项目编号：

**吉林大学“大学生创新创业训练计划”**

**创新训练项目**

**申请书**

项目名称 基于FUSE的用户自主式加密云存储系统

项目负责人 陈阳

所在学院、年级、专业 软件学院13级软件工程

联系电话 18553358649

电子邮件  1427714873@qq.com

指导教师姓名1 陈伟 职称 副教授

指导教师姓名2 职称

填表日期 2015 年 04 月 15 日

**吉林大学教务处制表**

**填表须知**

一、**本表适用于创新训练项目**。本科生个人或团队，在校内导师指导下，自主完成创新性实验方法的设计、设备和材料的准备、实验的实施、数据处理与分析、总结报告撰写等工作。

二、申报书请按顺序逐项填写，实事求是，表达明确严谨。空缺项要填“无”。

三、申请参加大学生创新训练项目团队的人数为3—5人。

四、申请项目，必须聘请教师作为指导老师，并请指导教师在申请书中的指导教师意见栏中签署意见。

五、填写时可以改变字体大小等，但要确保表格的样式不变；不得随意涂改；A4纸正反面打印，左侧装订。

六、本表由项目负责人报所在学院初审，学院签署初审意见后报送教务处实习与实验教学科（一式3份原件）。

七、“项目编号”由教务处填写。

八、申报过程有不明事宜，请与教务处实践教学科联系，电话85166413。

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **项目名称** | | | **基于FUSE的用户自主式加密云平台系统** | | | | | | | | |
| 项目起止时间 | | | **2015年 05月 至 2016 年 04 月** | | | | | | | | |
| 负责人 | 姓名 | | 学院 | 专业 | 教学号 | 联系电话 | | E-mail | QQ | | 各类实验班 |
| 陈阳 | | 软件学院 | 软件工程 | 54130304 | 18553358649 | | 1427714873@qq.com | 1427714873 | | 是√ 否□ |
| 项目组成员 | 宋治佳 | | 软件学院 | 软件工程 | 54130511 | 18844546278 | | sz0hj@qq.com | 1131293579 | | 是□ 否√ |
| 尹嘉伟 | | 软件学院 | 软件工程 | 54130317 | 15500020227 | | 1030645870@qq.com | 1030645870 | | 是□ 否√ |
| 肖君 | | 软件学院 | 软件工程 | 54120328 | 13134721395 | | 2324659524@qq.com | 2324659524 | | 是□ 否√ |
| 丁雪松 | | 软件学院 | 软件工程 | 54130426 | 15764352826 | | 1767794367@qq.com | 1767794367 | | 是□ 否√ |
| 指导教师1 | 姓名 | | 陈伟 | | | | | 职务/职称 | | | 副教授 |
| 所在单位 | | 吉林大学 计算机学院 | | | | | | | | |
| 联系电话 | | 13843027869 | | | | E-mail | | [chenw@jlu.edu.cn](mailto:chenw@jlu.edu.cn) | | |
| 对本课题相关领域研究情况 | |  | | | | | | | | |
| 指导教师2 | 姓名 | |  | | | | 职务/职称 | | |  | |
| 所在单位 | |  | | | | | | | | |
| 联系电话 | |  | | | | E-mail | | |  | |
| 对本课题相关领域研究情况 | |  | | | | | | | | |
| **项目性质** | | 1.小发明、小创作、小设计（ ）  2.开放实验室或实习基地中的创新性实验或新实验开发（ ）  3.基础性研究（ ） 4.应用性研究（√）  5.社会调研 （ ） | | | | | | | | | |
