## 软件系统分析与设计

## Software System Analysis and Design

第三次作业

### 一、题目重述

请基于权限的用户访问控制（RBAC）机制的原理，并在基于监听器模式和事件响应机制下，在事件处理的机制上实现一个RBAC的应用实例。其中要求：

1）完整的代码实现；

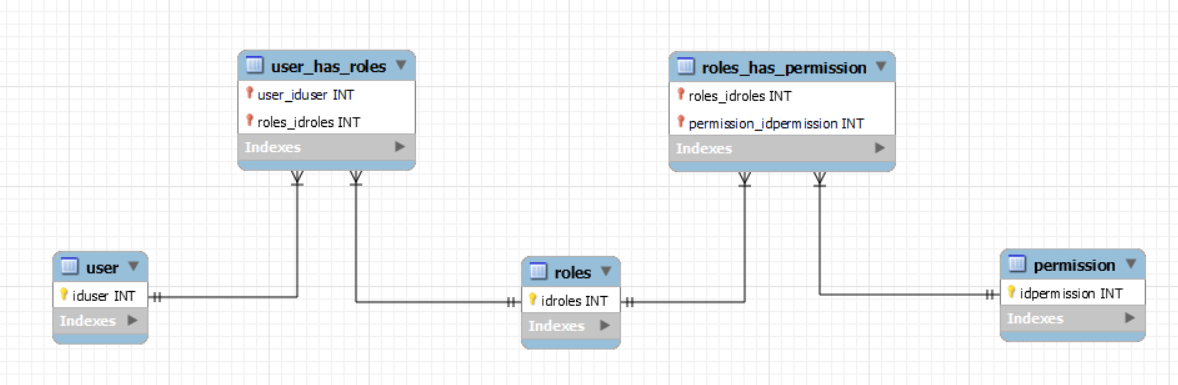
2）页面操作的显示，与角色和权限控制的实现；

3）对RBAC权限控制机制进行分析（例如对页面、对象、功能按钮之间控制的异同）；

扩展：RBAC是一个模型簇，可以展开对比分析。

### 二、RBAC模型簇

RBAC(Role-Based Access Control)即基于角色的访问控制，其主要思想是通过定义角色的权限，并对用户授予某个角色从而来控制用户的权限。目前得到普遍公认的RBAC模型是RBAC96模型簇，它又包括RBAC0，RBAC1，RBAC2和RBAC3四种模型。其中，RBAC0是最基础的模型：



其中用户和角色可以也是一对多的关系，根据业务逻辑的复杂性，若一个用户可以被分配多个角色，则必须使用多对多的权限体系，反之则只需要采用一对多的权限体系。

在RBAC0的基础上，RBAC1增加了子角色的概念。例如，在某一企业管理系统中可能存在总经理、主管、员工这几种角色，在RBAC1模型中，总经理是主管的子角色，主管是员工的子角色，因此总经理会拥有主管和员工的所有权限。RBAC1模型使权限分配更加方便，有效避免了下级权限比上级高的错误。

RBAC2引入了静态职责分离SSD和动态职责分离DSD。SSD包括角色互斥、基数约束、先决条件角色等。角色互斥是指一个用户不能被同时分配为两个互斥的角色。基数约束是指限制用户拥有的角色数量或角色被分配的用户数量。先决条件角色是指，用户必须已经是某一先决角色，才能被设置为这一角色。在上例中可以理解为，用户必须先是企业员工，才能被晋升为主管乃至总经理。DSD是对会话和角色的动态约束，如要求用户在某时刻只能有一个身份有效。

