****

**实验报告**

**课程名称： 计算机系统安全**

**实验名称： 完整性访问控制系统设计与实现**

**实验日期： 2018.12.27**

**班 级： 1603102**

**姓 名： 安宏展**

**指导教师： 张玥**

1. 给出应用系统的安全策略文档。

首先用户可以进入登陆界面，选择登陆，如果这名用户是真实注册过的，则进入操作界面，共有四种操作，取款、存款、查询、返回。

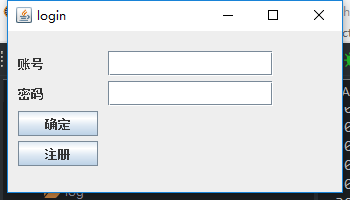
取款和存款需要首先输入金额，然后管理员处会出现取款或存款的金额，管理员认证通过后才能该操作成功。取款金额不能超过当前拥有的金额。

查询即为调用当前数据库中的数据。

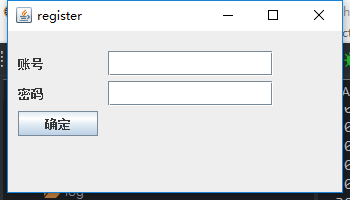
返回操作为退出登陆。

1. 提供交互界面，能够完成录入、查询等功能。

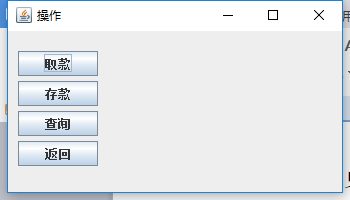
登陆界面：



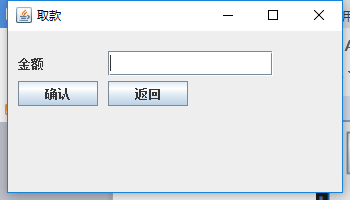
注册界面



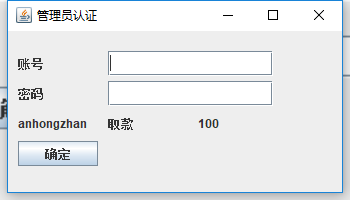
操作界面



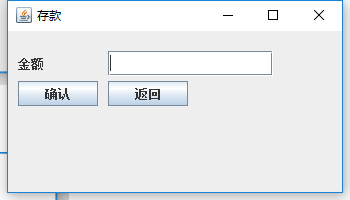
取款界面



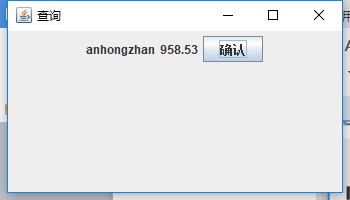
输入金额后弹出的管理员界面



存款界面



查询界面



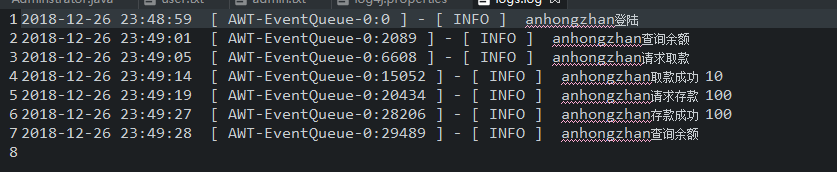
1. 满足责任分离原则。

在完整性策略定义的授权方式里面，责任分离原则禁止一个实体完成单独完成一个操作。我们的用户相当于一个实体，对于查询和退出登陆两种操作是用户自身的权力，而且不影响数据的完整性。

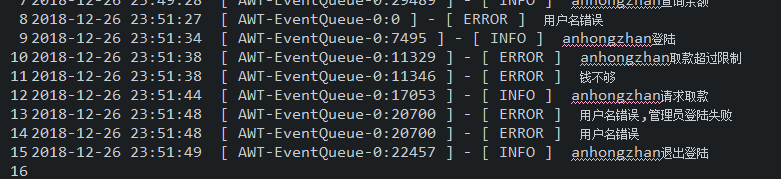
对于取款和存款两种操作，会对数据库中的内容进行修改，所以此时必须采用责任分离的原则，管理员用户由此诞生。单独有管理员时他不能做任何事情，单独有用户他只能查询余额，只有在用户申请这两种然后管理员同意时操作才能完成，符合责任分离的原则，同时也能保证数据的完整性。

1. 保存审计日志。

所有正确操作都使用INFO类型的日志记载



同理，操作错误会用ERROR类型的日志记载



1. 遵循Clark-Wilson模型，定义应用系统的完整性限制条件。

Clark-Wilson模型考虑如下几点：

1）主体必须被识别和认证

2）客体只能通过规定的程序进行操作

3）主体只能执行规定的程序

4）必须维护正确的审计日志

5）系统必须被证明能够正确工作

如果把管理员看作主体，用户为客体，则管理员登陆界面即为认证过程，管理员的用户和密码只有自己才能知道的，满足1）。

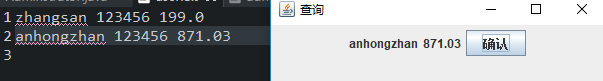
作为客体的用户只能进行取款、存款、查询、返回四种操作，满足2）

主体管理员只能进行认证，不能单独进行存款取款等操作，满足3）

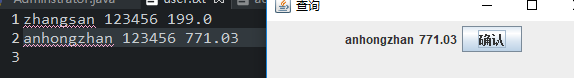
证明4）、5）

下面以几个操作为例：1、登陆2、查询3、取款100 4、存款12 5、返回

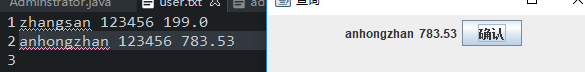
首先登陆查询，可以发现与当前存款完全相同



然后取款100



最后存款12.5



（6）遵循Clark-Wilson模型的证明规则和实施规则，并在设计报告中有所体现。