文章编号:1671-4598(2017)08-0183-04 DOI:10.16526/j.cnki.11—4762/tp.2017.08.047 中图分类号:TP39 文献标识码:A

脑卒中信息管理系统权限控制的设计与实现

贺建峰[1],李雅娜[1],潘帅涛[1],高 毅[2],宝媛媛[1],杨 建[1],张 俊[3]
(1.昆明理工大学 信息工程与自动化学院,昆明 650500;2.云南师范大学 文理学院,云南 昆明 650000;
3.玉溪师范学院 教师教育学院,云南 玉溪 653100)

摘要:随着医疗信息技术和互联网的飞速发展,医疗信息资源的安全越来越备受关注,权限管理为解决信息系统安全性问题提供了重要保障,为防止非法获得或破坏信息起着重要的作用;脑卒中信息管理系统存放大量脑卒中患者的治疗信息,为医生发现其潜在的疾病提供依据;针对脑卒中信息管理系统复杂的权限控制需求,提出了一种权限控制方法,采用SpringMVC+Hibernate后台框架,Bootstrap前台框架技术,以及B/S结构软件设计中的精粒度权限管理思路,实现了脑卒中软件系统中的权限管理;同时将权限控制设计为一套与业务无关的权限管理组件,该组件不需要做代码级的更改可以轻松的移植到其它Web系统中;结果表明,系统能够满足权限控制需求,具有良好的可操作性、灵活性和移植性。

关键词:脑卒中信息管理系统;权限管理;B/S;SpringMVC;Hibernate;Bootstrap

Authority Management Design and Realization of Stroke Information System

He Jianfeng[1], Li Yana[1], Pan Shuaitao[1], Gao Yi[2], Bao Yuanyuan[1], Yang Jian[1], Zhang Jun[3]
(1. School of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650500, China; 2. College of Arts and Sciences, Yunnan Normal University, Kunming 650000, China; 3. School of Teacher Education, Yuxi Normal University, Yuxi 653100, China)

Abstract: With the rapid development of medical information technology and Internet, more and more attention has been focused on the security of medical information. Privilege management provide an important guarantee to solve the security problem of information system, and it play an important role preventing illegal access to information. Stroke information management system stores large number of treatment information of stroke patients, which provide the basis for the doctors to discover the underlying diseases. Aiming at complex authority control requirements of stroke information management system. In this paper, it proposes a privilege control method, which adopts SpringMVC + Hibernate backstage framework and combined with technology of Bootstrap foreground framework, introducing the fine granularity of right management method in the B/S structure software design. At the same time, the privilege control is designed as a set of business independent management components, which can be easily transplanted to other Web systems without changing the code level. The results show that the system can meet the requirements of the authority control, and has good operability, flexibility and portability.

Keywords: stroke information management system; authority management; B/S; SpringMVC; Hibernate; Bootstrap

0 引言

随着医院管理内容信息化的不断发展和深化,给医院带来了极大的信息量,而对于医疗信息的有效管理、共享、分析和处理,不论是从数量上还是种类上都大大增加,所以将计算机技术融入医疗信息管理无疑是最好的办法。然而,随着因特网和计算机技术应用的快速发展,医疗信息资源的安全越来越备受关注,权限管理为解决信息系统安全性问题提供了重要保障,为防止非法获得或破坏信息起着重要的作用。“脑卒中”又称“中风”是一种急性脑血管疾病,脑卒中已成为世界上人类第二大致死疾病和第一大致残因素[1-2]。并且我国每年因为脑卒中疾病而导致死亡人数、发病人数都比较多[2]。脑卒中信息管理系统就是利用计算机网络技术和数据存储、处理技术,快速高效的对脑卒中信息的采集、存储、处理、传输、查询和分析等全方位管理的计算机软件系统,同时建立了一个有关脑卒中患者信息的资料仓库,将数据提取技术应用在医学领域,有助于医生识别出其潜在的疾病,也有助于患者及时发现疾病、早期诊断、早期治疗[3]。

