**第二组-锟斤拷烫烫烫**

**文件加密软件需求文档**

**1.典型用户与场景**

**1.1典型用户1 （高管）**

|  |  |
| --- | --- |
| 名字 | X先生 |
| 性别、年龄 | 男 35 |
| 职业 | A公司高管 |
| 收入 | 5w /month |
| 知识层次和能力 | 世界top50名校毕业，行政管理能力突出 |
| 生活/工作情况 | 工作状态良好 |
| 动机、目的、困难 | 希望输入账号和正确的密码后即可进入信息安全系统，不希望出现差错 |
| 用户偏好 | 访问与管理文件 |
| 用户比例 | 10%以内 |
| 典型场景 | 独立办公室 |

典型场景：

X坐在办公室里，准备处理一些重要文件。X打开电脑，输入了X的账号和密码。系统验证了X的身份，并且确认了X有权访问该系统中存储的所有文件。

一旦X成功登录信息安全系统，X可以使用搜索功能来查找特定文件或者浏览整个目录结构。如果X需要修改某个文件或者新建一个文件夹，只需单击鼠标即可完成操作。

当X完成工作后，记得及时退出信息安全系统并锁定电脑屏幕，以确保公司机密不会被未经授权的人员访问。

功能点

1. 软件登录UI层：

提供账号和密码输入框，允许用户输入账号和密码。

验证用户输入的账号和密码是否正确，并且确认用户有权访问该系统中存储的所有文件。

如果验证通过，则将用户重定向到主界面；如果验证失败，则提示用户重新输入或联系管理员。

2. 数据库：

存储公司机密文件，包括文件名、文件路径、文件大小、修改时间等信息。

存储用户信息，包括用户名、密码、权限等信息。

3. 逻辑层：

处理用户输入的账号和密码，与数据库中存储的信息进行比对，并返回验证结果。

提供搜索功能，允许用户查找特定文件或者浏览整个目录结构。

处理用户新建文件夹或修改某个文件的请求，并更新数据库中相应的记录。

提供注销功能，允许用户退出信息安全系统并锁定电脑屏幕。

**1.2典型用户2（转正职员）**

|  |  |
| --- | --- |
| 名字 | 黄婉婷 |
| 性别、年龄 | 女 24 |
| 职业 | 公司转正职员 |
| 收入 | 6000 /month |
| 知识层次和能力 | 普通一本毕业，能力一般 |
| 生活/工作情况 | 刚刚转正，需要注册公司的内部管理系统 |
| 动机、目的、困难 | 希望通过注册获取身份，注册成功后只需账号密码登录即可，以便于登录账号进行访问与管理文件，不擅长繁琐的流程 |
| 用户偏好 | 喜欢摸鱼，想要工作更快捷 |
| 用户比例 | 20%以上 |
| 典型场景 | 办公室 |

典型场景：

你是一家刚刚成立的科技公司的转正女职员，你负责公司内部文件的管理和分享。而正巧，你因为公司有一个简单的注册登录系统而欣喜。

首先，在公司内部网站上有一个注册页面，用户可以在该页面填写基本信息并提交。为了减少繁琐的流程，只要求用户输入必要的信息，如姓名、邮箱、密码等。提交后，系统会自动发送一封验证邮件到用户填写的邮箱中，用户只需点击邮件中的链接即可完成账号激活。

一旦用户或管理员成功注册并登录，他们就可以访问公司内部网站上的文件库了。为了保证文件安全性，管理员设置了不同的权限等级。普通用户只能查看和下载文件，而管理员还可以上传和删除文件。