RBAC3是RBAC1和RBAC2的结合，它既支持角色分层又支持角色约束，是最全面的RBAC模型。

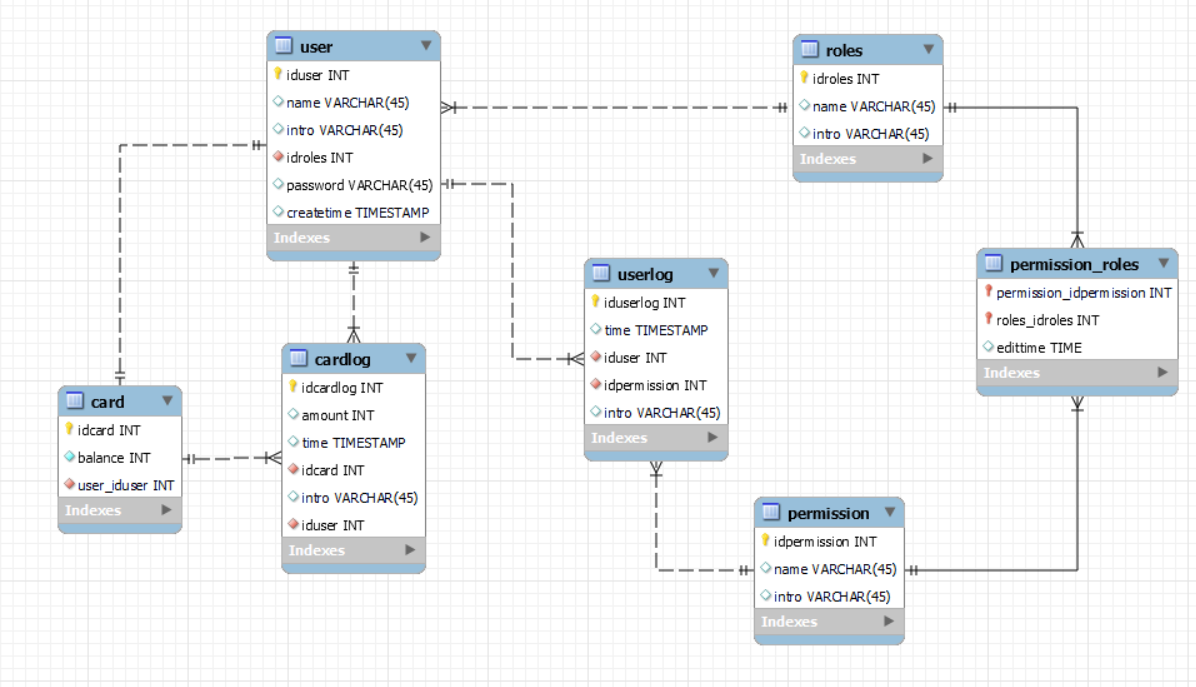
### 三、利用RBAC设计校园卡管理系统

利用RBAC模型，我们可以设计并实现一个校园卡管理系统。对校园卡管理系统进行分析，可以将其中的用户划分为三种角色：

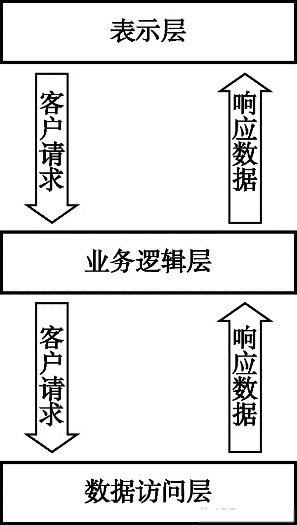
管理员：管理员可以对任意卡信息和用户信息进行增删改查。

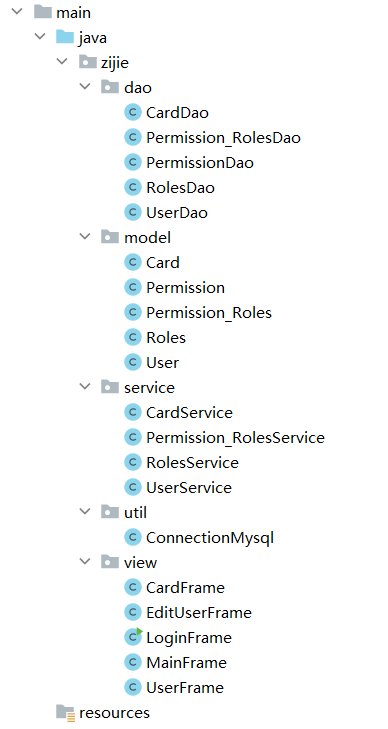
操作员：操作员是消费窗口或充值窗口的工作人员，可以对任意校园卡进行查询、消费或充值，只能对自己的用户信息进行修改或查询。