| **项目选题来源** | | 1.自主立题（√）  2.教师科研课题的子项目（ ） | | | | | | | | | |
| **项目学科类别** | |  | | | | | | | | | |
| **项目受其他渠道资助情况**（填“无”或具体资助来源和经费，包括获奖情况） | | 无 | | | | | | | | | |
| 1. **立项背景和依据**（包括研究目的、国内外研究现状分析与评价、研究意义，应附主要参考文献及出处）   **研究目的**  随着网络的迅速普及，云存储成为了人们日常生活和工作中不可分割的一部分。无论音乐分享、网络通讯录还是文件存储，资料、密码等数据，都开始从本地硬盘向服务器“云端”转移。大量的敏感信息在网络中通过有线或无线等方式在网络节点之间传递，越来越多的用户数据存储在各种网络服务器中**[1]**。对于不法分子、企业甚至政府而言，这些隐私数据极具价值。这些数据一旦被窃取，用户个人隐私、经济财产将受到极大威胁。而目前尚无相关的法律法规来保障用户的数据财产安全。这时如果有一个权威机构——银行以类似于“电子数据保险柜”的形式来提供保障用户数据安全的服务，那么就可以使个人隐私信息的安全性得到更完善的保障。  这种服务可以基于一个在数据通过网络传输过程前对该数据于用户本地进行数据加密并上传到银行“私有云”的系统，于用户本地进行加密可以使用嵌入加密算法的FUSE系统进行实现，“私有云”可以使用OpenStack进行搭建，通过本地客户端将两者结合在一起，这样就可以避免数据在网络节点之间传输或在云端存储时被窃取。  **国内外研究现状分析与评价**  “云存储”是在“云计算”概念上延伸和发展出来的一个新的概念，是一种新兴的网络存储技术，是指通过集群应用、网络技术或分布式文件系统等功能，将网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供数据存储和业务访问功能的一个系统**[2]**。  目前国外主流云存储软件有iCloud、OneDrive、Google Drive等，国内主流云存储软件有百度网盘、360云盘、金山快盘等，而这些软件的“云端”大多是使用美国NASA和Rackspace合作研发并发起的开源项目——OpenStack搭建的。它们的共同点是都提供了提供多元化数据存储服务、大容量的存储空间，用户可以在不同地点、不同设备上上传和下载文件。但当所欲存储的数据较为机密时，则对存放于云存储服务提供商的安全性有疑虑**[3]**。  用户空间文件系统（Filesystem in Userspace，简称FUSE）是操作系统中的概念，指完全在用户态实现的文件系统。文件系统是一个通用操作系统重要的组成部分。传统的操作系统在内核层面上对文件系统提供支持。而通常内核态的代码难以调试，生产率较低。FUSE不需要了解文件系统的内幕和内核模块编程，能够大幅提高生产率**[4]**，简化了为操作系统提供新的文件系统的工作量，特别适用于各种虚拟文件系统和网络文件系统。  目前在国内外，DES加密算法在POS、ATM、磁卡及智能卡（IC卡）、加油站、高速公路收费站等领域被广泛应用，以此来实现关键数据的保密，如信用卡持卡人的PIN的加密传输，IC卡与POS间的双向认证、金融交易数据包的MAC校验等，均用到DES算法。DES成为世界范围的数据加密标准以存在多年。其前身是由IBM公司的一个研究小组研制的Lucifer密码算法。在此基础上，经过3年多的研究，不断正价密码强度，最终完成了该算法的设计和编制。在DES算法中，用到了两个加密的基本技术：混乱和扩散。其基本组件分组是这两种技术的组合。DES采用了标准的算术和逻辑运算，系统的安全性由密钥保证**[5]**。  目前，上述三种技术在国内外均取得了一定的应用上的成功，但鲜有将上述三种技术结合起来，用以保障隐私数据在各个网络节点间传输和服务器上存储的安全性的系统。其中杭州奕锐电子公司所开发的“隐形云”在一定程度上结合了上述三种技术，一定程度上完成了上述目标，但是，该系统有诸多不足之处，如软件主体使用JAVA编写，其源码可以轻易通过反编译的手段获得；密钥存储于本地且发送到用户邮箱，存在密钥泄露的风险；该软件为程序级别的加密，而非于文件系统层面进行加密，对文件的操作并不够灵活，等等。