(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103049684 A
(43)申请公布日 2013.04.17

(21)申请号 201210563361.8

(22)申请日 2012.12.21

(71)申请人 大唐软件技术股份有限公司
地址 100012 北京市朝阳区北苑路乙 108 号北美国际商务中心 B 座

(72)发明人 赵雨佳 王强 赵守来

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 苏培华

(51)Int.Cl.
G06F 21/30(2013.01)

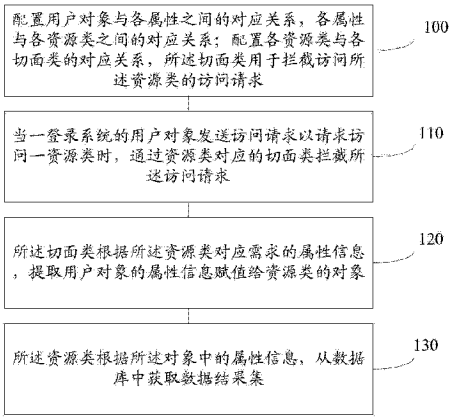
权利要求书 2 页 说明书 10 页 附图 2 页

(54)发明名称

一种基于 RBAC 模型扩展的数据权限控制方法和系统

(57)摘要

本发明提供了基于 RBAC 模型扩展的数据权限控制方法和系统，涉及计算机技术领域。所述方法包括：配置用户对象与各属性之间的对应关系，各属性与各资源类之间的对应关系；配置各资源类与各切面类的对应关系，基于上述配置，数据权限的控制过程包括：当一登录系统的用户对象发送访问请求以请求访问一资源类时，通过资源类对应的切面类拦截所述访问请求；所述切面类根据所述资源类对应需求的属性信息，提取用户对象的属性信息赋值给资源类的第一对象；所述资源类根据所述第一对象中的属性信息从数据库中获取数据结果集。本发明针对资源的业务逻辑完全与对数据权限相分离，提高了系统针对数据权限控制的灵活性，扩展性强，且代码冗余量低，节省空间。



CN 103049684 A

1. 一种基于 RBAC 模型扩展的数据权限控制方法，其特征在于，包括：

配置用户对象与各属性之间的对应关系，各属性与各资源类之间的对应关系；配置各资源类与各切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求；

基于上述配置，数据权限的控制过程包括：

当一登录系统的用户对象发送访问请求以请求访问一资源类时，通过资源类对应的切面类拦截所述访问请求；

所述切面类根据所述资源类对应需求的属性信息，提取用户对象的属性信息赋值给资源类的第一对象；

所述资源类根据所述第一对象中的属性信息，从数据库中获取数据结果集。

2. 根据权利要求 1 所述的方法，其特征在于，所述切面类根据所述资对应的属性信息，提取用户对象的属性信息赋值给资源类的第一对象包括：

所述切面类根据所述资源类对应需求的属性信息，判断对应用户对象的 SESSION 中是否存在所述属性信息；

如果存在，则从所述 SESSION 中提取用户对象的属性信息赋值给资源类的第一对象；

如果不存在或者不全部存在，则从对应所述用户对象的属性信息表中，提取所述需求的属性信息中缺少的属性信息写入所述 SESSION 中，再从 SESSION 中将所述需求的属性信息赋值给资源类的对象。

3. 根据权利要求 1 所述的方法，其特征在于，所述配置各资源类与各切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求包括：

在 SPRING 框架的 XML 配置文件中定义各资源类与相应切面类的对应关系；所述切面类用于拦截访问所述资源类的访问请求；

和 / 或，采用数据库表结构建立各资源类与相应切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求。

4. 根据权利要求 1 所述的方法，其特征在于，所述资源类根据所述第一对象中的属性信息，从数据库中获取数据结果集包括：

所述资源类获取所述对象中的各属性信息，传入所述资源类中的动态 SQL 语句执行并生成所述用户对象的数据结果集；所述动态 SQL 语句用于根据属性信息确定查询条件并进行查询。

5. 根据权利要求 4 所述的方法，其特征在于，所述资源类获取所述对象中的各属性信息，传入所述资源类中的动态 SQL 语句时还包括：

将所述第一对象中的属性信息，对当前属于用户对象的数据权限的各属性信息进行标记；

进一步的，所述执行并生成所述用户对象的数据结果集之后还包括：

当所述数据结果集不为空时，直接将数据结果集返回给所述用户对象所在终端；

当所述数据结果集为空时，则根据各属性信息的标记，判断数据结果集是否根据属于所述用户对象的数据权限获得的；如果是，则生成所述用户对象没有相应权限的提示信息返回给所述用户对象所在终端。

6. 一种基于 RBAC 模型扩展的数据权限控制系统，其特征在于，包括：

配置模块，用于配置用户对象与各属性之间的对应关系，各属性与各资源类之间的对

应关系；配置各资源类与各切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求；

拦截模块，用于当一登录系统的用户对象发送访问请求以请求访问一资源类时，通过资源类对应的切面类拦截所述访问请求；

赋值模块，用于所述切面类根据所述资源类对应需求的属性信息，提取用户对象的属性信息赋值给资源类的第一对象；

数据获取模块，用于所述资源类根据所述第一对象中的属性信息，从数据库中获取数据结果集。

7. 根据权利要求 6 所述的系统，其特征在于，所述赋值模块包括：

判断模块，用于所述切面类根据所述资源类对应需求的属性信息，判断对应用户对象的 SESSION 中是否存在所述属性信息；

第一赋值模块，用于如果存在，则从所述 SESSION 中提取用户对象的属性信息赋值给资源类的第一对象；

第二赋值模块，用于如果不存在或者不全部存在，则从对应所述用户对象的属性信息表中，提取所述需求的属性信息中缺少的属性信息写入所述 SESSION 中，再从 SESSION 中将所述需求的属性信息赋值给资源类的对象。

