# **1.研究背景意义**

在当今信息时代，互联网已经渗入到人们生活的各个领域。随着互联网技术不断的升级，人们工作与生活产生的数据也呈现指数形式的增长。面对大量的数据，数据的存储已经成为了最迫切的需求。为了解决这一现象，云计算的技术也正不断革新。云计算，按照美国国家标准与技术研究院定义：云计算是一种按使用量付费的模式，这种模式提供可用的、便捷的、按需的网络访问， 进入可配置的计算资源共享池（资源包括[网络](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C/143243)，服务器，存储，[应用软件](https://baike.baidu.com/item/%E5%BA%94%E7%94%A8%E8%BD%AF%E4%BB%B6/216367)，服务），这些资源能够被快速提供，只需投入很少的管理工作，或与服务供应商进行很少的交互。在云计算概念上延伸和发展出来的新型网络存储技术云存储可以很好的解决数据的存储问题。目前互联网用户使用最多的基于云存储衍生的产品就是网盘。网盘，又名网络U盘、网络硬盘，是由互联网公司推出的在线存储服务，服务器商为用户划分一定的磁盘空间，为用户免费或收费提供文件的存储、访问、下载等文件管理等功能。网盘技术的兴起，越来越多人选择将日常或办公文件存储在云端并随时随地的使用PC、便携式笔记本或手机在线查看和管理文件，这种文件管理方式将人们从繁杂的存储和备份文件的操作中解放出来，从而更专心的专注于文件本身的内容。

当今社会也不乏一些主流的网盘服务，例如百度公司的百度云、115网盘和国外Dropbox公司的Dropbox。这些网盘服务确实给用户提供了很好的服务体验，但是如果从安全性和隐私性来看，这些网盘服务可能存在一些安全漏洞和隐私问题。就当今主流产品对比，按照安全性和对隐私性的保护，网盘可以分为两大类。第一类网盘是对用户的数据没有任何加密和保护，即用户数据明文上传和明文保存，。这类网盘产品有115网盘、百度网盘等产品。这种情况下任意用户的数据内容可以被服务商获知，用户的隐私得不到保证。其次明文上传和明文保存如果被他人非法获取，那么用户数据的安全也受到的相应的威胁。第二类网盘是网盘服务提供商对用户保存的文件进行加密和解密。这类网盘的产品代表是Dropbox公司的Dropbox网盘。这种情况下首先缓解了用户的数据安全问题，只要服务商加密解密的密钥不丢失，那么服务商可以防止他人盗取数据内容。但是这种加密手段是由运营商提供，密钥也是由运营商保管。这种情况运营商也具有检索用户数据的能力，用户的隐私问题还是没有很好地解决。第三类网盘是由客户端在本地加密，加密完成后上传到服务端，密钥由用户进行管理。这类网盘代表是一个叫“隐形云”的产品，是由”是杭州奕锐电子有限公司和阿里云合作推出的一个云盘。这种产品确实可以保护用户的隐私，但是使用中必须要先下载客户端才能使用，其次使用中对于网盘中输入查找信息时发现并没有对用户搜索信息进行加密，有可能造成用户的部分信息泄露。首先,用户上传到网盘的文件都是以明文状态上传，这样一来在文件的传输过程中很可能被黑客拦截接受，上传之后服务端也可以查看用户的文件。其次，很多网盘服务在文件上传过程中采用的是TCP链接服务，而这种服务通常开销较大，网咯波动对文件传输的速度会有较大影响。最后，客户会对其网盘内容进行进行搜索，而服务商可能会不经过授权，私自搜集用户数据用于自身分析。为了解决以上情况我们新的系统有以下功能。

1. 我们的系统在用户上传文件时先经过加密，密钥由客户端进行管理，这样就可以避免黑客获知上传文件的具体内容，同时也防止服务端私自查看用户文件内容，保护了用户的隐私。
2. 文件传输过程中采用的是UDP文件传输，之所以采用UDP文件传输是因为相比较TCP文件传输，UDP是无状态，消耗资源少以及速度稳定，在网络状况不好的情况下我们仍然可以维持一个不错的文件发送速度。
3. 为了解决服务端搜集用户搜索记录的情况，我们采用了加密搜索的相关技术。这种技术可以针对搜索时的关键字进行加密，从而服务端不会获知具体的搜索内容，用户的隐私也得到了保障。

2、课题