这些方面都还有进一步完善的余地。  **研究意义**  随着互联网的发展和普及，云存储必将被越来越多的人所使用，“云端”数据的安全性也将变得尤为重要。开发基于用户文件系统的用户自主式加密云平台系统能够满足人们日益增长的对于数据隐私安全的渴望，方便人们的日常生活，避免数据在网络节点之间传输或在云端存储时被窃取，被不法分子所利用，导致用户个人隐私泄露、经济财产遭受极大损失。因此该系统对于用户的日常生活中的数据隐私来说，意义重大。  **主要参考文献出处**  **[1]** 芦天亮，周运伟，刘颖卿。网络用户隐私泄露问题综述。2014 第10A期  **[2]** 刘鹏，罗圣美，赵淦森。 中国云存储发展报告。  **[3]** ZDNet, Nasuni Cloud Storage Gatewa技术的分组y By Dan Kusnetzky, June 1, 2010  **[4]** Sumit Singh, Software Engineer, IBM. Develop your own filesystem with FUSE. October 2014  **[5]** 王立胜，王磊，顾训穰。Analysis and Attack Research of DES Cipher ，August，2003 | | | | | | | | | | | |
| **二、项目研究内容**（项目主要研究内容；拟解决的关键问题、重点和难点）  **研究内容**   1. **用户文件系统在本机的搭建：**   拟通过使用Windows平台下的开源用户文件系统——Dokan来实现在Windows端的用户文件系统的搭建。搭建时主要需要完成的是Dokan Library库的实现，即对文件的新建、读写、复制、剪切等功能进行实现。   1. **加密算法在用户文件系统上的实现：在本地实现云端数据的加解密**   加密算法在用户文件系统上的实现主要是为了文件在通过系统I/O通道时，DES加密模型使用一串长度为64位的字符型密钥对文件编码进行具有一定规律性的转换，这样原有文件在通过I/O通道后就会转换成内容无规则的密文。  当用户文件系统启用时，文件在通过I/O通道时会经过该用户文件系统。拟将加密算法嵌入到用户文件系统的读写操作中，同时用户文件系统改变原有文件流流向以实现加解密目的。  **3. “云端”服务器的部署与搭建：**  用OpenStack中的nova-network来分配ip地址、配置虚拟网络和通信使主机之间以及与外部网络互相访问。用OpenStack中的Cinder组件来管理和分配“云端”服务器的存储空间。通过Controller节点来管理整个OpenStack“云端”服务器各个节点之间的配合和运作。同时使用OpenStack的Nova节点使“云端”服务器能够完成各种复杂情况下的计算任务。  **4. 本地客户端的实现：**  本地客户端拟使用C++进行编写，通过调用FUSE文件系统的相关API实现文件的相关操作；使用Qt Creator实现客户端界面，便于项目日后跨平台开发；通过FTP或SSH网络传输协议实现与服务器端的联接。  **拟解决的关键问题、重点和难点**  **1.Dokan中I/O系统的实现：**  Dokan包含一个用户模式Dokan Library(dokan.dll)和内核模式文件系统驱动程序(dokan.sys)。一旦Dokan文件系统驱动程序启动，就可以创建一个与Windows端文件系统类似的用户文件系统。当文件操作请求被发送到Windows I/O内核时，该请求会被转发到Dokan文件系统，此时会调用Dokan Library中的方法来执行该请求。  Dokan是一个开源项目，开源部分提供了文件系统的驱动程序（dokan.sys）,而Dokan Library需要开发者自行实现。文件操作需要通过调用Dokan Library中的I/O方法来代替Windows内核的I/O操作。实现Dokan Library中的I/O部分的过程中会涉及到对Window底层操作，Windows提供的API使得实现该部分内容变得灵活却复杂。  **2.****在Dokan中嵌入DES加密算法：**  DES对64位(bit)的明文分组M进行操作，M经过一个初始置换IP，置换成m0。将m0明文分成左半部分和右半部分m0 = (L0，R0)，各32位长。然后进行16轮完全相同的运算（迭代），这些运算被称为函数f，在每一轮运算过程中数据与相应的密钥结合。在每一轮中，密钥位移位，然后再从密钥的56位中选出48位。通过一个扩展置换将数据的右半部分扩展成48位，并通过一个异或操作替代成新的48位数据，再将其压缩置换成32位。这四步运算构成了函数f。然后，通过另一个异或运算，函数f的输出与左半部分结合，其结果成为新的右半部分，原来的右半部分成为新的左半部分。将该操作重复16次。经过16轮迭代后，左，右半部分合在一起经过一个末置换（数据整理），这样就完成了加密过程。解密过程也遵循以上相同的流程。  将DES加密算法嵌入到Dokan文件系统中，可以使加密过程无痕化，用户使用时不用对加解密过程做任何多余的操作，使整套系统更加人性化。但在完成加密算法嵌入Dokan文件系统时存在几个难点：  （1）使用C++准确的实现上述加密算法的加解密过程。  DES算法不依托于任何的实现语言，它本身是一种实现文件加密和解密的方法。用C++实现该算法，并且使该加密算法准确运行，能保证功能的完整行和可靠性，这本身具有一定的难度。  （2）实现加密算法与Dokan方法的结合。  Dokan是基于Windows API完成的，通过Dokan进行的所有操作都是直接和Windows系统底层进行交互，将加密算法嵌入Dokan的I/O方法中，就可能会影响到整个系统的正常工作，甚至导致系统崩溃。因此在加密算法嵌入过程中，每一个细节都必须要谨慎。  **3.部署与配置服务器端的环境**  服务器是基于OpenStack搭建的，OpenStack的6个组件支撑起了OpenStack的主要功能，它们分别为：Nova组件、Keystone组件、Dashboard组件、Glance组件、Quantum组件、Swift组件、Cinder组件。  在服务器端OpenStack的搭建过程中，Nova、Quantum、Cinder这三个组件是搭建过程中的重点与难点。因此，在搭建过程中确保上述三个组件的正确搭建是保证OpenStack正常运行的关键。  此外，OpenStack配置相对复杂，并且在配置过程中需要考虑许多影响配置的因素。当用户数量较多时，OpenStack的配置会有所不同；在配置过程中需要考虑对OpenStack进行分区以适应多个服务器端甚至是多家银行或者是多家提供服务的机构进行数据的存储。  **4.保证系统的高安全性和可靠性**  本系统操作的数据都是用户的隐私数据，所以对这些数据的操作必须保证其完整性和保密性，这对本系统的安全性和可靠性是极大的考验。因此，该系统必须有详细的测试计划和完整的测试方案。比如说普通文本文件的测试，各种流媒体文件的测试，100k以下小型文件的测试，1G以上大型 | | | | | | | | | | | |
| **三、项目特色及创新点**  **项目特色**  **1.**传统云盘大多没有加密功能，少数具有加密功能的云盘也是在“云端”对数据进行加密，一方面数据可能在传输过程中泄露。另一方面，数据可以被服务器的管理运营商所获取，用户的隐私数据可能被运营商利用。本系统于用户本地对数据进行加解密，不仅保障了数据在“云端”服务器的安全，而且避免了数据在网络节点间传输时被窃取的可能，增加了系统整体安全性。  **2.**目前国内外具有加密功能的主流云盘，其加解密时由服务器生成密钥并保存在服务器，一旦服务器被不法分子侵入，存在密钥和数据一并被窃取的风险。本系统的加密密钥由用户自主输入，并不存于任何物理介质，即使服务器被非法入侵，不法分子也只能得到密文，而无法获得解密密钥。因此，用户的数据即使被窃取也依然安全。  **3.**本系统将加密算法嵌入FUSE，并将FUSE通过本地客户端与OpenStack联接起来，形成一整套完整的系统，这种形式上的创新与突破是国内外鲜有的。  **创新点**  **1.**将加密算法嵌入于FUSE文件系统中，使文件通过I/O通道时，以用户提供的密钥进行了加解密。这样的组合是传统云盘在本机的客户端所不具备的。  **2.**具有加密功能的云盘将密钥存储于物理介质，而本系统不将密钥存储于任何的物理介质上，保证了密钥不被窃取。  **3.**使原本不具有本质联系的FUSE和OpenStack进行了结合，并在FUSE上加以加密算法，产生了一个全新的更加可靠的加密云存储系统。 | | | | | | | | | | | |