8. 根据权利要求 6 所述的系统，其特征在于，所述配置模块包括：

第一配置模块，用于在 SPRING 框架的 XML 配置文件中定义各资源类与相应切面类的对应关系；所述切面类用于拦截访问所述资源类的访问请求；

和 / 或，第二配置模块，用于采用数据库表结构建立各资源类与相应切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求。

9. 根据权利要求 6 所述的系统，其特征在于，所述数据获取模块包括：

第一数据获取模块，用于所述资源类获取所述对象中的各属性信息，传入所述资源类中的动态 SQL 语句执行并生成所述用户对象的数据结果集；所述动态 SQL 语句用于根据属性信息确定查询条件并进行查询。

10. 根据权利要求 9 所述的系统，其特征在于，在所述数据获取模块还包括：

标记模块，用于将所述第一对象中的属性信息，对当前属于用户对象的数据权限的各属性信息进行标记；

进一步的，所述数据获取模块之后还包括：

第一返回模块，用于当所述数据结果集不为空时，直接将数据结果集返回给所述用户对象所在终端；

第二返回模块，用于当所述数据结果集为空时，则根据各属性信息的标记，判断数据结果集是否根据属于所述用户对象的数据权限获得的；如果是则生成所述用户对象没有相应权限的提示信息返回给所述用户对象所在终端。

一种基于 RBAC 模型扩展的数据权限控制方法和系统

技术领域

[0001] 本发明涉及计算机技术领域，特别是涉及一种基于 RBAC 模型扩展的数据权限控制方法和系统。

背景技术

[0002] 企业应用系统建设都涉及权限管理：一种是功能操作权限，一种是数据操作权限。其中，功能权限可以理解为：能做什么的问题，如增加销售订单。数据权限可以理解为：能在哪里干什么的问题，如察看北京分公司海淀销售部张三的销售订单。

[0003] 对于权限控制，现在基本上均基于 RBAC(ROLE-BASED ACCESSCONTROL，基于角色访问控制）模型构建权限控制系统。参照图 1，其为 RBAC 的核心模型。在 RBAC 中，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。这就极大地简化了权限的管理。在一个组织中，角色是为了完成各种工作而创造，用户则依据它的责任和资格来被指派相应的角色，用户可以很容易地从一个角色被指派到另一个角色。

[0004] 现有技术中，基于 RBAC 模型的权限控制系统已经实现功能操作方面的权限控制，而对于数据操作权限没有控制或者采用硬编码方式，局限性比较大，灵活度不够。比如对于电信行业、广电行业等行业的运营商的在对客户资料信息、敏感的财务数据等信息的数据权限访问控制方面，运营商已经不仅仅局限于功能操作权限的访问控制，更多的数据权限的访问控制。

[0005] 比如，现有技术中，由于针对一资源的数据权限是根据具体的业务定制的，即由业务人员确定哪些用户对应哪些角色，这些角色拥有哪些数据权限，然后业务人员将其针对所述资源的上述需求告诉开发人员进行编码，开发人员即根据需求在针对所述资源的访问类中，将验证逻辑及需求的属性硬编码在该类中，那么该种思路及操作过程，针对所述资源的业务类型变更，则需要业务人员提供数据权限的需求关系给开发人员重新进行编码，导致代码冗余量大，并且系统局限也比较大，不能灵活的适应各种不断变化的业务需求。

发明内容

[0006] 本发明所要解决的技术问题是提供一种基于 RBAC 模型扩展的数据权限控制方法和系统，解决现有技术中在原系统架构情况下，变更数据权限时代码冗余量大，并且数据权限控制不灵活，系统局限也比较大，不能灵活的适应各种不断变化的业务需求的问题。

[0007] 为了解决上述问题，本发明公开了一种基于 RBAC 模型扩展的数据权限控制方法，包括：

[0008] 配置用户对象与各属性之间的对应关系，各属性与各资源类之间的对应关系；配置各资源类与各切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求；

[0009] 基于上述配置，数据权限的控制过程包括：

[0010] 当一登录系统的用户对象发送访问请求以请求访问一资源类时，通过资源类对应的切面类拦截所述访问请求；

[0011] 所述切面类根据所述资源类对应需求的属性信息，提取用户对象的属性信息赋值给资源类的第一对象；

[0012] 所述资源类根据所述第一对象中的属性信息，从数据库中获取数据结果集。

[0013] 优选的，所述切面类根据所述资对应的属性信息，提取用户对象的属性信息赋值给资源类的第一对象包括：

[0014] 所述切面类根据所述资源类对应需求的属性信息，判断对应用户对象的 SESSION 中是否存在所述属性信息；

[0015] 如果存在，则从所述 SESSION 中提取用户对象的属性信息赋值给资源类的第一对象；

[0016] 如果不存在或者不全部存在，则从对应所述用户对象的属性信息表中，提取所述需求的属性信息中缺少的属性信息写入所述 SESSION 中，再从 SESSION 中将所述需求的属性信息赋值给资源类的对象。

