(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109522707 B
(45)授权公告日 2021.07.13

(21)申请号 201811276951.6
(22)申请日 2018.10.30
(65)同一申请的已公布的文献号
申请公布号 CN 109522707 A
(43)申请公布日 2019.03.26
(73)专利权人 珠海伟诚科技股份有限公司
地址 519080 广东省珠海市香洲区唐家湾镇大学路101号清华科技园二期H栋二楼
(72)发明人 刘玉成 李文帅 贺承明 陈金活
(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
代理人 俞梁清
(51)Int.Cl.
G06F 21/45(2013.01)
G06F 21/31(2013.01)

审查员 郭岚晞

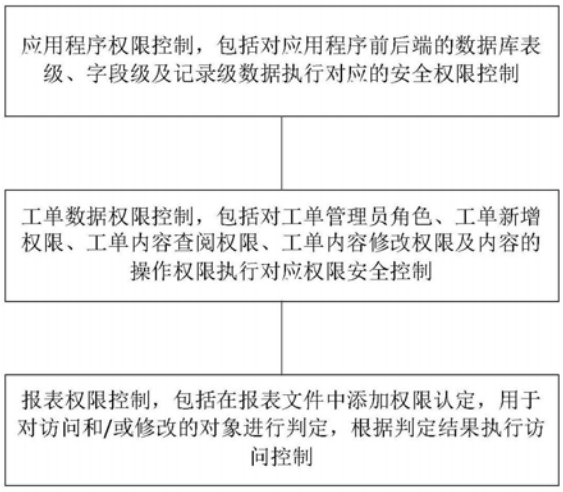
权利要求书2页 说明书7页 附图4页

(54)发明名称

一种基于角色和资源的用户数据读写安全权限控制方法及系统

(57)摘要

本发明的技术方案包括一种基于角色和资源的用户数据读写安全权限控制方法及系统，用于实现：应用程序权限控制，包括对应用程序前后端的数据库表级、字段级及记录级数据执行对应的安全权限控制；工单数据权限控制，包括对工单管理员角色、工单新增权限、工单内容查阅权限、工单内容修改权限及内容的操作权限执行对应权限安全控制；报表权限控制，包括在报表文件中添加权限认定，用于对访问和/或修改的对象进行判定，根据判定结果执行访问控制。本发明的有益效果为：自定义匹配性灵活定义各种复杂的字段或报表筛选条件；可以实现灵活多变的表级、字段级和记录级全方位矩阵式权限控制等。



CN 109522707 B

1.一种基于角色和资源的用户数据读写安全权限控制方法,其特征在于,该方法包括以下步骤:

应用程序权限控制,包括对应用程序前后端的数据库表级、字段级及记录级数据执行对应的安全权限控制;所述应用程序权限控制包括:通过资源权限定义表实现表和字段级权限控制;使用服务层接口对数据库的增删改查进行监控;基于Hibernate的HQL和SQL语句所提供查询入口,对任何数据库表的数据读取都必须通过该入口;对应用程序访问数据库所返回的数据进行调控,返回的数据为角色权限、数据源及查询对象;对网页应用程序的JavaScript访问的数据源进行唯一命名,若还包括多个子访问,则将唯一命名的数据源作为访问对象,并记录访问日志,添加与当前登录用户所属角色相关的固定筛选条件,可以通过后台控制台或系统日志文件内容查看生成的HQL语句;

工单数据权限控制,包括对工单管理员角色、工单新增权限、工单内容查阅权限、工单内容修改权限及内容的操作权限执行对应权限安全控制;

报表权限控制,包括在报表文件中添加权限认定,用于对访问和/或修改的对象进行判定,根据判定结果执行访问控制。

2.根据权利要求1所述的基于角色和资源的用户数据读写安全权限控制方法,其特征在于,所述应用程序具体为网页应用程序。

3.根据权利要求1所述的基于角色和资源的用户数据读写安全权限控制方法,其特征在于,所述通过资源权限定义表实现表和字段级权限控制具体包括:

通过对数据库表或持久化实体的资源权限定义表中指定角色与持久化实体的授权关系,以及增删改查四个选项分别控制对应角色针对指定数据库表的增删改查权限控制,同时,还可以采用正则表达式定义对应角色针对指定数据库表的可访问字段或采用排他方式的不可访问字段清单。

4.根据权利要求1所述的基于角色和资源的用户数据读写安全权限控制方法,其特征在于,所述使用服务层接口对任何对数据库的增删改查进行监控具体包括:

对于指定数据库表记录的增删改操作,通过对应的实体类增删改事件前定义的方法实现记录级权限控制。

5.根据权利要求1所述的基于角色和资源的用户数据读写安全权限控制方法,其特征在于,所述对应用程序访问数据库的角色权限、数据源及查询对象对访问时返回的数据进行调控包括:

