访问控制实验

## 1 实验目的

访问控制是信息系统安全的重要组成部分。基于角色的访问控制（RBAC）方法通过设置权限与角色相关联，用户通过成为适当角色的成员而得到这些角色的权限，从而极大地简化了权限的管理并提高了灵活性。通过本次实验，理解和掌握RBAC的原理及设计方法，掌握RBAC中对于主体、角色、访问权限的设计与配置。

## 2 实验内容

使用RBAC方法，完成针对文件的访问控制管理。需要根据不同用户所充当角色的权限进行相应的访问控制。访问控制操作包括新建、删除、读取、更改、执行等，可以根据自己系统设计需求自行进行定义。

实验要求完成基本的访问控制功能具有，1）角色分级和继承，2）角色之间具有约束关系（角色互斥）。也可根据个人需要自行增加特性。

**举例如下：**

系统中有某个文件夹存有公司的重要生产文件。公司员工A、B可以对其中的文件具有读取，执行的权限；他们的部门经理M1具有读取、删除、执行的权限；公司员工C、D具有这些文件的新建、读取、更改的权限；他们的经理M2具有新建、删除、读取、更改的权限；公司的大boss拥有所有权限。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 用户 | 新建 | 删除 | 读取 | 更改 | 执行 |
| A |  |  | √ |  | √ |
| B |  |  | √ |  | √ |
| C | √ |  | √ | √ |  |
| D | √ |  | √ | √ |  |
| M1 |  | √ | √ |  | √ |
| M2 | √ | √ | √ | √ |  |
| BOSS | √ | √ | √ | √ | √ |

经理都有删除权限 AB是执行 CD是计划

M1负责AB ，M2负责CD

具体包括：

* 1. 对主体、角色、权限进行定义和配置；
  2. 对角色进行授权；
  3. 对角色的访问权限进行控制；
  4. 对角色的层次关系进行分配控制；
  5. 对角色权限继承进行管理；

例子：经理和员工

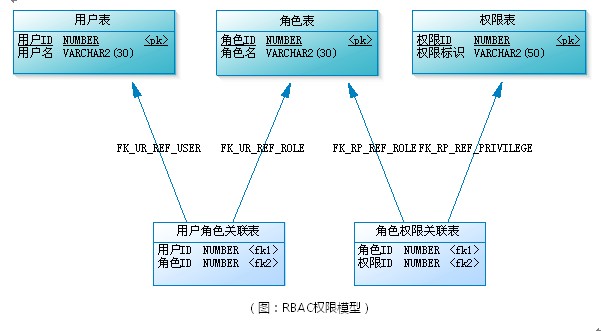
* 1. 对角色约束（互斥）条件进行检查；

例子：不能同时属于执行组和计划组

* 1. 对访问成功与不成功的两种情形均给出结果；

根据下图中的模型，设计用户表、角色表、权限表、用户角色关联表、角色权限关联表、角色继承关系表等；

1. 用户通过角色所对应的权限，完成文件的访问控制；
2. 根据访问权限，完成对相应文件的访问操作，包括允许访问与拒绝访问；



## 3 实验报告

详细描述系统设计方法，以及对RBAC模型及设计的理解，对操作过程及效果用截图描述。