总之，通过这个简单的注册登录系统，用户和管理员都可以轻松地访问和管理公司内部文件库。同时也保证了文件的安全性和隐私性。

功能点：

UI层：

1. 注册页面：提供用户输入账号和密码的表单，以及注册按钮。

2. 文件管理页面：显示当前用户可以访问的文件列表，并提供上传、下载、删除等操作。

数据库：

1. 用户信息表：存储所有已注册用户的账号和密码信息。

2. 文件信息表：存储所有文件的相关信息，如文件名、上传者、上传时间等。

逻辑层：

1. 注册逻辑：当用户在注册页面填写完账号和密码并点击注册按钮时，系统将检查该账号是否已经被注册过。如果未被注册，则将该账号和密码信息保存到用户信息表中；否则提示用户该账号已存在。

2. 文件管理逻辑：根据当前登录用户的身份，在文件信息表中查询该用户可以访问的文件列表，并在文件管理页面中展示出来。同时，还需要实现上传、下载、删除等操作。在进行这些操作时，需要对文件进行权限控制，确保只有具备相应权限的人才能进行操作。

**1.3典型用户3（会计）**

|  |  |
| --- | --- |
| 名字 | 刘姐 |
| 性别、年龄 | 女，33 |
| 职业 | A公司会计 |
| 收入 | 1.5w/month |
| 知识层次和能力 | 中专毕业，有高级会计师职称 |
| 生活/工作情况 | 家庭和睦，公司账目基本经她过目 |
| 动机、目的、困难 | 在使用文件加密系统的过程中，可以自由地访问、删除、修改、移动、复制、创建、搜索文件，以便  对公司的文件进行快捷处理，不擅长记住目录 |
| 用户偏好 | 做完账后分类存 |
| 用户比例 | 10%左右 |
| 典型场景 | 查账 |

典型场景：

你在电脑上打开文件夹，准备查看最近的财务报表。由于该文件夹被加密，在双击打开之前，系统要求你输入密码进行验证。验证通过后，你可以自由地访问、删除、修改、移动、复制、创建、搜索文件。

首先，你使用搜索功能快速找到了最新的财务报表，并复制到了一个新的文件夹中。然后，你对该报表进行了细致的阅读和分析，并发现其中有一些错误。因此，你使用修改功能对报表进行了修正，并保存在原来的位置。

接着，你需要将修正后的报表发送给其他部门的同事进行审核。为了方便起见，你将该报表复制到一个共享文件夹中，并设置相应权限以确保只有授权人员可以访问。

过一段时间后，你接到了领导的电话要求提供某个月份的财务数据。由于之前已经创建过该月份的数据报告，所以你直接在原来的位置上创建新的报告并填写相关数据即可。

最后，在完成任务后，你使用删除功能将不再需要的旧报告从系统中删除，以保证系统的整洁和安全性。

功能点：

UI层：

1. 文件夹浏览页面：提供用户自由访问、删除、修改、移动、复制、创建、搜索文件的功能

2. 文件共享页面：提供用户设置文件权限和共享的功能

逻辑层：

1. 密码验证逻辑：对用户输入的密码进行验证

2. 文件操作逻辑：实现自由访问、删除、修改、移动、复制、创建、搜索文件等功能

3. 共享权限逻辑：实现对共享文件夹中的文件设置权限和共享

数据库：

1. 用户表：存储用户信息，包括用户名和密码等

2. 文件夹表：存储所有文件夹的基本信息，例如名称和路径等

3. 文件表：存储所有文件的基本信息，例如名称和路径等

4. 权限表：存储每个用户对每个文件或文件夹的访问权限和共享权限等信息。

**1.4 典型用户4 （开发人员）**

|  |  |
| --- | --- |
| 名字 | 李明 |
| 性别、年龄 | 男，33 |
| 职业 | 资深开发人员 |
| 收入 | 40w/year |
| 知识层次和能力 | 精通主流语言，擅长写框架 |
| 生活/工作情况 | 喜欢呆在办公室，宁愿加班看日志记录也不想回家 |
| 动机、目的、困难 | 希望任何用户（包括管理员）在信息安全系统中的任何操作都被系统自动记录并保存在一个不能被修改的日志文件中，并可以被任何人查看。以便确保信息安全系统的使用与管理清晰透明，进一步加强其安全性。 |
| 用户偏好 | 信息安全系统的使用与管理清晰透明 |
| 用户比例 | 30%左右 |
| 典型场景 | 办公室 |

