各位老师大家好，我们组的项目叫做“基于Fuse的用户自主式加密云存储系统”。屏幕上是我们经常使用的几款云存储软件，众所周知，目前比较主流的云存储的软件都或多或少地存在着安全性的问题，大家应该都听说过前一阵的iCloud泄露事件，可想而知，我们存储于云盘的个人隐私信息数据存在着怎样的风险，而我们的创意由此而生，我们在想可不可能以一种类似“银行保险柜”的形式向用户提供“电子数据保险柜”的服务，而服务提供者就像银行这样的权威机构，这样就能更高程度的提高用户的安全感。基于这样的想法，我们的系统由此而生。以下我将从四个方面来展示今天内容。

第一部分：项目概况。我们的系统是基于windows平台的，这张图是我们的系统总体架构的示意图，一般的windows系统的软件在文件交互上都是直接与windows的io系统进行交互，而我们的系统是在软件与io系统进行交互时，加入了FUSE，而我们也将加密算法注入于fuse系统中，用户在调用windows io方法时，会首先调用fuse的io方法，之后将处理结果返还给系统IO。这是我们的客户端部分，箭头与虚线相连，这是一般的windows应用程序部分，箭头是和io直接相连，可见两者之间的差别。这样的处理可以实现用户在进行文件处理时实现加解密过程的无痕化。这一部分是客户端与云盘进行数据传输。

第二部分：技术路线，由前面的介绍，我们的系统主要是分这四个部分，fuse部分（FUSE的全称filesystem in userspace，用户空间文件系统，指完全在用户态实现的文件系统，FUSE的概念是来自于Linux，而windows有一款以FUSE的实现方式实现的开源软件叫做dokan，这也是我们使用的主要的工具之一），加密算法部分我们打算使用des加密算法（des加密算法是一种应用较为广发的比较成熟而且安全性较高的对称加密算法），客户端部分（我们打算使用qt的环境进行开发,以方便进行多平台编译）还有云存储部分我们打算使用Openstack，（openstack是美国NASA和Rackspace合作研发的开源项目，提供云存储和云计算的功能）。

第三部分：项目特色，在第一部分的介绍中，我提到过我们的系统是加解密过程是无痕的，能很好地保证用户的体验度。因为我们是在客户端加密所以服务器保存的数据是经过加密的密文。相比之下，一般的云存储系统都是未经加密直接上传到云，第三我们的密钥是不存储于任何物理介质上的，这也是我们系统的核心所在，因为密钥不管存储于任何物理介质上都有遗失的风险，如果被他人掌握就存在着不可估量的后果，简而言之我们的系统的安全性更高，用户使用的安全感更强。

第四部分就是我们的预期成果，第一是完成我们的应用系统的开发，第二是发表一篇核心期刊论文，第三获得软件著作权一项，第四项目总结报告一篇。

以上就是我今天讲的所有的内容，谢谢各位老师。

DES加密算法安全性：

DES算法具有极高安全性，到目前为止，除使用穷举搜索法对DES算法进行攻击外，未发现更有效的办法。而56位长的密钥的穷举空间为256，这意味着现阶段计算机需要上千年的时间才能搜索完全部密钥。