[0017] 优选的，所述配置各资源类与各切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求包括：

[0018] 在 SPRING 框架的 XML 配置文件中定义各资源类与相应切面类的对应关系；所述切面类用于拦截访问所述资源类的访问请求；

[0019] 和 / 或，

[0020] 采用数据库表结构建立各资源类与相应切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求。

[0021] 优选的，所述资源类根据所述第一对象中的属性信息，从数据库中获取数据结果集包括：

[0022] 所述资源类获取所述对象中的各属性信息，传入所述资源类中的动态 SQL 语句执行并生成所述用户对象的数据结果集；所述动态 SQL 语句用于根据属性信息确定查询条件并进行查询。

[0023] 优选的，所述资源类获取所述对象中的各属性信息，传入所述资源类中的动态 SQL 语句时还包括：

[0024] 将所述第一对象中的属性信息，对当前属于用户对象的数据权限的各属性信息进行标记；

[0025] 进一步的，所述执行并生成所述用户对象的数据结果集之后还包括：

[0026] 当所述数据结果集不为空时，直接将数据结果集返回给所述用户对象所在终端；

[0027] 当所述数据结果集为空时，则根据各属性信息的标记，判断数据结果集是否根据属于所述用户对象的数据权限获得的；如果是，则生成所述用户对象没有相应权限的提示信息返回给所述用户对象所在终端。

[0028] 相应的，本发明还公开了一种基于 RBAC 模型扩展的数据权限控制系统，包括：

[0029] 配置模块，用于配置用户对象与各属性之间的对应关系，各属性与各资源类之间的对应关系；配置各资源类与各切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求；

[0030] 拦截模块，用于当一登录系统的用户对象发送访问请求以请求访问一资源类时，通过资源类对应的切面类拦截所述访问请求；

[0031] 赋值模块，用于所述切面类根据所述资源类对应需求的属性信息，提取用户对象的属性信息赋值给资源类的第一对象；

[0032] 数据获取模块，用于所述资源类根据所述第一对象中的属性信息，从数据库中获取数据结果集。

[0033] 优选的，所述赋值模块包括：

[0034] 判断模块，用于所述切面类根据所述资源类对应需求的属性信息，判断对应用户对象的 SESSION 中是否存在所述属性信息；

[0035] 第一赋值模块，用于如果存在，则从所述 SESSION 中提取用户对象的属性信息赋值给资源类的第一对象；

[0036] 第二赋值模块，用于如果不存在或者不全部存在，则从对应所述用户对象的属性信息表中，提取所述需求的属性信息中缺少的属性信息写入所述 SESSION 中，再从 SESSION 中将所述需求的属性信息赋值给资源类的对象。

[0037] 优选的，所述配置模块包括：

[0038] 第一配置模块，用于在 SPRING 框架的 XML 配置文件中定义各资源类与相应切面类的对应关系；所述切面类用于拦截访问所述资源类的访问请求；

[0039] 和 / 或，

[0040] 第二配置模块，用于采用数据库表结构建立各资源类与相应切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求。

[0041] 优选的，所述数据获取模块包括：

[0042] 第一数据获取模块，用于所述资源类获取所述对象中的各属性信息，传入所述资源类中的动态 SQL 语句执行并生成所述用户对象的数据结果集；所述动态 SQL 语句用于根据属性信息确定查询条件并进行查询。

[0043] 优选的，在所述数据获取模块还包括：

[0044] 标记模块，用于将所述第一对象中的属性信息，对当前属于用户对象的数据权限的各属性信息进行标记；

[0045] 进一步的，所述数据获取模块之后还包括：

[0046] 第一返回模块，用于当所述数据结果集不为空时，直接将数据结果集返回给所述用户对象所在终端；

[0047] 第二返回模块，用于当所述数据结果集为空时，则根据各属性信息的标记，判断数据结果集是否根据属于所述用户对象的数据权限获得的；如果是则生成所述用户对象没有相应权限的提示信息返回给所述用户对象所在终端。

[0048] 与现有技术相比，本发明包括以下优点：

[0049] 本发明将采用开源 SPRING 框架的 AOP 面向切面编程，将执行具体业务逻辑设置于资源类，将进行数据鉴权的逻辑设置于切面类，将业务逻辑与数据权限鉴权进行分离、解耦，在资源的整体框架不变的情况下，针对资源的业务逻辑完全与对资源的数据权限相分离，资源类无确切的、主动的知道需要获取何种属性信息，只需被动接收切面类传输的参数即可完成整个过程，因此，代码冗余量低，节省存储空间；另外，业务人员只需要关系其业务中各用户角色的数据权限，而不用需求技术人员根据业务人员的需求重新改编代码，提高了系统针对数据权限控制的灵活性，扩展性强。

附图说明

[0050] 图 1 是 RBAC 基本模型示意图；

[0051] 图 2 是本发明一种基于 RBAC 模型扩展的数据权限控制方法的流程示意图；

[0052] 图 3 是本发明的一种基于 RBAC 模型扩展后的系统模型示意图；

[0053] 图 4 是本发明一种基于 RBAC 模型扩展的数据权限控制系统的结构示意图。

具体实施方式

[0054] 为使本发明的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本发明作进一步详细的说明。

[0055] 参照图 2，示出了本发明一种基于 RBAC 模型扩展的数据权限控制方法，具体可以包括：

[0056] 步骤 100，配置用户对象与各属性之间的对应关系，各属性与各资源类之间的对应关系；配置各资源类与各切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求。