典型场景：

李明是该公司的一名管理员，他负责管理信息安全系统并确保其正常运行。今天早上，他收到了一份来自IT部门的报告，称有员工在信息安全系统中进行了异常操作。李明立即打开信息安全系统的日志文件，并搜索有关该员工的记录。

他发现该员工在昨晚登录了信息安全系统，并尝试访问与其职位无关的文件夹。虽然该员工没有成功访问这些文件夹，但这种行为仍然违反了公司的规定。李明决定将此事通知公司领导并采取必要措施。

由于信息安全系统已经自动记录了所有操作并保存在一个不能被修改的日志文件中，李明能够轻松地找到有关该员工的记录，并证实了其异常行为。这不仅有助于加强公司对信息安全系统的管理和监督，还能预防类似事件再次发生。

功能点：

UI层：

1. 提供登录界面和主界面，允许用户输入用户名和密码进行身份验证并访问系统。

2. 在主界面上显示所有文件夹和文件，并允许用户对其进行操作。

3. 提供一个日志查看器，允许管理员查看所有操作记录。

4. 在日志查看器中提供搜索功能，允许管理员根据关键字搜索特定记录。

逻辑层：

1. 实现用户身份验证功能，确保只有经过授权的用户才能登录并访问系统。

2. 实现全局日志记录功能，自动记录所有操作并保存在一个不能被修改的日志文件中。

3. 实现搜索功能，允许管理员根据关键字搜索特定记录。

数据库：

1. 存储所有文件夹和文件的元数据，并确保它们与实际文件系统同步。

2. 存储所有操作记录，并确保它们与实际操作同步。

**1.5 典型用户5 （高管）**

|  |  |
| --- | --- |
| 名字 | Y先生 |
| 性别、年龄 | 男，40 |
| 职业 | B公司高管 |
| 收入 | 5w/month |
| 知识层次和能力 | 国内C9硕士毕业，能力突出 |
| 生活/工作情况 | 工作状态良好 |
| 动机、目的、困难 | 希望 限制人员访问我司的文件，采用我司指定的加密算法  以便 保证用户的文件安全 |
| 用户偏好 | 采用公司指定的加密算法 |
| 用户比例 | 10%左右 |
| 典型场景 | 访问 |

典型场景：

张总是A公司的高管，他需要监控和管理公司内部的敏感文件访问情况，以确保公司机密信息得到充分保护。

1. 张总登录到A公司信息安全系统，并进入管理界面。

2. 系统提供了敏感文件访问情况的概览和详细信息。张总可以查看不同员工对不同文件的访问记录，包括时间、地点、操作类型等。

3. 如果系统检测到某个员工进行了异常操作（比如尝试多次访问未授权的文件），系统会自动向张总发送警报信息，以便及时采取措施。

4. 张总可以对不同员工的权限进行管理，包括添加或删除授权、修改权限范围等。这样可以确保只有经过授权的人员才能访问敏感文件。

5. 如果需要更新加密算法或其他安全策略，张总可以通过管理界面进行设置，并通知相关人员进行相应调整。

功能点：

UI层：

1. 在主界面上，提供敏感文件访问情况的概览和详细信息，以及权限管理等功能入口。

2. 在权限管理界面上，允许高管添加或删除授权、修改权限范围等操作。

逻辑层：

1. 实现对敏感文件的加密和解密操作，并采用A公司指定的加密算法。

2. 记录每个员工对不同文件的访问记录，并进行异常检测和警报发送。

3. 实现权限管理功能，确保只有经过授权的人员才能访问敏感文件。

数据库：

1. 存储员工信息、文件信息、授权信息等数据，并确保数据安全性和完整性。

2. 记录每个员工对不同文件的访问记录，并支持查询和统计分析。

**1.6 典型用户6（数据库管理员）**

|  |  |
| --- | --- |
| 名字 | 张先生 |
| 性别、年龄 | 男，29 |
| 职业 | 数据库管理员 |
| 收入 | 1w/month |
| 知识层次和能力 | 某211大学毕业，能力扎实 |
| 生活/工作情况 | 工作情况良好 |
| 动机、目的、困难 | 希望 有一个控制用户访问的软件  以便 让相应的员工访问到正确的文件 |
| 用户偏好 | 设置用户独有的密钥库，便于管理用户访问 |
| 用户比例 | 15%左右 |
| 典型场景 | 数据库管理 |