| **四、申请理由**（1、团队条件——自身/团队具备的知识、素质、能力、特长、兴趣；2、前期准备基础等）  **团队条件**  **陈阳：**软件学院卓越班成员，曾参加过于郑州举办的计算机学术交流大会，大二寒假期间曾到大连东软实习。编程能力突出，对于软件工程、代码的整洁性和重构有一定的兴趣与认识，在设计模式方面具有自己独特的认识和理解，对于一些课程的学习领先于同届大多数同学。  **宋治佳：**曾获得蓝桥杯省赛一等奖，具有优秀的代码实现能力。接受新事物能力强，具有独特的想象力。对于敏捷开发和Linux服务器方面有浓厚的兴趣和初步的了解。在程序架构的分析与设计方面有一定的了解与认识。  **尹嘉伟：**年级前五，在蓝桥杯等比赛中获得奖项，积累了较多编程经验，动手能力强，思维活跃，对事物有较强的总结能力。熟练掌握C、C++等语言编程并且对数据结构，算法等有一定研究，在以往课程设计中得分均为优秀，专业知识丰富。  **肖君：**年级排名前五，课程设计成绩优秀，学习能力强，思维很有跳跃性、富有创新性，擅长整理分析问题，对C、C++、JAVA编程均较为熟练，对操作系统、计算机网络等领域的知识均有一定的了解，专业知识丰富。  **丁雪松：**学习能力较强，思维活跃，具有独特的想法与创新能力，办事专注认真，对于C、C++、Java均有不同程度的了解。对于前端有浓厚的兴趣，对该领域有一定了解与认识并初步掌握了一定的前端知识。  **前期准备**   1. 查阅了国内外关于云加密的现状，对项目的整体可行性做出结论。 2. 初步学习了OpenStack的搭建、用户文件系统以及Windows编程的知识。 3. 查阅了国内外相关文献，了解了国内外主流的加密算法。 | | | | | | | | | | | |
| **五、项目实施方案**（研究思路和方法，实施计划、技术路线、人员分工等）  **研究思路和方法：**  本项目从三方面进行研究:   1. FUSE文件系统:通过对Dokan Library库的二次开发，并且在读写方法中嵌入加解密算法。实现文件的本地加解密。 2. 本地客户端：本地客户端拟使用Qt Creator完成前端UI的设计和制作，程序后端使用C++进行开发。 3. OpenStack服务器端：使用OpenStack的Cinder组件来搭建私有云空间，使用Quantum组件来进行网络相关内容的管理。   **技术路线：**    （1）用户登录操作：  系统启动时，用户在客户端端输入账户密码，通过客户端后端拟通过FTP或者SSH传输协议将账户和密码上传到OpenStack服务器，通过KeyStone组件进行用户身份信息的确认并返回登陆信息和文件列表索引，拟使用XML进行用户文件索引。  （2）上传文件操作：  用户在登录系统之后，通过客户端UI选择需要上传的文件，并且提供加密算法的密钥。客户端后端将文件和加密算法密钥提供给FUSE文件系统。  FUSE文件操作系统通过DES加密算法对用户所选取的文件进行加密。FUSE文件系统将密文放入虚拟磁盘**，**客户端后端将密文文件通过FTP或者SSH协议将密文上传到OpenStack服务器端。  OpenStack服务器端将更新后的云端文件列表返回到本地客户端后端，显示在客户端UI上。  （3）下载文件操作：  用户在登陆系统之后，通过客户端UI选择所需要下载的文件，并且提供加密算法的密钥。客户端后端下载请求发送给OpenStack服务器。  OpenStack获取到请求，通过XML获得用户所选取的文件通过FTP或者SSH协议将密文文件传输给本地客户端后端，后端将密文文件和解密密钥提供给FUSE文件系统进行解密过程。  FUSE文件系统通过DES解密算法对密文文件进行解密，并将解密后得到的文件回传给后端，后端将文件写到用户指定的位置。  **实施计划:**  1.调研查阅相关文献，熟悉Dokan，OpenStack，DES加密算法以及虚拟磁盘、  2.在进一步整理分析系统要求的基础上完成系统的概要设计。  3.完成详细设计，同时制定测试计划。。  4.完成功能实现。  5.做充分测试优化额完善。  6.整理开发资料，撰写项目总结报告，撰写论文。  **人员分工：**  1.系统调研：陈阳，宋治佳，尹嘉伟，肖君，丁雪松。  2.概要设计：陈阳，宋治佳，尹嘉伟。  3.详细设计：陈阳，宋治佳，尹嘉伟，肖君。  4.设计测试用例：丁雪松，肖君。  5.开发，分组：  ① OpenStack服务器端：宋治佳，陈阳。  ② FUSE系统：尹嘉伟，陈阳。  ③ 本地客户端：肖君，丁雪松。  ④ 加密算法：尹嘉伟，肖君。  6.整理开发资料，撰写论文、项目总结报告：陈阳，宋治佳，尹嘉伟，肖君，丁雪松。 | | | | | | | | | | | |
| **六、项目进度安排**（文献查阅、社会调查、方案设计、开题报告、实验研究、数据处理与分析、研制开发、填写结题表、撰写论文和研究报告、结题答辩和成果推广等时间安排）  2015年02月 - 2015年05月：项目的前期调研考察，具体了解国内外现状和相关情况。  2015年05月 - 2015年07月：项目正式启动，相关专业知识的了解与学习。  2015年07月 - 2015年12月：项目整体实施，对具体功能的实现。  2015年12月 - 2016年03月：项目的后期测试、优化与完善。  2016年03月 - 2016年04月：项目总结，撰写论文与研究报告。 | | | | | | | | | | | |
| **七、项目研究所需资源**（实验室、仪器设备、实验材料、资料等）  **实验室:**可以依托软件学院实训基地进行实验，测试等工作。  **仪器设备：**指纹识别相关设备，小型服务器。  **资料：**关于Windows开发、数据库、服务器、OpenStack、用户态文件系统、加密算法等相关书籍和资料。 | | | | | | | | | | | |
| **八、项目经费预算与用途**（购置实验消耗材料、低值品、资料、加工测试、打字复印、调研、市内公交、论文发表、专利申请等经费开支）  **1.**实验消耗材料:4.5千元  **2.**资料与相关书籍:1千元  **3.**打字复印:0.5千元  **4.**市内公交费：0.5千元  **5.**软件著作权费用：0.5千元  **6.**论文发表:3千元  **合计:1万元** | | | | | | | | | | | |
| **九、项目完成预期成果**（成果形式：研究论文、专利、设计、产品、软件、研究或调研报告等）  **1.产品：**  基于FUSE的用户自主式加密云存储系统  **2.论文：**  \*\*\*公开发表核心期刊论文1-2篇（写上的东西必须达到，万一没评上国家级。。。）  **3．软件著作权：**  取得软件著作权1项  **4. 项目总结报告：**  项目总结报告1篇 | | | | | | | | | | | |
| **十、项目诚信承诺**  **本项目负责人和全体成员郑重承诺：该项目研究不抄袭他人成果，不弄虚作假，按项目研究进度保质保量完成各项研究任务。**  项目负责人签名： 年 月 日  项目组成员签名：  年 月 日 | | | | | | | | | | | |
| **十一、指导教师意见**（从项目科学性、前沿性、可行性、研究性、可操作性和成效性进行评价，是否同意立项）  签 名：  年 月 日 | | | | | | | | | | | |
| **十二、学院评审意见**（学术价值、预期效果、研究方案可行性、是否同意立项）  工作组组长签名（公章）：  年 月 日 | | | | | | | | | | | |
| **十三、校专家组评审意见**  专家组组长签名：  年 月 日 | | | | | | | | | | | |
| **十四、学校意见**  领导小组组长签名（公章）：  年 月 日 | | | | | | | | | | | |