[0057] 为了更清楚的说明本发明的应用环境，在此首先介绍本发明基于图 1 的 RBAC 模型扩展后的模型结构，参照图 3，基于 RBAC 模型扩展后的模型结构示意图：

[0058] 其中对于本模型来说：

[0059] 1、本模型包含了 RBAC 模型中的核心模型 RBAC0、角色间继承 RBAC1 模型、责任分离关 RBAC2 模型；

[0060] 2、基于 RBAC 模型进行扩展，增加了数据权限约束配置，主要包括资源属性、资源操作条件、ACTOR 属性等信息；

[0061] 3、RBAC0 区域中的针对 ACTOR 进行扩展，将员工、组织机构、岗位、虚拟团队、系统都作为 ACTOR。

[0062] 对于图中各个实体，具体为：

[0063] 1、资源规格实体：定义资源种类，包括业务数据、共享服务等；

[0064] 2、资源实例实体：指的是资源规格的实例化；例如业务数据实例化：客户视图查询、客户资料管理等，共享服务实例化客户积分查询、客户缴费查询等；

[0065] 3、资源属性实体：定义某个资源实例的属性信息，并建立资源属性与 ACTOR 属性的对应关系；例如：登陆的员工编码、所属分公司等；

[0066] 4、操作：定义操作的基础数据，例如：查询、修改、删除等；

[0067] 5、资源操作：定义资源的各种可控制的操作信息；例如：客户资料查询、客户资料修改、客户资料删除等；

[0068] 6、资源操作条件：定义资源操作的约束条件信息；例如：客户经理只能查询其名下的客户信息、修改其名下的客户资料信息等；

[0069] 7、角色：定义人、系统在信息化应用软件系统中扮演的角色；例如：系统管理员、客户经理等

[0070] 8、角色继承：描述 A、B 两个角色的继承关系，如果 A 继承 B 角色，则 A 角色享受 B 角色的所有权限；

[0071] 9、角色继承约束：描述A角色继承B角色享受B角色的权限同时，进行一些权限的约束限制；

[0072] 10、ACTOR：定义数据权限的作用对象，包括用户、员工、组织机构、虚拟团队、系统等；

[0073] 11、ACTOR属性：定义ACTOR的属性信息；例如登陆系统的ACTOR所属本地网、服务区、营维中心等；

[0074] 12、ACTOR特权：描述除授予ACTOR角色权限范围之外的一些特殊权限；

[0075] 13、ACTOR约束：描述授予ACTOR的一些约束权限，包括约束限制授予ACTOR角色的部分权限。

[0076] 其中，对于权限配置实现思路为：

[0077] 1、建立资源规格：维护资源规格对应的业务实体等信息；

[0078] 2、配置资源操作：针对每一种资源规格配置其资源实例，配置资源操作信息，定义数据操作信息；

[0079] 3、配置资源属性：设置资源的属性、属性限制条件；通过属性限制条件设置，建立资源属性与登录系统的ACTOR属性的关系实现数据权限访问控制；

[0080] 4、配置资源操作条件：设置访问资源操作限制条件，限制条件为资源属性的子集；

[0081] 5、创建角色：建立角色信息；

[0082] 6、角色授权：给予角色分配对应的资源的据操作权限，此处要求，针对某一个资源，首先分配的功能操作权限，其次基于已分配的功能操作权限再分配其数据权限；

[0083] 7、ACTOR分配角色：针对具体的ACTOR分配对应的角色；

[0084] 8、ACTOR授权：针对具体的ACTOR直接分配其角色外资源访问的特权与约束；

[0085] 9、ACTOR属性配置：配置ACTOR属性信息，该属性与属性限制条件存在内在的关系，且是其子集；

[0086] 10、角色继承配置：包括配置角色继承关系、角色继承约束；A角色继承B角色后，A角色也享受B角色所有的权限；角色继承约束，主要是针对A角色的一些约束限制，约束其只能享有B角色的部分权限。

[0087] 在步骤100中，所述用户对象即为前述ACTOR，如前所述配置资源属性：设置资源的属性、属性限制条件；通过属性限制条件设置，建立资源属性与登录系统的ACTOR属性的关系实现数据权限访问控制；与ACTOR属性配置：配置ACTOR属性信息，该属性与属性限制条件存在内在的关系，且是其子集；即配置用户对象与各属性之间的对应关系，各属性与各资源类之间的对应关系。

[0088] 比如“客户视图”资源类，需要员工编码、员工所属分公司编码、员工职位编码、特殊权限标识等等。对于可访问客户视图的一用户对象(ACTOR)，可设置其属性信息与其员工编码、员工所属分公司编码、员工职位编码对应。在本实施例中配置用户对象与各属性之间的对应关系，各属性与各资源类之间的对应关系可由具体设计数据权限的业务人员进行配置。

[0089] 其中，配置各资源类与各切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求，可采用开源SPRING框架的AOP面向切面编程，将业务逻辑与数据权限鉴权

进行分离、解耦，本方法以数据权限鉴权作为横切面，实现数据权限的访问控制。其中，资源类为实现业务系统具体的业务逻辑，无需通过 set 语句将所需的 Actor 属性值信息 Set 到对应的对象中；切面类可以理解为，负责完成从 Session 中将 ACTOR 的属性信息 Set 到对应的资源属性实体表中配置的对应的 VO(value object，值对象）等对象中。该配置可由技术人员进行配置。