典型场景：

张先生是一家大型企业的机密数据库管理员，他需要确保员工只能访问到他们被授权访问的文件。他使用了一个控制用户访问的软件来实现这个目标。

1. 张先生登录控制用户访问的软件，并进入权限管理界面。

2. 在权限管理界面上，张先生可以查看所有员工的信息和相应的权限范围。

3. 张先生可以添加或删除授权，并修改员工的权限范围。

4. 当新员工加入公司时，张先生可以为其分配相应的权限，并将其添加到系统中。

5. 当员工离开公司时，张先生可以删除其帐户并撤销其所有权限。

6. 张先生还可以查看每个员工对每个文件的访问记录，并进行必要的调整和警告操作。

7. 当员工尝试访问未经授权的文件时，系统会自动发送警报给张先生并记录该事件。

8. 张先生还可以定期生成报告以检查系统性能和安全性，并进行必要的更新和维护。

功能点：

UI层：

1. 提供登录界面和主界面，允许管理员输入用户名和密码。

2. 提供权限管理界面，允许管理员查看员工信息和权限范围，进行添加、删除和修改授权等操作。

3. 提供访问记录查询界面，允许管理员查看每个员工对每个文件的访问记录。

4. 提供报告生成界面，允许管理员定期生成系统性能和安全性报告。

逻辑层：

1. 实现用户登录验证功能，确保只有管理员可以进入系统。

2. 实现权限管理功能，包括添加、删除和修改授权等操作。

3. 实现访问记录查询功能，并将记录存储到数据库中以备查询。

4. 实现报告生成功能，包括数据收集、分析和展示等操作。

数据库：

1. 存储员工信息、权限范围和访问记录等数据。

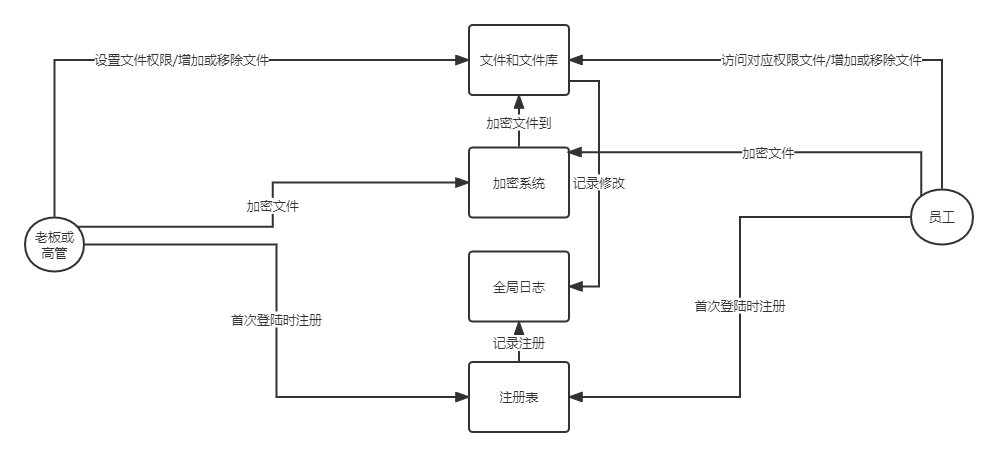
2. 提供数据查询接口，以便逻辑层能够获取所需数据。

1. **需求规格说明书**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 编写人 | 高凡、李佳宸 | 编写时间 | 2023.3.12 | 修订内容 | 编写源需求 |