就目前而言,脑卒在我国城镇居民的死亡原因中已高居首位,临床医生在治疗脑卒中过程中将产生大量的医学数据[3]。但国内绝大多数医院是以C/S模式进行开发的,这种开发模式设计的系统需要在每个终端安装客户端并且对硬件系统要求较高。除此之外,绝大多数医院系统存储数据以非结构化文档进行存储,该方式存储的数据不能被直接提取、统计和分析[4],造成严重的资源浪费,医生也很难从以往的临床数据中发现疾病的发展趋势和其中隐含的规律,对于疾病的研究极为不利。

脑卒中管理系统中信息量比较大,功能比较多,用户也比较多。为保障信息的安全性,设计一个健壮的符合“脑卒中管理系统”业务需求的安全管理机制是非常必要的。一个健全的信息系统均会设置大量的功能和供许多用户使用,这些用户被

收稿日期:2017-02-18; **修回日期**:2017-03-07。
基金项目:国家自然科学基金(11265007)。
作者简介:贺建峰(1965-),男,云南昆明人,博士,教授,主要从事信息工程,数据挖掘方向的研究。
通讯作者:张 俊(1990—),男,云南开远人,硕士,主要从事计算机应用方向的研究。

分配不同的角色、具有不同的操作权限，他们从信息系统中获取信息与处理信息的职权也不尽相同，这就要求应用系统提供一种动态权限管理机制，控制各种用户使用系统的访问权限。在防止信息泄露和非法访问方面，目前有三种广泛应用的技术：授权、访问控制和审计。其中前两者属于权限管理的范畴，是信息系统安全管理的重要手段[5]。其中基于角色的访问控制模型（RBAC）是目前最为流行的。

基于以上 C/S 模式开发的脑卒中信息系统和非结构化文档存储数据的不足之处，以及医院对脑卒中信息管理的实际需求，设计和开发了基于 B/S 模式的脑卒中信息管理系统来满足医院的实际需求。这种模式开发的系统分布性强、共享性强，不受客户端约束，只要有操作系统和浏览器且能上网，可以在随时随地的就能访问服务器端部署的系统来进行信息处理，不需要安装任何专门的软件。除此之外，在这种模式下，系统的升级和后期维护工作也只需在服务器端进行配置即可，且对电脑配置要求较低。脑卒中信息管理平台中权限控制设计成为一个组件，且与业务无关的 Web 权限管理模块，这个权限管理模块可以轻松的移植到别的 Web 系统中，且不需要更改代码。具有较高的应用价值。结合前台 Bootstrap 框架技术，能使脑卒中信息管理平台在手机、平板和台式机上都能很好地展示，系统前端界面不美观的问题也得到了解决。

1 系统支撑环境

本权限管理信息平台基于 B/S 模式进行开发，采用 Tomcat7.0.54 作为系统服务启动项，Oracle 作为后台数据库。Bootstrap 作为前台界面开发框架并采用了 SpringMVC＋Hibernate 作为后台数据的开发框架。其中 Bootstrap 是目前最流行的一种开源的 Web 前端开发框架，它是基于规范的 CSS、JavaScript 插件和 Less 前端开发库开发出来的框架，并且提供了很多 CSS 和 JavaScript 的效果[6]，内置了很多漂亮的样式。其最大的优势是开发响应式布局，移动设备优先。Bootstrap 使用 Less 作为 CSS 处理器，使 CSS 具有动态性，使得开发者可以方便的让网页无论在台式机、平板设备、手机上都获得最佳的体验。总之，Bootstrap 更能满足对脑卒中信息管理系统界面设计的需要。

整个 Web 的集成框架从逻辑上分为表示层、业务逻辑层和数据持久层三部分，其中表示层通过 Bootstrap 来展示，Bootstrap 接收用户输入的数据，把信息传递给业务层，同时 Bootstrap 通过 Ajax 方式从业务层获取相应的数据，并将数据展示到前台的页面上。业务逻辑层通过 SpringMVC 来实现，SpringMVC 从页面表单获取数据并进行数据的各种业务处理。合法用户登录系统后，在后台对用户权限的各种业务处理就是通过 SpringMVC 中的 Controllor 来完成的。数据持久层通过 Hibernate 来实现，Hibernate 用于 Dao 层与数据库进行交互，对数据进行增（Create）、删（Delete）、改（Update）、查（Read）操作，在权限管理系统中 Hibernate 主要用于对权限管理中的各功能数据表进行操作[7]。图 1 展示了各层之间的分布情况。