[0090] 所述配置各资源类与各切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求包括：

[0091] 步骤 S101，在 spring 框架的 XML 配置文件中定义各资源类与相应切面类的对应关系；所述切面类用于拦截访问所述资源类的访问请求；

[0092] WEB 服务器配置 Spring(Spring 也表示是一个开源框架，是为了解决企业应用程序开发复杂性由 Rod Johnson 创建的）AOP 的拦截器；最后在 Spring 的 XML 的 Extensible Markup Language，可扩展标记语言）配置文件中完成切面配置，即建立切面类与资源类的对应关系，定义当程序执行资源类之前要完成切面类的执行。

[0093] 和 / 或，步骤 S102，采用数据库表结构建立各资源类与相应切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求。

[0094] 可以采用数据库表结构方式，建立普通类与切面类的对应关系完成切面配置，即建立切面类与资源类的对应关系，定义当程序执行资源类之前要完成切面类的执行。

[0095] 基于上述配置，数据权限的控制过程包括：

[0096] 步骤 110，当一登录系统的用户对象发送访问请求以请求访问一资源类时，通过资源类对应的切面类拦截所述访问请求；

[0097] 在本发明实施中，对于用户以某一 id 登陆后，系统会将其与 actor（用户对象）对应，首先进行功能权限校验，比如 actor 具有查看“客户视图”的功能校验通过，那么在用户的显示界面可显示相应的功能界面和按钮，以接受用户进行后续的数据操作，比如查看具体数据等。

[0098] 那么在本实施例中，假如“张三”是海口分公司客户经理，查询“客户视图”时，只能查询海口分公司、且其名下客户的客户资料等信息。那么用户以“张三”登陆系统时，系统首先将“张三”与对应的 actor 对应，然后验证具有查询“客户视图“的功能，么在用户的终端界面展现“客户视图”功能界面。

[0099] 当用户访问“查询视图”的具体数据时，即访问“查询视图”资源类时，比如点击“查询视图”功能界面的查询按钮时，那么根据资源类与切面类的对应关系，系统调用所述切面类拦截所述访问请求。

[0100] 步骤 120，所述切面类根据所述资源类对应需求的属性信息，提取用户对象的属性信息赋值给资源类的第一对象；

[0101] 切面类拦截了所述访问请求后，即提取访问请求的目的资源类对应需求的属性信息，也即资源类对应的属性信息，然后根据资源类需求的属性信息去提取 actor 的相应属性信息赋值给资源类的对象。

[0102] 其中，所述切面类根据所述资对应的属性信息，提取用户对象的属性信息赋值给资源类的第一对象包括：

[0103] 步骤 S121，所述切面类根据所述资源类对应需求的属性信息，判断对应用户对象

的 session 中是否存在所述属性信息；

[0104] 在用户登陆时，服务器会针对用户对象维护一个 session（会话）以进行通信。

[0105] 比如“客户视图”资源类需要的属性包括：员工编码，部门编码，职位编码。那么对于前述“张三”对应的 actor，本步骤首先去 session 中查询是否存在张三的员工编码、部门编码、职位编码，如果没有，则进入步骤 S123。如果有则进入步骤 S122。从数据表中获取张三的员工编码、部门编码、职位编码，比如员工编码 1001、海口分部门编码 4601、客户经理编码 CM46011001 信息。

[0106] 步骤 S122，如果存在，则从所述 session 中提取用户对象的属性信息赋值给资源类的第一对象；

[0107] 如果存在，则获取张三的员工编码、部门编码、职位编码，比如员工编码 1001、海口分部门编码 4601、客户经理编码 CM46011001 信息，然后将张三的员工编码 1001、海口分公司编码 4601、客户经理编码 CM46011001 的值 Set 到客户视图的普通类中的 VO 对象 custViewMVO 对应的属性 staffId、regionId、custManager 中。

[0108] 本步骤 session 中存在相应属性信息可能是因为，张三本在次操作之前，可能访问其他某个资源类，而该资源类第一次也用到上述信息，如果是第一次使用，则通过步骤 S123 获取相应属性信息写入 session。

[0109] 步骤 S123，如果不存在或者不全部存在，则从对应所述用户对象的属性信息表中，提取所述需求的属性信息中缺少的属性信息写入所述 session 中，再从 session 中将所述需求的属性信息赋值给资源类的对象。

[0110] 另外，当 session 信息中不存在资源类所需求的属性信息，或者 session 中缺少资源类所需求的属性信息中的一个或者多个，那么则从对应所述用户对象的属性信息表中，提取所述需求的属性信息中缺少的属性信息写入所述 session 中，再从 session 中将所述需求的属性信息赋值给资源类的对象。

[0111] 比如对于前述“张三”例子，如果缺少“客户视图”所述的全部属性信息，那么本步骤从对应所述用户对象的属性信息表中提取张三的员工编码 1001、海口分部门编码 4601、客户经理编码 CM46011001 信息写入 session 中，然后张三的员工编码 1001、海口分公司编码 4601、客户经理编码 CM46011001 的值 Set 到客户视图的普通类中的 VO 对象 custViewMVO 对应的属性 staffId、regionId、custManager 中。

[0112] 对于缺少部分资源类所需的属性信息，其操作过程类似，在此不加以限制。

[0113] 步骤 130，所述资源类根据所述第一对象中的属性信息，从数据库中获取数据结果集。

[0114] 切面类将资源类所需的 actor 的属性信息赋值给资源类的对象后，则放弃拦截，通知资源类执行其逻辑，根据所述对象中的属性信息，从数据库中获取数据结果集。