| 修订人 | 高凡 | 修订时间 | 2023.3.17 | 修订内容 | 部分设计修缮 |
| 修订人 | 罗成勇 | 修订时间 | 2023.3.28 | 修订内容 | 登录需求修改并实现 |
| 修订人 | 高凡、李佳宸 | 修订时间 | 2023.5.11 | 修订内容 | 各项需求集中检查并实现，舍弃部分需求 |
| 修订人 | 李佳宸 | 修订时间 | 2023.5.16 | 修订内容 | 最后检查各项需求并汇总 |
| 修订人 | 李安南 | 修订时间 | 2023.5.20 | 修改内容 | 规范格式和做部分更正 |

需求规格说明书编写及修订记录

**2.1 产品总体业务流程图：**



**2.2 产品功能列表**

|  |  |  |
| --- | --- | --- |
|  | 功能名称 | 功能点 |
| 用户端 | 登录 | ·用户登录 |
| 注册 | ·用户注册 |
| 文件加解密 | ·加密文件  ·打开加密文件  ·关闭加密文件 |
| 文件操作 | ·文件上传  ·文件下载  ·文件删除（管理员独有） |
| 用户管理 | ·管理用户权限（管理员独有） |
| 系统管理端 | 全局日志记录 | ·读取日志文件 |

**2.3 功能详细描述：**

**2.3.1 登录**

**功能描述：**

用户通过系统类提供的可视化界面登入时，输入密码，用户类创建对象并调用login函数，通过访问注册表文件类来完成检索，确认用户是否匹配，若登入成功，运行系统类的消息响应函数，使界面刷新 ，从而调出相应可供用户操作的界面，在这个界面实现对后续任务的调用；如果登入不成功，消息响应函数将调动注册界面，管理员类管理用户相关数据时，登入和注册时的相关逻辑与用户相似，但是在运行管理员类时，系统类的消息响应函数将调用不同的登入和注册界面，以确保管理员身份的真实性，管理员注册需要额外输入密钥 （这应该是提前在系统类中录入过的密码），管理员类将调用用户类，用户类再访问注册表类，对注册表文件进行修改。同样地，管理员的行为痕迹也将被日志类记录并以文件形式输出。