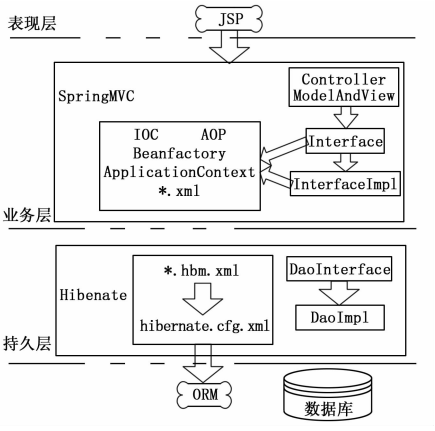

图 1 架构图

2 权限管理设计

2.1 权限管理的粒度

权限管理采用基于角色的认证技术，从而实现了对用户操作权限的精细控制。

用户或操作（权限）粒度可以精确到具体的角色，即在用户和操作（权限）之间引入角色的概念，由系统中最高权限的系统管理员将某一系统资源的访问权限授权给角色，从而实现对数据库的增（Create）、删（Delete）、改（Update）查（Read）等操作。角色和用户之间是一个多对多的关系，角色和操作（权限）之间也是多对多关系，用户和操作（权限）之间没有直接的关系，但通过角色共同决定了权限管理的规则。角色是根据一个组织内工作性质的不同来设定的，角色可以是实际工作中的岗位、职位。一旦某个用户被赋予某种角色，则此用户可以完成该角色所具有的全部职能，通过将权限指定给某个角色而不是具体的用户，以此来建立用户和权限之间的关系。如果有新的操作（权限）需要加入系统，因此角色能被赋予新的操作（权限）。操作（权限）既能赋予也能撤销。

就“脑卒中信息管理系统”而言，操作对象从功能上要细化到菜单项目、功能模块和操作按钮，从数据上要细化到中心和单位，即用户即使具有相应的功能权限，也只能操作其权限范围内的业务数据。将权限细化为模块入口权限、功能按钮权限、数据对象权限，模块入口权限控制系统菜单的加载，功能按钮权限对模块的各个功能按钮进行授权控制，数据对象权限通过系统内部的业务逻辑将权限控制细化到具体的数据对象上[8]，实现了细粒度的访问控制。

2.2 权限管理数据库表结构设计

权限管理模块主要通过功能模块、操作、岗位、用户、中心及单位 6 个功能模块来进行设计。其中功能模块管理以 Bootstrap 页面的树形结构来完成对整个“脑卒中信息管理”平台所需的多级功能模块入口进行动态管理；权限管理属于对用户最终需要操作的模块（菜单）及模块中的操作按钮和访问数据的动态加载；角色功能完成了系统角色的动态管理以及对指定角色所拥有的功能模块和操作权限的分配；用户功能完成了对整个“脑卒中信息管理系统”用户的动态管理和对指定用户赋予合适的角色，从而实现不同系统用户对于系统不同功能模块的不同操作权限；中心管理和单位管理用来表示用户所属的部门信息。

当系统管理员创建一个中心或单位的信息时，同时为单位和中心分配等级和中心或单位管理员，在脑卒中信息管理平台中，中心的等级为一级，单位的等级为二级。当创建中心或单

位管理员后，为其管理员分配了对应的角色（岗位），随之中心或单位的管理员也就拥有了操作一些功能模块和操作按钮的权限，当中心或单位的管理员登录系统时，在 WEB 页面中只能加载其授权的功能模块，未被授权的功能模块不予显示。权限管理结构图如图 2 所示。