[0115] 其中，所述资源类根据所述第一对象中的属性信息，从数据库中获取数据结果集包括：

[0116] 步骤 S130，所述资源类获取所述对象中的各属性信息，传入所述资源类中的动态 SQL 语句执行并生成所述用户对象的数据结果集；所述动态 SQL 语句用于根据属性信息确定查询条件并进行查询。

[0117] 资源类的 VO 等对象获得属性信息后，则获取 VO 对象的属性值信息，传入普通类中

的动态 SQL 语句中执行生成 Actor 的数据权限范围的数据结果集，比如将 regionId = 4601 且 custManager = CM46011001 做为 SQL 语句的查询条件筛选出张三权限范围内的客户列表。

[0118] 在本发明中，对于资源类的动态 SQL 语句查询获得的结果集，如果结果集不为空，则可直接返回结果集给用户对象所在终端；如果结果集为空，则说明可能数据库存在对应相应功能权限的数据，但是用户没有相应数据权限，或者数据库中对应相应功能权限根本就没有数据，那么可提示用户对象所在终端“没有查询到相应的数据或者用户数据权限不足”。

[0119] 另外，所述资源类获取所述对象中的各属性信息，传入所述资源类中的动态 SQL 语句时还包括：

[0120] 步骤 A130 将所述第一对象中的属性信息，对当前属于用户对象的数据权限的各属性信息进行标记；

[0121] 即标记所述动态 SQL 语句中的查询条件是否是对应用户对象的数据权限。

[0122] 从数据库中获取数据结果集之后还包括：

[0123] 步骤 A131，当所述数据结果集不为空时，直接将数据结果集返回给所述用户对象所在终端；

[0124] 步骤 A132，当所述数据结果集为空时，则根据各属性信息的标记，判断数据结果集是否根据属于所述用户对象的数据权限获得的；如果是，则生成所述用户对象没有相应权限的提示信息返回给所述用户对象所在终端。

[0125] 在步骤 A130 至 A132 实施例中，资源类将相应切面类传入的参数（资源类需求的 actor 的属性信息），作为查询数据库的查询条件进行搜索，那么对于数据库来说，其检索结果可能因为是数据库中根本不存在相应功能权限的数据而导致得到空集，或者是因为数据库中存在相应功能权限的数据但是该用户对象没有数据权限而导致的空集，为了使用户明确知道其是没有相应数据权限，那么当检索结果为空集时，则可根据各属性信息的标记，判断数据结果集是否根据属于所述用户对象的数据权限获得，如果是可返回当前用户对象没有相应数据权限的提示信息给用户对象所在终端，如果不是则可返回当前不存在实际数据内容的提示给用户对象所在终端；避免使用者认为服务器没响应，而一直重复发送请求，导致服务器资源浪费。

[0126] 本发明将采用开源 Spring 框架的 AOP 面向切面编程，将执行具体业务逻辑设置于资源类，将进行数据鉴权的逻辑设置于切面类，将业务逻辑与数据权限鉴权进行分离、解耦，在资源的整体框架不变的情况下，针对资源的业务逻辑完全与对资源的数据权限相分离，资源类无确切的、主动的知道需要获取何种属性信息，只需被动接收切面类传输的参数即可完成整个过程，因此，代码冗余量低，节省存储空间；另外，业务人员只需要关系其业务中各用户角色的数据权限，而不用需求技术人员根据业务人员的需求重新改编代码，提高了系统针对数据权限控制的灵活性，扩展性强。

[0127] 参照图 4，其示出了本发明一种基于 RBAC 模型扩展的数据权限控制系统，包括：

[0128] 配置模块 200，用于配置用户对象与各属性之间的对应关系，各属性与各资源类之间的对应关系；配置各资源类与各切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求；

[0129] 拦截模块 210，用于当一登录系统的用户对象发送访问请求以请求访问一资源类时，通过资源类对应的切面类拦截所述访问请求；

[0130] 赋值模块 220，用于所述切面类根据所述资源类对应需求的属性信息，提取用户对象的属性信息赋值给资源类的第一对象；

[0131] 数据获取模块 230，用于所述资源类根据所述第一对象中的属性信息，从数据库中获取数据结果集。

[0132] 其中，所述赋值模块包括：

[0133] 判断模块，用于所述切面类根据所述资源类对应需求的属性信息，判断对应用户对象的 session 中是否存在所述属性信息；

[0134] 第一赋值模块，用于如果存在，则从所述 session 中提取用户对象的属性信息赋值给资源类的第一对象；

[0135] 第二赋值模块，用于如果不存在或者不全部存在，则从对应所述用户对象的属性信息表中，提取所述需求的属性信息中缺少的属性信息写入所述 SESSION 中，再从 SESSION 中将所述需求的属性信息赋值给资源类的对象。

[0136] 其中，所述配置模块包括：

[0137] 第一配置模块，用于在 spring 框架的 XML 配置文件中定义各资源类与相应切面类的对应关系；所述切面类用于拦截访问所述资源类的访问请求；

[0138] 和 / 或，第二配置模块，用于采用数据库表结构建立各资源类与相应切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求。

[0139] 其中，所述数据获取模块包括：

[0140] 第一数据获取模块，用于所述资源类获取所述对象中的各属性信息，传入所述资源类中的动态 SQL 语句执行并生成所述用户对象的数据结果集；所述动态 SQL 语句用于根据属性信息确定查询条件并进行查询。

