## 1.需求分析

随着网路技术的进一步发展，现代人的日常工作与网络之间的关系也越来越紧密。越来越多的人为了办公的方便或者数据的备份选择将部分文件上传到网上进行保存。当今社会上也不乏一些成熟的网盘软件，这些软件给我们带来了许多的的便利。但是一个很明显的问题出现了。文件保存在网盘里面真的安全吗？目前主流的网盘系统中，文件在上传过程中以及存放在网盘里时文件都是明文，这对于我们自身文件的安全性带来了巨大的挑战。一些号称可以对文件进行在线加密和解密的技术虽然可以防止他人获取自己的文件信息，但是服务端却可以私自查看用户文件，从某种程度上说用户在服务商面前也没有了隐私。因此我们提出一个基于加密搜索的可靠在线网盘管理系统。在这个系统中，文件在上传之前会经过加密，文件下载下来后会经过解密，文件存储在服务端是经过加密的，密钥由客户端管理服务端无法获知用户文件内容。客户与服务器之间的文件传输采用了UDP分片技术，更加稳定和安全。与此同时，客户端在对其文件进行搜索时其搜索内容和得到的信息也都是经过加密处理的，不会泄露用户的个人网盘内容相关信息。

### 1.1功能需求

1.客户端对于指定的文件可以采用对称加密的技术进行加密和解密，通过给定的安全系数可以生成指定密钥，加密解密的密钥由客户端进行管理。用户可以对其网盘数据进行加密搜索，得到的信息在传输中也是加密的，由客户端进行解密。

2.客户端与服务端之间可以采用UDP协议方式进行可靠文件传输，文件在传输过程中是经过加密处理。

3.服务端存储上传的加密文件，对于用户的数据具有简单的版本控制功能，支持通过特定的关键字。

### 1.2性能需求

1.加密与解密的速度在本地能达到100Mb/s（机械硬盘7200转情况下）。

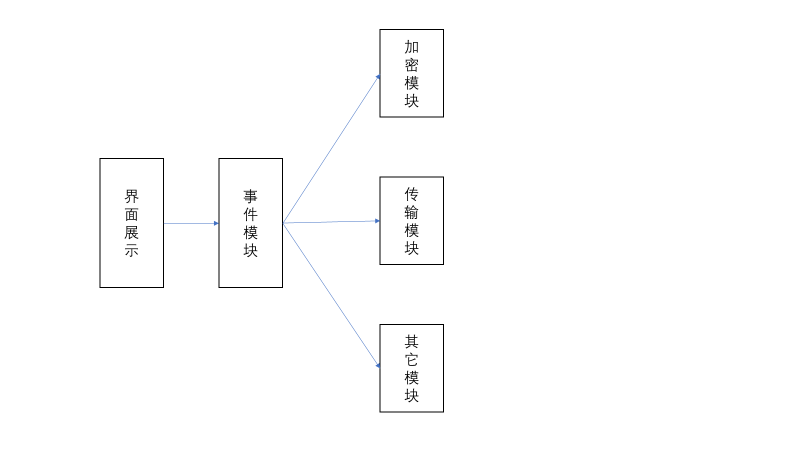
2.传输速度在100M宽带下达到20Mb/s。

3.对文件的版本控制长达一年。

4.客户端在windows PC端64位系统下运行

## 2.模块设计

### 2.1客户端模块架构设计



#### 2.1.1加密模块

1.给与指定安全系数生成密钥。

2.给定的文件加密和解密。

3.对于指定的信息进行加密和解密。

4基于指定信息生成关键字

#### 2.1.2传输模块

1.通讯模块（包含发送模块和工具模块） 在TCP指令控制进行UDP文件传输

2.工具模块 对文件的完整性进行检查，对文件缺少的部分信息进行统计，对文件发送时装配文件头部信息。

3.发送模块 对于指定的文件以UDP的方式发送到指定端口地址

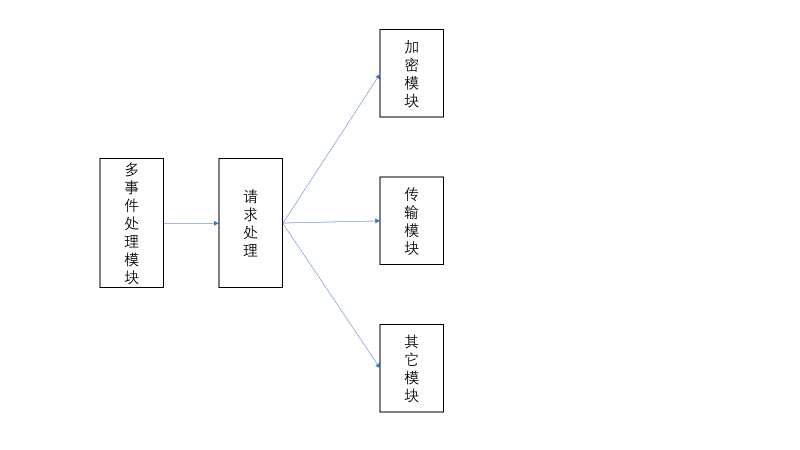
#### 2.1.3其它模块

1.xml文件解析模块 根据xml文档内容展现网盘结构

2.网络请求解析模块 根据不同网络返回值对应不同的请求结果，同时将不同的客户端操作映射为网络请求。

.

### 2.2服务端模块设计



#### 2.2.1加密模块

1.加密搜索 给定加密关键字的情况下检索密文

2.映射函数 给定的的信息通过确定性算法转化为映射为另外一个值

#### 2.2.2传输模块.

1.通讯模块（包含发送模块和工具模块） 在TCP指令控制进行UDP文件传输

2.工具模块 对文件的完整性进行检查，对文件缺少的部分信息进行统计，对文件发送时装配文件头部信息。

3.发送模块 对于指定的文件以UDP的方式发送到指定端口地址

#### 2.2.3存储模块（包含数据库模块）

1.基于时间追踪文件变化，具有简单的版本控制功能。

2.数据库模块 ：以键值对方式存储相关文件描述信息与文件地址

3.为文件分配存放地址

4.基于文件（夹）组织形式生成xml文档

#### 2.2.4其它模块

1.指令模块 根据不同的请求转化为指令进行处理，然后将处理结果经过处理转化为特殊信息返回给请求对象。