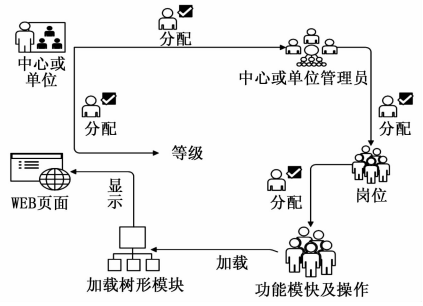

图 2　权限管理结构图

根据对权限管理结构的分析，权限管理作为 WEB 软件系统中最重要的部分之一，将采用 7 张数据库表来实现。模块信息表（MKXXB）记录每个模块的编号和名称（前台主菜单），子模块信息表（ZMKXXB），记录每个子模块的所属模块编号、入口地址等信息，它是前台显示菜单的主要依据。岗位信息表（GWXXB）用来记录岗位编号及岗位名称。操作信息表（CZXXB）用来记录对象数据的增加、删除、修改、查询等操作权限，用户信息表（YHXXB）用来记录用户信息，用户和角色（岗位）是多对多关系，需要通过用户岗位关联信息表（YHGWGLXXB）的外键来进行维护，角色（岗位）和权限（操作）也是多对多的关系，要岗位权限关联信息表（GWQXGLXXB）通过外键方式来维护，从而建立起用户和权限之间的联系。它们之间的关系及物理模型如图 3 所示。

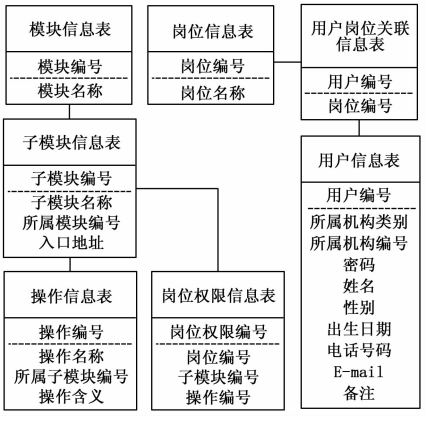

图 3　系统物理模型图

3　权限管理的实现

本系统权限管理主要包括授权和认证。授权是指将某一资源的增（Create）、删（Delete）、改（Update）、查（Read）等操作授权给具体的角色。认证是确认某个用户对某一系统资源是否具有相应操作权限的过程。从而达到对用户权限的细粒度控制。

3.1　权限管理分析

授权就是给角色进行授权。角色授权是对某个角色能访问的系统资源进行增（Create）、删（Delete）、改（Update）、查（Read）等操作权限分配，再将角色分配给指定的用户。例如在“脑卒中信息管理系统”中，给“中心管理员”这个角色分配对中心信息和对单位信息的增加、删除、修改和查询的操作权限，所有中心的管理员拥有“中心管理员”角色，最终他们就拥有了对中心信息和对其下级单位信息进行增（Create）、删（Delete）、改（Update）和查（Read）的操作权限。给“单位管理员”这个角色分配对单位信息的增（Create）、删（Delete）、改（Update）和查（Read）的操作权限，所有单位的管理员只拥有“单位管理员”角色，最终他们可以对本单位信息进行增（Create）、删（Delete）、改（Update）和查（Read）的操作权限，而不能对其所属中心的信息进行增（Create）、删（Delete）、改（Update）和查（Read）操作。角色授权的优点是可以批量授权，可以降低为很多用户分配多种角色的工作量，简化操作的同时降低了出错率，极大的提高管理效率。

认证就是用户登录系统后，系统根据他所被赋予的角色，在 WEB 页面左侧的菜单栏中列出相应的菜单及菜单所属的页面中的操作按钮。具有不同操作权限的用户登录系统后，前台视图中展现的菜单（功能模块）是有所差异的。在具体实现的过程中，认证就是从岗位权限信息表中检索出登录到系统的用户所能访问的功能模块信息，形成前台视图中显示菜单需要的数据格式，共前台显示菜单使用。同时，将用户所能访问的资源标识及用户对资源具有的增、删、改、查、导出等操作权限，写入 session 当中，转发到前台，然后在视图上从后台转发过来的数据中取出用户的操作权限控制列表，根据用户拥有的权限，在 jsp 页面上进行识别，然后根据识别的结果分别显示“增加”、“删除”、“修改”、“查询”、“导出”等按钮，实现精粒度的权限控制。