**输入项目**

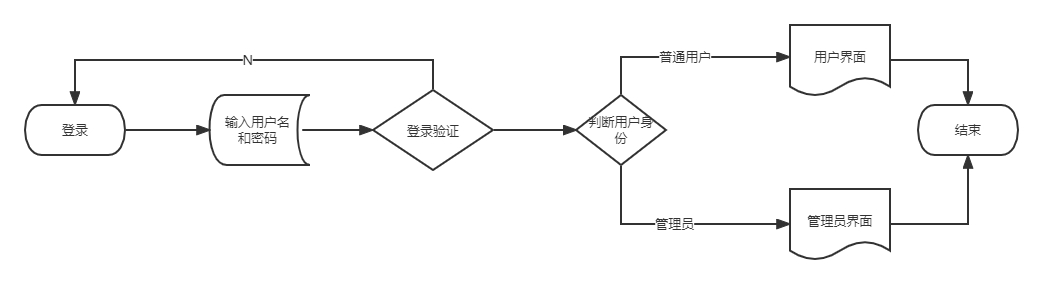
1.用户名

2.密码

**校验项目**

1. 用户名：检验文件库中是否有该用户名

**登录流程图**



**预计所需时间和投入人员**

所需2天完成，投入一名小组成员

**2.3.2注册**

**功能描述**

用户通过点击注册链接进入到注册页面，注册只需填写邮箱、密码、昵称、选择身份即可，注册成功将从注册界面跳转回登陆界面，注册界面将记录用户输入的数据生成一个新账户

**输入项目**

1.姓名

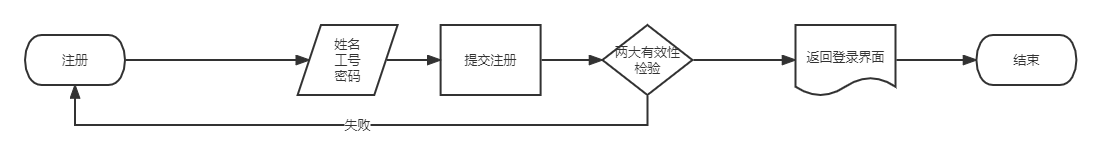
2.工号

3.密码

**校验项目**

1. 姓名 姓名合法性校验
2. 工号 工号唯一性检验

**注册流程图**

****

**预计所需时间和投入人员**

所需5天完成，投入一名小组成员

**2.3.3文件加解密**

**2.3.3.1加密文件**

**功能描述**

当用户对一个文件加密时，文件管理系统将根据用户设置的密码生成128位密钥，AES加密算法将利用128位密钥通过字节代换、行移位、列混和、轮密钥加实现明文的加密操作，并将密文替换原有文件中的明文。用户所设置的密码应当附有文件路径属性和权限属性，以便未来访问文件时调用（用户创建的密码权限等级与用户当前权限等级一致）

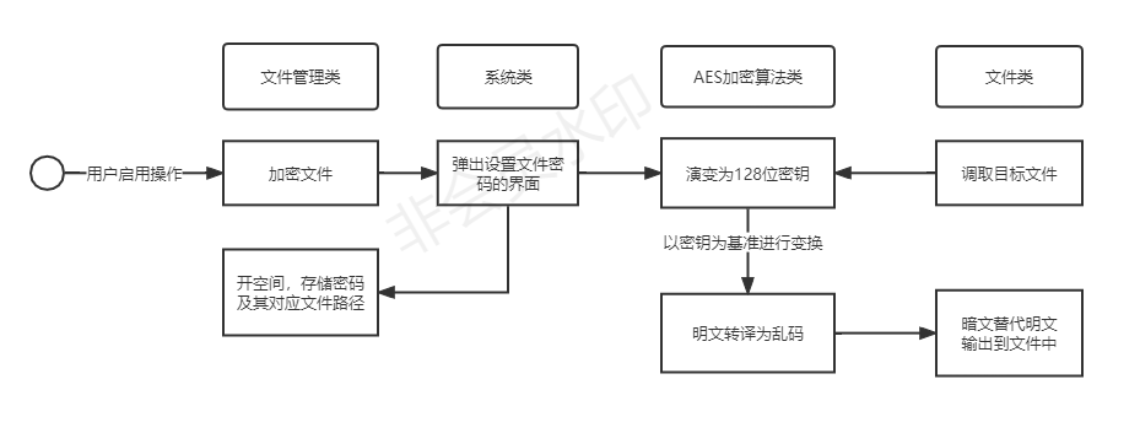
**输入项目**

文件路径

**校验项目**

文件路径 是否合法且存在该文件

**加密流程图**



**预计所需时间和投入人员**

所需10天完成，投入一名小组成员

**2.3.3.2打开加密文件**

**功能描述**

当用户打开一个权限匹配的文件时，文件管理类会在密钥存储空间内寻找对应路径上的密钥信息以快速打开文件，此外，用户也可以手动输入密码来打开文件；文件被打开时，文件管理类将提前调用解密算法将解密出的明文替换原来存储的密文，以方便用户查看