[0141] 在所述数据获取模块还包括：

[0142] 标记模块，用于将所述第一对象中的属性信息，对当前属于用户对象的数据权限的各属性信息进行标记；

[0143] 进一步的，所述数据获取模块之后还包括：

[0144] 第一返回模块，用于当所述数据结果集不为空时，直接将数据结果集返回给所述用户对象所在终端；

[0145] 第二返回模块，用于当所述数据结果集为空时，则根据各属性信息的标记，判断数据结果集是否根据属于所述用户对象的数据权限获得的；如果是则生成所述用户对象没有相应权限的提示信息返回给所述用户对象所在终端。

[0146] 需要说明的是，对于上述方法实施例而言，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

[0147] 对于系统或系统实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0148] 本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

[0149] 本发明可用于众多通用或专用的计算系统环境或配置中。例如：个人计算机、服务器计算机、手持设备或便携式设备、平板型设备、多处理器系统、基于微处理器的系统、网络PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境等等。

[0150] 本发明可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本发明，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0151] 最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。

[0152] 以上对本发明所提供的一种基于RBAC模型扩展的数据权限控制方法和系统，进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

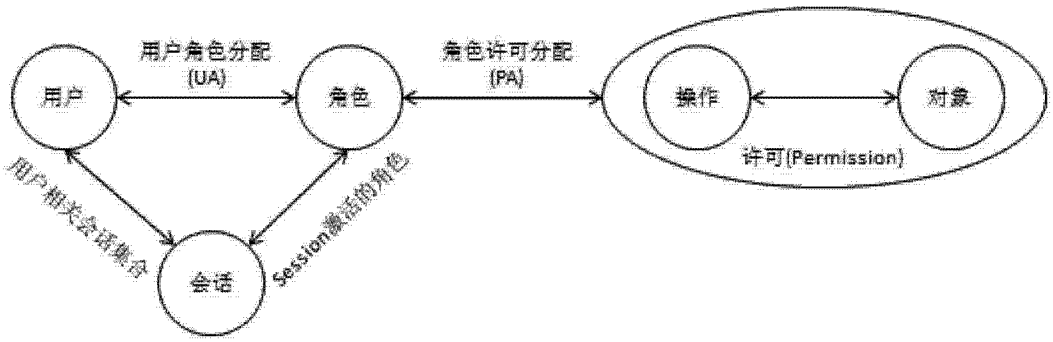

用户
用户角色分配
(UA)
角色
角色许可分配
(PA)
操作
对象
许可(Permission)
用户相关会话集合
会话
Session激活的角色

图 1

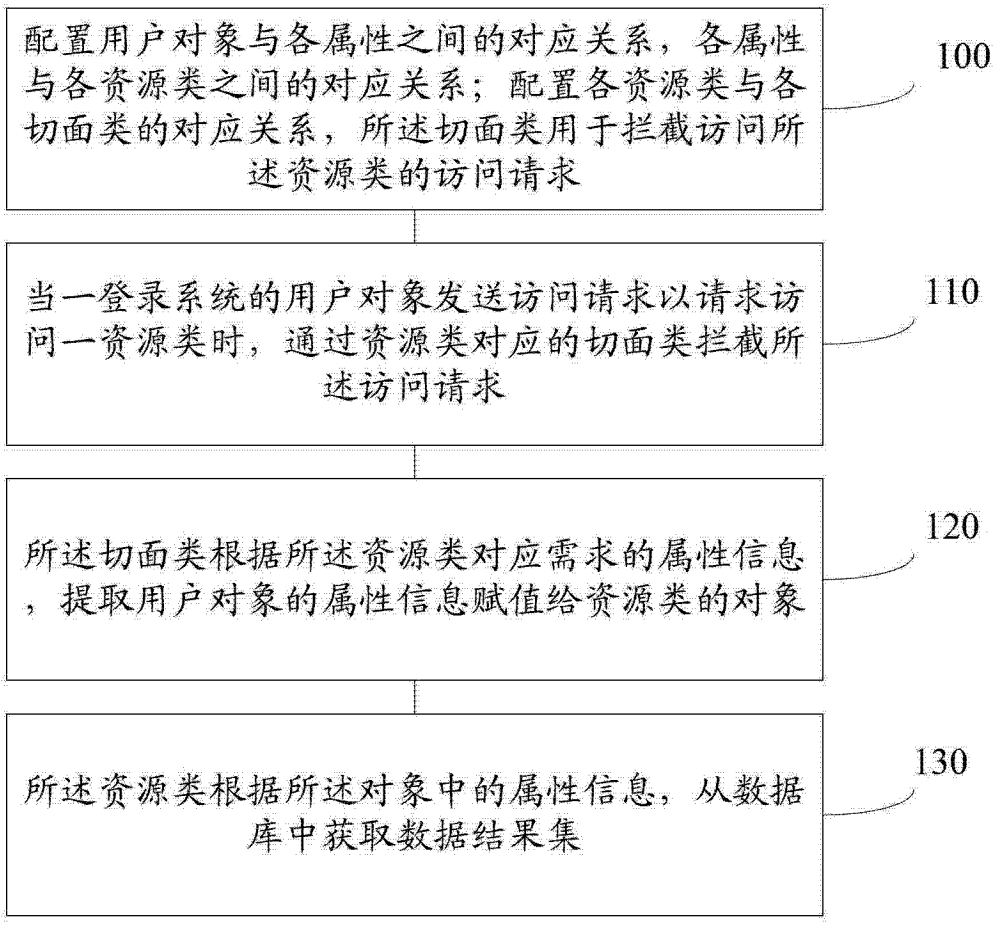

配置用户对象与各属性之间的对应关系，各属性与各资源类之间的对应关系；配置各资源类与各切面类的对应关系，所述切面类用于拦截访问所述资源类的访问请求
100
当一登录系统的用户对象发送访问请求以请求访问一资源类时，通过资源类对应的切面类拦截所述访问请求
110
所述切面类根据所述资源类对应需求的属性信息，提取用户对象的属性信息赋值给资源类的对象
120
所述资源类根据所述对象中的属性信息，从数据库中获取数据结果集
130