3.2　权限管理实现

在 B/S 结构的软件系统中，一般会设计导航菜单，导航菜单可以为用户提供清晰的、层次分明的模块信息，且每一个导航菜单实现相应的功能。例如在“脑卒中信息管理系统”中，导航菜单具有“病例管理”、“基础数据管理”、“用户权限管理”和“统计分析”等一级菜单，这些一级菜单对应数据库中的模块信息，每个模块下包含有子菜单（数据库中的子模块信息），“病例管理”菜单中有“新建病例”、“病例列表”、“病例导出”、“病例导出记录”和“病例上传”二级子菜单；“基础数据管理”菜单中有“中心信息维护”和“单位信息维护”二级菜单，“用户权限管理”菜单中有“用户信息维护”、“模块信息维护”和“岗位信息维护”二级菜单；“统计分析”菜单中有“病例来源统计分析”和“病例信息统计分析”。每个子模块都对应有具体的功能，每一个子菜单都具有子菜单名称、入口地址等信息，它们存放在数据库的子模块信息表中。在读写数据库时，采用 Hibernate 与数据库进行交互。

在程序的设计过程中，采用 SpringMVC＋Hibernate 后台框架和 Bootstrap 前台框架，由于每个实体都要进行增、删、改、查等操作，因此使用 Java 的泛型设计了一个 BaseDao 基类，该基类中提供了基本的增、删、改、查的方法，可以完成基本的 CRUD 等操作。对岗位权限、用户、岗位、模块等的

Dao 操作则设计继承于 BaseDao 的子类，只要在泛型中传入相应的实体即可，就可以实现完成基本的增、删、改、查操作，不需要写大量重复的代码，从而增强了代码的复用性。前台与后台的交互由 SpringMVC 的标注@Controller 的 Controllor 来完成，在 Controllor 中注入 BaseDao 并且调用 Dao 层的业务逻辑来处理业务需求，然后将处理结果通过 ModelAndView 转发至前台 jsp 页面。

1）权限配置：采用 Controllor 的 Model 模型传递参数，Controllor 中会自动根据前台传入的角色数据实例化一个 GWXXB 类，只需要在 Controllor 中调用 GwxxbDao（完成对角色数据的 CRUD 等操作）的增加方法将其持久化到数据库中即可。授权是对角色的授权，在岗位权限关联的 WEB 页面中，当前台用户点击每个子模块所包含的操作复选框将其选中时，单击提交按钮后，将子模块的 id、角色的 id、对该子模块中的对象数据的查询、增加、修改、删除、导出等权限写入数据库。当取消选中复选框时，则应从数据库中删除相应的信息。

2）用户认证：为保证系统的安全性，脑卒中信息管理系统中用户的密码以 MD5 加密算法加密后存储在文件系统中。当用户登录系统时，系统会把用户当前输入的密码计算成 MD5 值，然后再去和保存在文件系统中的 MD5 值进行匹配，进而确定输入的密码是否正确。通过验证后，系统获取用户信息，查询出用户所拥有的所有岗位信息，用 Bootstrap 框架中的模态框进行显示，同时将用户所选的岗位信息写入 session 中，完成认证过程。

3）权限获取：当用户选择岗位后，系统根据用户所选择的岗位在后台调用业务逻辑 GwqxxxbDao 从岗位权限信息表中查找出该岗位所拥有的权限。根据权限中的子模块编号从模块信息表和子模块信息表中检索出模块信息和子模块信息存放入 moduleList，同时将用户所拥有的操作权限放入一个 gwqxList。当用户选择相应的岗位登入系统后，后台将 moduleList 转发到前台，当用户对某一资源（子模块）访问时，后台将 gwqxList 转发到前台，供前台对操作按钮进行显示。