创建记录级权限控制表实现记录级读取权限控制,通过数据源作为唯一标识,并通过固定过滤条件属性,对指定表的行级数据过滤。

6.根据权利要求1所述的基于角色和资源的用户数据读写安全权限控制方法,其特征在于,所述工单数据权限控制包括:

工单管理员角色权限,包括增加工单管理员角色,工单管理员角色用于负责流程的发布和更新、上传和下载、工单配置及工单调度;

工单新增权限,包括工单公共主表和私有主表记录的新增,根据工单的功能项执行单权限控制;

工单内容查阅权限,用于指定工单内容的查询通过调用接口实现,根据输入的单号查阅权限;

工单内容修改权限，指定工单主细表内容的更改和删除；

工单附件的操作权限，用于使用多个控制器对指定工单附件的上传、更新和删除。

7.根据权利要求6所述的基于角色和资源的用户数据读写安全权限控制方法，其特征在于，所述工单内容修改权限包括：

S81，通过查询实体定义表，判断要操作的实体资源是否为工单主表和工单明细表；

S82，若是工单主表，则根据SQL语句，将当前用户和工单号作为筛选条件查询该工单是否为当前用户的待办工作；

S83，通过工单号查询流程实例唯一标识查找对应流程变量，根据变量的值判定当前用户是否有对应的更改或删除权限。

8.根据权利要求1所述的基于角色和资源的用户数据读写安全权限控制方法，其特征在于，所述报表权限控制具体包括：

在BIRT报表请求头部增加用户关键字，用户关键字通过用户账号和当前日期进行加密，报表服务器端通过拦截器进行解密，然后查询报表权限定义表判定是否有权对资源进行访问；

对于记录级权限控制，若要启用，报表必须带用户账号参数，数值为当前用户账号，拦截器会将用户账号参数数值与用户关键字解密后获得的当前用户账号进行比较，若不一致，则不允许访问指定报表。

9.一种用于执行权利要求1-8任一所述方法的一种基于角色和资源的用户数据读写安全权限控制系统，其特征在于，该系统包括：

应用程序权限控制模块，用于对应用程序前后端的数据库表级、字段级及记录级数据执行对应的安全权限控制；

工单数据权限控制模块，用于对工单管理员角色、工单新增权限、工单内容查阅权限、工单内容修改权限及内容的操作权限执行对应权限安全控制；

报表权限控制，用于在报表文件中添加权限认定，用于对访问和/或修改的对象进行判定，根据判定结果执行访问控制。

一种基于角色和资源的用户数据读写安全权限控制方法及系统

技术领域

[0001] 本发明涉及一种基于角色和资源的用户数据读写安全权限控制方法及系统,属于计算机领域。

背景技术

[0002] 基于角色的权限访问控制(RBAC:Role-Based Access Control)作为传统访问控制(自主访问,强制访问)的有前景的代替受到广泛的关注。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。角色可依新的需求和系统的合并而赋予新的权限,而权限也可根据需要而从某角色中回收。角色与角色的关系可以建立起来以囊括更广泛的客观情况。

[0003] RBAC认为权限授权实际上是Who、What、How的问题。在RBAC模型中,who、what、how构成了访问权限三元组,也就是“Who对What(Which)进行How的操作”。

[0004] Who:权限的拥用者或主体(如Principal、User、Group、Role、Actor等等)。

[0005] What:权限针对的对象或资源(Resource、Class)。

[0006] How:具体的权限(Privilege,正向授权与负向授权)。

[0007] Operator:操作。表明对What的How操作。也就是Privilege+Resource

[0008] Role:角色,一定数量的权限的集合。权限分配的单位与载体,目的是隔离User与Privilege的逻辑关系.

[0009] Group:用户组,权限分配的单位与载体。权限不考虑分配给特定的用户而给组。组可以包括组(以实现权限的继承),也可以包含用户,组内用户继承组的权限。User与Group是多对多的关系。Group可以层次化,以满足不同层级权限控制的要求。

[0010] RBAC的关注点在于Role和User,Permission的关系。称为User assignment(UA)和Permission assignment(PA).关系的左右两边都是Many-to-Many关系。就是user可以有多个role,role可以包括多个user。

[0011] 对于用户业务数据的安全和权限控制,软件通常控制到数据库业务表级别就够了,如:项目经理应有项目表的CRUD(增删改查)权限。但若进一步细化权限控制,比如公司规定项目经理只负责项目的执行过程控制,不能查阅外接项目产值和相关合同额,这就涉及到项目表字段级(有时也称为列级)权限控制。另外,若有多个项目经理,分别负责管理不同的项目,项目经理只能编辑维护自己所负责的项目,不能查阅或修改其他人负责的项目,这就涉及到项目表记录级(有时也称为行级)权限控制。这些对于一个严密的管理信息系统是必须实现的数据安全和权限控制。对于API接口也应根据用户及其所属角色权限进行类似管理。