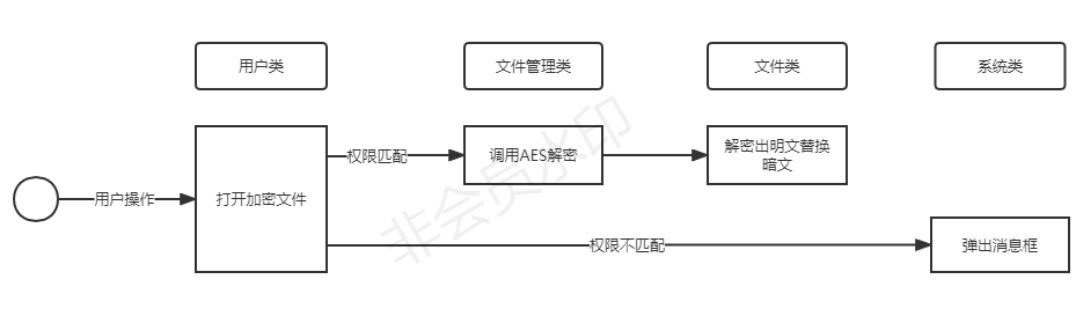
**输入项目**

文件密码

**校验项目**

文件密码是否符合数据库文件对应密码

**打开加密文件流程图**



**预计所需时间和投入人员**

所需5天完成，投入2名小组成员

**2.3.3.3关闭加密文件**

**功能描述**

关闭加密文件时，权限匹配情况下，系统调用加密算法再次加密，暗文重新替换明文，如果权限不匹配，则弹出消息框

**输入项目**

无

**校验项目**

无

**关闭加密文件流程图**



**预计所需时间和投入人员**

所需3天完成，投入2名小组成员

**2.3.4文件操作**

**2.3.4.1文件上传**

**功能描述**

文件视图界面为用户和管理员共有，用户可以在这里上传需要加密的文件，上传时，选择需要上传文件的文件路径，系统将文件上传至数据库中，上传后下一步则是选择是否进行加密

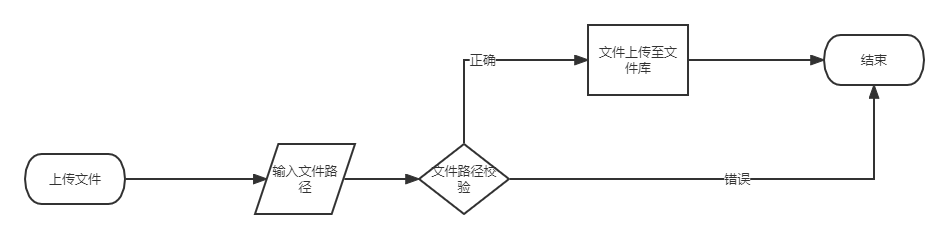
**输入项目**

文件路径

**校验项目**

文件路径是否存在且合法

**文件上传流程图**

****

**预计所需时间和投入人员**

所需2天完成，投入1名小组成员