学生/普通用户：可以查询自己的用户信息和校园卡信息，可以修改个人简介等信息。

在此系统中，一个用户一般只具有一个角色，且用户的权限都相对简单，我们可以采取一对多的用户-角色关系和多对多的角色-权限关系模式，并使用相对简单的RBAC0模型。除此之外，用户和校园卡的拥有关系应当是一对一的关系，用户和校园卡的操作关系是多对多的关系（校园卡流水记录），用户和权限的操作关系是多对多的关系（用户操作记录）。因此数据库设计如下：

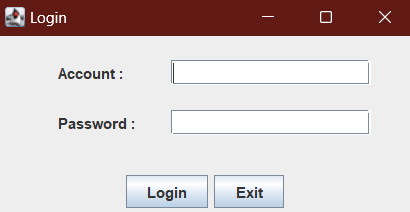
页面显示上，可以选择Java Swing的相关组件，如JFrame、JPanel、JButton、JTextField等，并运用ActionListener对用户操作进行处理。

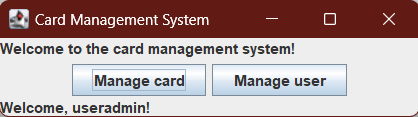
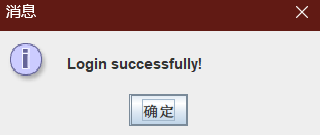
系统架构上，参考DAO和MVC设计模式，将整个系统分为四层。其中，model层与数据库中的表对应，用于数据的传输；dao层负责与数据库进行通信，根据输入信息生成sql语句，执行并返回对应的信息；service层提供实用功能，如登录、充值等，它对用户的请求进行一定处理后，交由dao层对数据库进行修改；view层兼具视图与控制器的功能，监听器监听到用户操作后，调用service层提供的实用功能，并根据返回内容对视图进行修改。

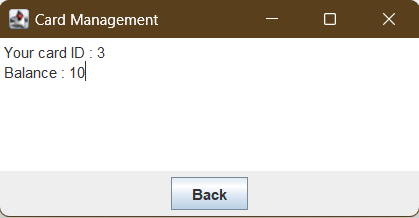
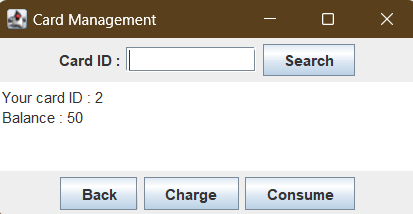
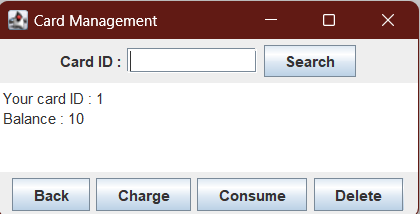
如右图所示，view层就是表示层，service层是业务逻辑层，dao层是数据访问层。

