char	64	收藏夹的唯一标识符	主键
用户 ID	char	64	拥有该收藏夹的用户	外键，来自 Users 表
创建日期	char	128	创建该收藏夹时间	

注：收藏夹数据表 BookMarks 设计

6.4.2.5 举报审核数据表设计

6.4.2.6 压缩解压数据表设计

6.5 安全性设计

数据库每小时进行备份，并导出数据到备份服务器上。

数据库所在的磁盘使用带冗余的磁盘阵列。

数据库使用普通权限用户进行权限控制，设定数据表的读写权限。

表 6.5　举报数据表 Reports 设计

字段名	类型	大小	说明	备注
举报 ID	char	64	举报信息的唯一标识符	主键
用户 ID	char	64	提供该举报信息的用户	外键，来自 Users 表
文件 ID	char	64	举报的文件 ID	外键，来自 Files 表
举报类型	int	1	被举报文件的类型	
举报内容	char	1024	举报的具体信息	
举报附件	bin	2MB	举报内容附件	
审核状态	int	1	审核该举报信的进度	

注：举报审核数据表 Reports 设计

表 6.6　压缩解压表 Presses 设计

字段名	类型	大小	说明	备注
算法 ID	char	64	压缩解压算法的唯一标识符	主键
程序路径	char	64	执行文件的路径	

注：压缩解压数据表 Presses 设计

6.6 数据库管理与维护说明

数据库的具体备份、压缩功能的实现主要交由 MySQL 的功能来完成。

备份的主要策略为: 每次操作由主数据库完成之后，备份数据库向主数据库 fetch 更新。备份的恢复方式为将备份数据库的内容 copy 到主数据库。

对于文件系统的备份，由 ceph 这一高可用的文件系统来完成，其内部已有 replication 以及灾害恢复的功能，无需在外部另作备份。

第 7 章　界面设计

7.1　客户端界面

客户端界面如图 7.1 所示。

图 7.1　用户初始界面

7.2　服务器端界面

由于服务器端由管理员使用命令行进行交互，因此无界面图

7.3　登录界面

用户登陆界面如图 7.2 所示。

7.4　缩略图模式界面

缩略图模式界面如图 7.3 所示。

图 7.2　用户登录界面

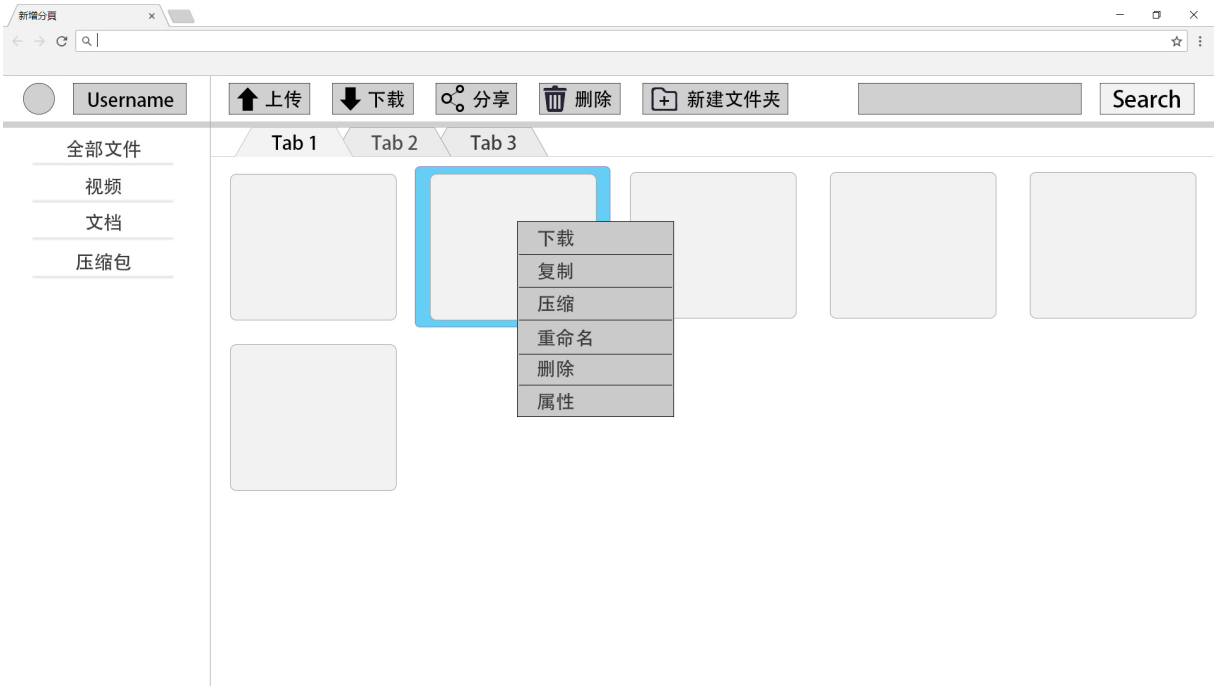

图 7.3　缩略图模式界面

第 8 章　出错处理设计

8.1　数据库出错处理