4）权限访问：通过后台转发过来的 Json 格式（{" moduleList"：{" success"：true，" nodes"：[{" text"：" 基础信息管理"，" nodes"：[{" text"：" 中心信息维护"，" href"：" centerInfo/index"}，{" text"：" 单位信息维护"，" href"：" organizationInfo/index"}]} …}}）的模块和子模块数据加载模块菜单，只要用户对某一资源（模块）具有增加、删除、查询、精确查询、修改中的任何一个权限，主菜单就要列出相应的子菜单，否则，子菜单不显示，当某个模块中的所有子模块中不具有任何的操作权限时，该模块也不会显示。当岗位权限信息表中有相应的操作时，将操作信息表中该操作的操作含义字段 CZHY 中变量的值设置为 inline，当岗位权限信息表中没有相应的操作时，将操作信息表中该操作的操作含义字段 CZHY 中变量的值设置为 none，前台根据后台转发过来的 Json 格式（{" czqxList"：{" GwqxxxCx"：" inline"，" GwqxxxJqcx"：" inline"，" GwqxxxSc"：" none" …}}）的操作权限的数据，在前台的每个操作按钮的 input 标签中设置 style（style＝'display：{czqxList. GwqxxxCx}'）样式，display 的值用 EL 表达式来进行表示，从而控制按钮对该用户是可见的还是屏蔽的。在前台页面中显示岗位权限信息列表时，在 JS 中进行判断，如果子模块对应的操作的值为 true 时，将列表中的值设置为√，如果子模块对应的操作的值为 false 时，将列表中的值设置为×。这样实现了“脑卒中信息管理系统”中对各种资源的精细的权限管理，岗位权限列表如图 4 所示。

岗位权限信息

查询条件 查询 精确查询 新增 修改 删除

	子模块名称	操作名称						
		查询	精确查询	打开	新增	修改	删除	导出
□	新建病例	×	×	×	×	×	×	×
□	病例列表	✓	✓	✓	×	×	✓	×
□	病例导出	×	×	×	×	×	×	✓
□	病例导出记录	✓	✓	×	×	×	✓	×
□	病例上传	✓	✓	×	×	×	×	×
□	省份信息维护	✓	✓	×	✓	✓	✓	×
□	中心信息维护	✓	✓	×	✓	✓	✓	×
□	单位信息维护	✓	✓	×	✓	✓	✓	×
□	模块信息维护	✓	✓	×	✓	✓	✓	×
□	岗位信息维护	✓	✓	×	✓	✓	✓	×
□	用户信息维护	✓	✓	×	✓	✓	✓	×
□	病例来源统计分析	✓	×	×	×	×	×	×
□	病例信息统计分析	✓	×	×	×	×	×	×

图 4 岗位权限列表

4 结语

本文设计与实现了一种基于 B/S 模式的精细的权限管理，重点介绍了该权限管理的核心业务的设计思想与实现。采用 SpringMVC＋Hibernate 后台框架和 Bootstrap 前台开发框架设计并实现了脑卒中信息管理系统中的权限管理，极大地提高了应用系统的可移植性、可扩充性和可维护性，很好的满足了脑卒中信息管理系统中复杂的权限控制需求，具有良好的可操作性和灵活性。这对信息管理系统安全及复杂的权限控制需求有借鉴作用。

参考文献：

[1] 曹 珂，刘 检，苗露阳，等. 皮质神经元 B27 原代培养及 MAP2 鉴定 [J]. 沈阳药科大学学报，2013，30 (1)：40－43.

[2] 吴小伟. 面向脑卒中的远程医疗协同服务系统 [D]. 哈尔滨：：哈尔滨工业大学.

[3] 邹 芳，田 晔，吴卫国，等. 基于非结构化电子病历的脑卒中数据挖掘管理系统设计和实现 [J]. 中国数字医学，2015，(3)：41－44.

[4] 李静华，等. 未来电子病历的发展与技术深讨 [J]. 中国数字医学，2012，6 (7)：8－10.

[5] 李 东，施懿闻，郝艳妮，等. 科学基金管理系统的用户权限管理模式研究 [J]. 计算机技术与发展，2012，22 (2)：159－167.

[6] 高榕岭. Bootstrap 在前端开发中的优势 [J]. 计算机光盘软件与应用，2015 (1)：74－76.

[7] 李天鸣，何月顺. 基于 ExtJS 技术与 SSH 框架的权限管理研究 [J]. 计算机应用与软件，2011，28 (5)：165－167.

[8] 张 珣，李 青，杨志峰. 飞机维修保障信息体统权限管理设计与实现 [J]. 计算机应用，2014，34 (S1)：70－73.