# 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。云存储是指将连在互联网的大量设备通过集群应用、网络技术或分布式文件系统串联起来，通过应用软件虚拟化这些网络设备对外提供数据存储和访问功能。云存储是指处理的事务是大量数据的存储与管理的云计算系统。

随着移动终端市场的兴起，人们现在通常拥有多种类型智能设备。不同类型的智能设备让我们生活和工作也变得十分便捷。而基于云存储的网盘系统更好的符合大众的需求，人们可以随时随地通过不同类型的设备查看和管理自己的文件。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。

# 2国内外现状

1网盘现状

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，其次用户在网盘使用中对自身数据进行检索时，网盘并没有对用户搜索信息进行加密，这样有可能造成用户的部分信息泄露，对数据存储的安全也造成了很大的挑战。因此一个既能安全存储用户数据又能支持对搜索记录加密的网盘是符合用户需求的。

基于以上需求，我们提出了一个新的网盘系统模型，相比较于之前的网盘系统模型，新的模型具有以下的优点。

一、新的网盘系统在文件上传之前会先进行加密，文件下载后在本地进行解密，文件加密解密的密钥由用户自身保管。确保了用户文件存储的安全性和隐私性。

二、网盘系统引进UDP文件传输方式，将大文件分片传输，后续对文件片进行校验更是确保文件传输过程的安全与完整性。

三、针对加密文件的索引，我们引入可搜索加密技术。可搜索加密（searchable encryption, SE），可搜索加密允许用户在密文上进行关键字查找，使用这种方式来处理用户的检索信息可以保证用户搜索时的隐私。

四、针对用户的不同文件，我们提供了对部分文件支持版本控制的功能。这样对一些重要的文件可以追踪其版本，如果用户不小心删除或者修改就可以回溯到之前的版本。

2加密搜索

加密搜索，又称可搜索加密（searchable encryption, SE），可搜索加密主要解决在服务端不完全可信的情况下对加密数据的关键字安全搜索。2000年，Song等人首次提出可搜索加密的概念。在借助这一技术下，用户借用服务器强大的计算资源进行关键字查询同时不会向服务器泄露任何隐私信息。这种模式下，不仅仅保护了用户数据的隐私，也防止他人窃取用户的信息，最后还能极大的提高对加密数据的查询效率。

可搜索加密发展历史。。。

3创新点分析

1. 首次将加密搜索引入到网盘系统中，并实现该系统。
2. 对加密搜索过程中搜索算法进行改进。