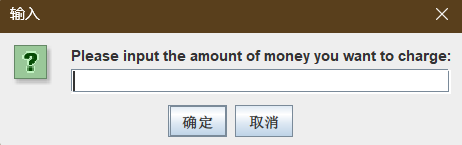
### 四、校园卡管理系统的实现

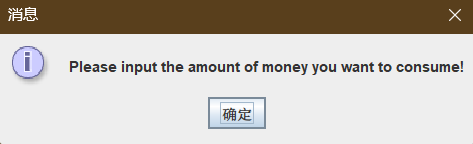
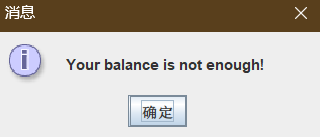
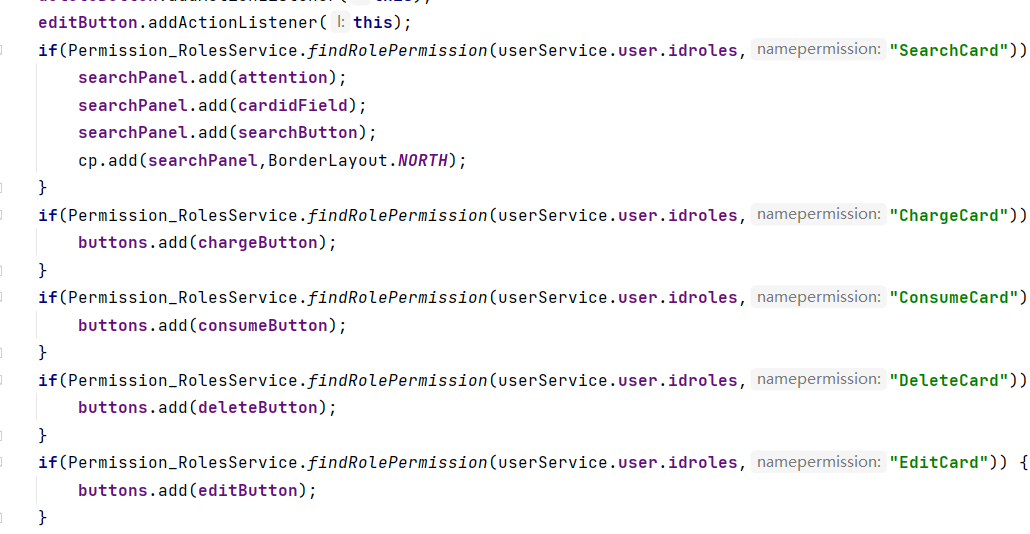
根据以上分析，实现校园卡管理系统。项目结构如图所示。

进入系统后，展示LoginFrame页面，用户输入账号密码后，调用UserService中的login方法校验账号密码正确性，并生成UserService对象。若账号密码正确，则展示MainFrame页面并传入UserService对象。

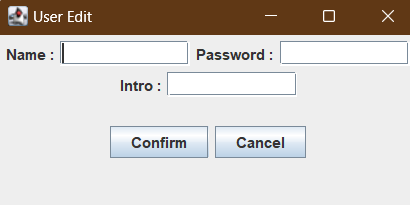
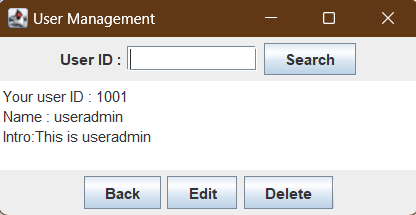
进入主页面后，提供校园卡管理和用户管理两个功能，点击后分别跳转CardFrame页面和UserFrame页面。

校园卡管理页面如图所示。该页面会校验用户的角色和权限，只会显示用户可以执行的操作。右图从上至下分别是管理员、操作员、普通用户的界面。

管理员或操作员可以搜索他人的卡片并进行充值、消费或删除。充值或消费时，系统会对当前用户的权限、输入的合法性进行校验。

以下代码分别实现了对页面的权限控制和对按钮操作的权限控制。系统调用Permission\_RolesService的findRolePermission方法，寻找当前用户的角色是否具有对应权限。

用户管理的页面逻辑与校园卡管理基本一致，只有管理员能看到搜索框、搜索按钮和删除按钮，并可以任意修改其他用户的密码、姓名等信息。

普通用户或操作员仅能看到自己的用户信息，并修改自己的姓名、密码、简介等信息。若需修改信息，系统将弹出修改窗口，将需要修改的信息输入即可，留空代表不修改。

### 五、总结

利用RBAC模型、java swing图形化界面等实现的校园卡管理系统可以实现基本的校园卡操作。在RBAC权限控制模型中，软件系统会获取当前用户的角色信息，并向数据库查询该角色信息是否能够执行某些操作。操作权限可能包括对某些数据的更改、对某些页面的访问或对某些页面元素的操作，根据查询到的权限信息，软件系统会对当前用户采取隐藏页面、隐藏按钮或文字框、拒绝用户的操作、弹出错误提示框等操作。

由于时间仓促等原因，该系统还存在诸多不足之处，如校园卡流水、操作记录等功能未完全实现，界面设计不美观等，需要进一步改进。

### 项目相关代码见附件

### 参考文献

[1] RBAC权限系统分析、设计与实现|shuwoom.com [EB/OL] https://cloud.tencent.com/developer/article/1802329

[2] 微服务 —— 通用角色权限(RBAC)设计实践案例 [EB/OL] https://juejin.cn/post/6999214390125805576

[3] 基础 | 三层架构与MVC模式 [EB/OL] https://zhuanlan.zhihu.com/p/101038664