**2.3.4.2文件下载**

**功能描述**

文件视图界面为用户和管理员共有，用户可以在这里下载需要解密的文件，下载时，选择文件框中的文件，系统类将文件下载至指定路径中

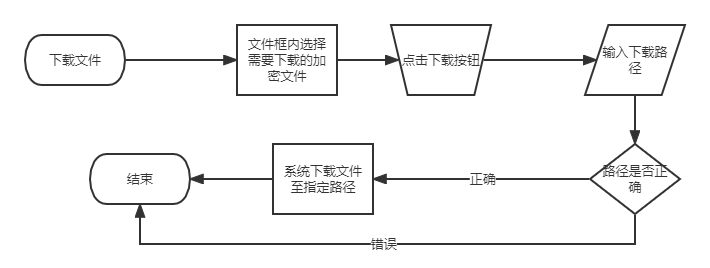
**输入项目**

文件路径

**校验项目**

文件路径是否存在且合法

**文件下载流程图**

****

**预计所需时间和投入人员**

所需1天完成，投入1名小组成员

**2.3.4.3文件删除**

**功能描述**

用户视图为管理员私有，删除其访问的特定文件

**文件删除流程图**

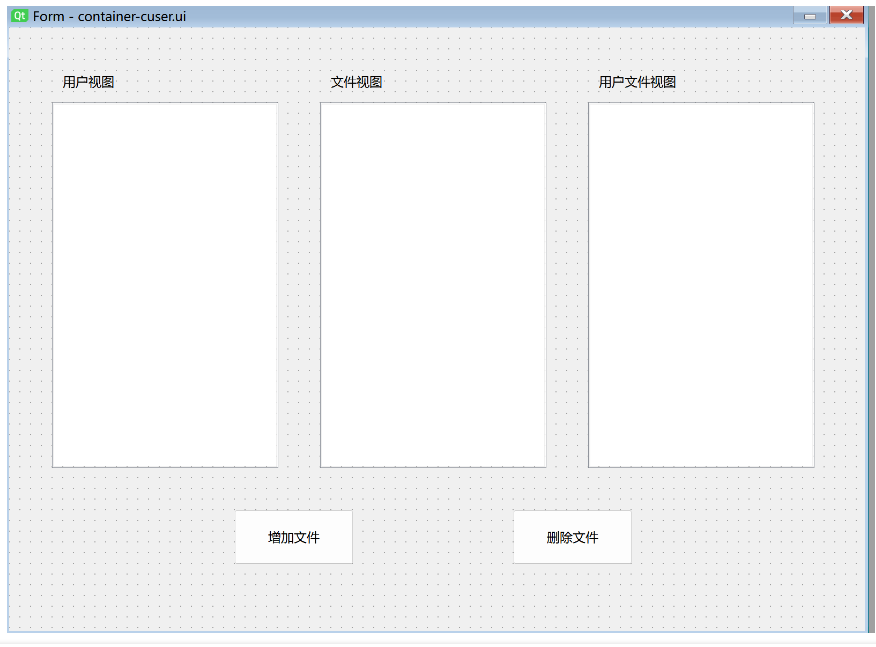
****

**2.3.4.4用户管理**

**功能描述**

用户视图为管理员私有，管理员可以在这里看到用户现在能访问的文件以及现有的所有文件，并有权对指定用户的访问权限做修改，删除或添加其访问特定文件的权力

**设计实现图**



**预计所需时间和投入人员**

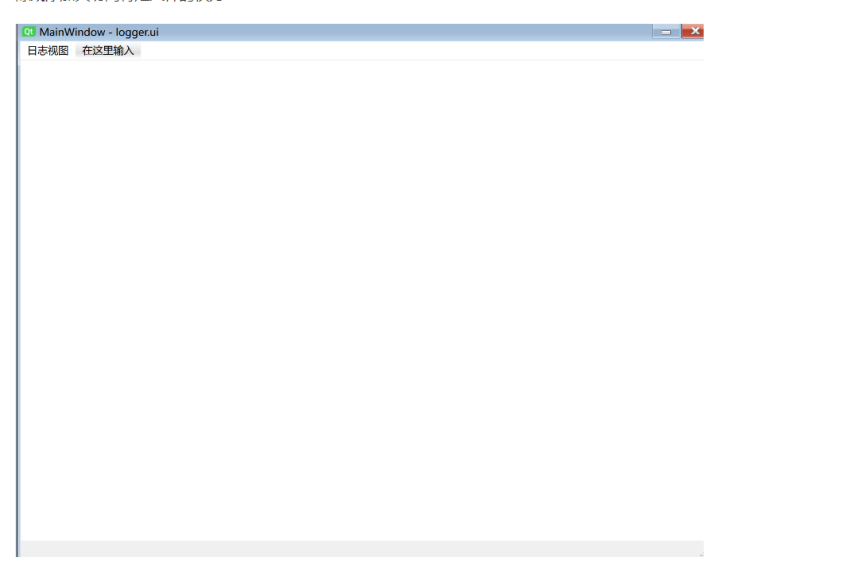
所需3天完成，投入1名小组成员

**2.3.5读取日志文件**

**功能描述**

日志视图为管理员界面，它读取日志文件的内容到界面中供管理员查看

**设计实现图**



**预计所需时间和投入人员**

所需4天完成，投入1名小组成员

**3.功能点分析**