本云盘系统仅针对于用户信息以及其权限建立了数据库，其十分轻量，改变量比较小，故采用同步的，完全备份的方式。当数据库出错时，切换至有备份的另一台服务器继续提供该功能，无需暂停在线服务，待主服务器恢复后切换回来提供服务。

8.2　某模块失效处理

模块失效时依据失效模块的功能取决我们的处理方式：若核心模块如登陆模块、数据库连接与请求、底层文件系统或者 HTTP 请求模块失效，则应暂停整个系统的服务，在客户端提示维护信息，并由该模块的开发人员为主，在其他开发人员支持下调整失效模块，同时注意调整与该模块相关的其他模块的接口，测试完成后将系统整体上线。若非核心模块如传输、分享，则先关闭失效模块提供的服务以及相关接口提供的服务，其余不相关的服务维持状态，之后由该模块的开发人员为主，在其他开发人员支持下调整失效模块，同时注意调整与该模块相关的其他模块的接口，测试完成后将要修改的所有模块一起上线。

第 9 章　安全保密设计

9.1　服务器安全性

系统运行所在的服务器为 CentOS 系统，定期使用 yum 包管理器进行软件升级以及进行系统版本升级，保证及时更新安全补丁。服务器禁止 root 用户登陆；普通用户的用户名、密码的长度、字符集均做限制；管理员使用公钥私钥登录服务器。服务器运行防火墙软件，禁止非 HTTP/HTTPS/ssh 的端口链接

9.2　数据库安全性

数据库只允许 localhost 链接。对于部分固定的信息，数据库只提供只读权限，同时禁止删除数据库等危险操作

9.3　网络传输安全性

本系统全站使用 HTTPS 安全连接，保证服务器于浏览器之间传输是安全加密的。

9.4　网络接口安全性

所有 API 都对 SQL 注入进行过滤，保证安全性

9.5　用户信息安全性

用户使用用户名与密码进行验证，忘记密码可以通过邮箱找回密码用户输错密码时延迟提示，连续 3 此密码错误则要求输入验证码，降低暴力破解可能性用户密码在数据库中不保存明文，而是保存加盐的散列值，即使数据斜率也不能得到用户密码

第 10 章　维护设计

维护设计主要为数据库的维护功能，包括数据库的日常备份、压缩、维护，以及文件的备份与恢复。数据库的具体备份、压缩功能的实现主要交由 MySQL 的功能来完成。备份的主要策略为：每次操作由主数据库完成之后，备份数据库向主数据库 fetch 更新。备份的恢复方式为将备份数据库的内容 copy 到主数据库。对于文件系统的备份，由 ceph 这一高可用的文件系统来完成，其内部已有 replication 以及灾害恢复的功能，无需在外部另作备份。