图 2

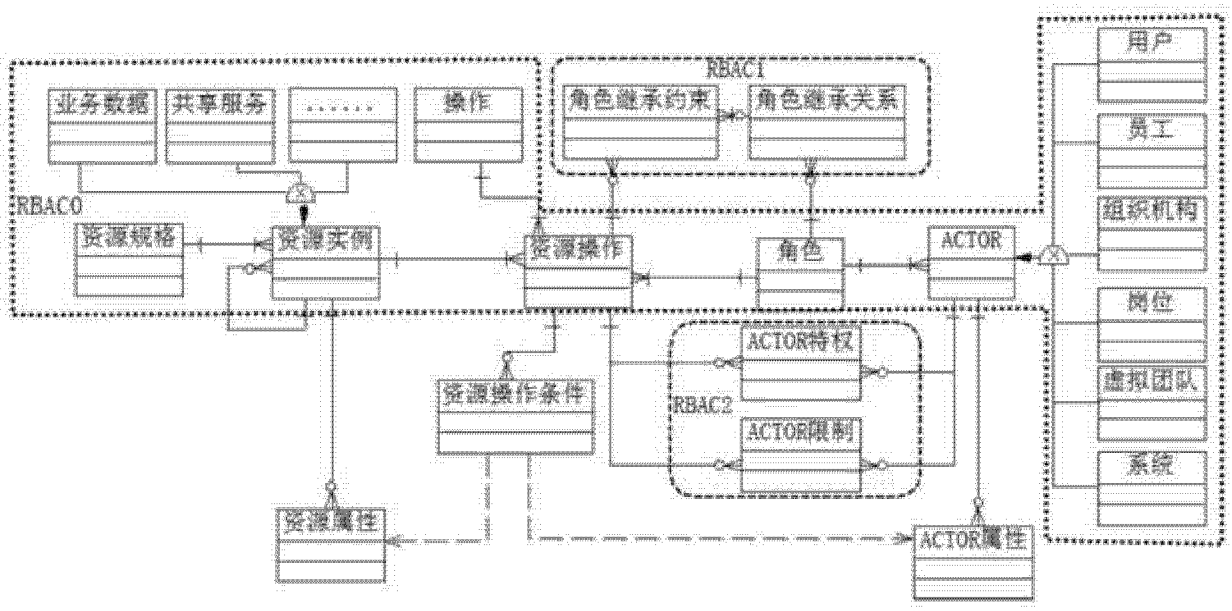

RBAC0
业务数据
共享服务
.....
操作
资源规格
资源实例
RBAC1
角色继承约束
角色继承关系
资源操作
角色
ACTOR
用户
员工
组织机构
岗位
虚拟团队
系统
资源操作条件
RBAC2
ACTOR特权
ACTOR限制
资源属性
ACTOR属性

图 3

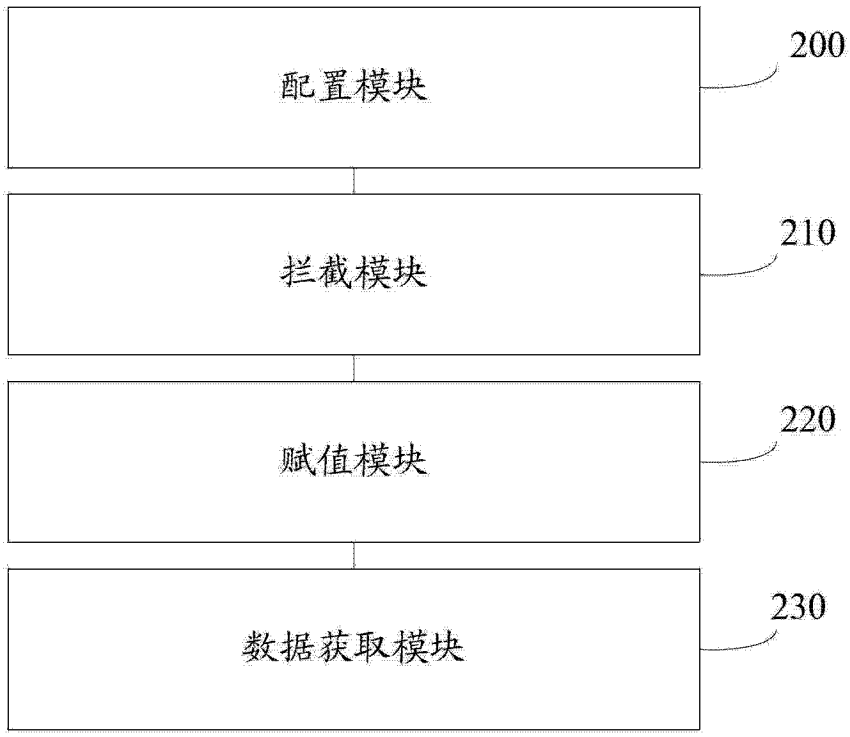

配置模块
200
拦截模块
210
赋值模块
220
数据获取模块
230

图 4