[0012] 对于报表,通常只需要将权限细化到模块级或报表级就可以了。

[0013] 对于文档的权限控制，通常与其所属资源权限一致，例如：对于资产的各种附件文档，只要有该资产的查阅权限，就可以查阅其相关文档。当然，也可以进一步通过文档密级及其所属类别进行进一步的权限控制。

[0014] 对于功能项的权限控制，统一采用RBAC进行控制。

[0015] 对于工单和流程的权限，员工起单权限通常根据系统统一的功能项权限控制即可。关于每个流程节点的查看和操作权限问题，还是要回归资源权限的统一管控，即：表级、字段级和记录级。对于一个权限严密的系统，不应该靠流程节点的变量定义就赋予新的权限。每个页面的权限只能基于角色和登录用户进行统一管控。流程节点的变量定义应该只是体现流程化分步骤、分阶段显示和操作原有权限内的对象内容，也就是要基于对象的状态变换图。如：借款单据的打印只能在单据内容填写完整、审批通过后才可打印；采购价格无论在哪个页面或工单上，都只有采购员及其主管、项目负责人等才可查看。原则上，为了简化资源权限管理，转让、代办、协办人也应该是有相应资源的权限。但若做得够细够好，只需保留下转让、代办、协办的授权记录，同保密邮件或文档一样，你有权限，但你授权另外一个没权限的人帮你处理，这就有了一个明确的授权，泄密责任由授权人承担，软件在打开工单时判定若是转让、待办或协办等过来的任务，同样有权限即可。

[0016] 现有技术的技术方案公开了一种控制数据访问权限的方法和系统(专利号为CN102063479A)，公开资料中介绍了一种与本发明近似的实现方案。该发明公开一种控制数据访问权限的方法和系统，该方法包括：预先针对数据库表建立数据资源类型表，在所述数据资源表中设置指定字段的过滤条件；根据所述数据资源类型表，筛选出符合所述字段过滤条件的数据记录，建立所述数据记录与用户之间的关联关系，并将所述关联关系保存到用户的访问权限表；接收用户对所述数据表的访问请求，查询该用户的访问权限表，并根据所述关联关系，获取该用户具有的访问权限；根据所述访问权限，对所述数据库表进行过滤，为该用户展现指定字段下符合过滤条件的记录。通过本发明能实现比字段级权限更细粒度的访问权限控制。

[0017] 现有技术存在以下不足

[0018] 1)权限控制不全面，没有覆盖到报表、工单流程、HQL、API接口等多种不同途径和入口的权限控制；

[0019] 2)没有细化到对数据库表CRUD(增删改查)不同组合的权限控制；

[0020] 3)权限直接授权给用户，而不是角色，这种授权方式不灵活，当涉及到用户离职、调岗等日常变动时，系统授权调整繁琐、复杂，工作量大；

[0021] 4)只采用简单字段过滤条件及其“与”或“或”的组合，难以满足复杂的数据记录过滤，实际上，数据记录的过滤往往不能仅通过数据库表本身的字段，还需要通过其多级关联表的其他多个字段取值进行多级关联查询过滤。

发明内容

[0022] 本发明提供本发明提供了一种基于角色和资源的用户数据读写安全权限控制方法及系统，实现通过基于角色和资源的用户数据读写安全权限控制，包括基于角色的用户权限控制、所有业务数据表(以及其下所有字段、任意筛选条件下的记录级数据)数据读写安全权限控制、报表查阅权限控制、Web API接口权限控制和工单权限控制，进而支持各种

复杂灵活、对用户数据安全有更高要求的业务系统数据安全全方位权限控制。

[0023] 本发明的技术方案包括一种基于角色和资源的用户数据读写安全权限控制方法，其特征在于，该方法包括以下步骤：应用程序权限控制，包括对应用程序前后端的数据库表级、字段级及记录级数据执行对应的安全权限控制；工单数据权限控制，包括对工单管理员角色、工单新增权限、工单内容查阅权限、工单内容修改权限及内容的操作权限执行对应权限安全控制；报表权限控制，包括在报表文件中添加权限认定，用于对访问和/或修改的对象进行判定，根据判定结果执行访问控制。

[0024] 根据所述的基于角色和资源的用户数据读写安全权限控制方法，其中应用程序具体为网页应用程序。

[0025] 根据所述的基于角色和资源的用户数据读写安全权限控制方法，其中特征在于，所述应用权限控制包括：通过资源权限定义表实现表和字段级权限控制；使用服务层接口对任何对数据库的增删改查进行监控；基于Hibernate的HQL和SQL语句所提供查询入口，进一步，对任何数据库表的数据读取都必须通过该入口；对应用程序访问数据库的角色权限、数据源及查询对象对访问时返回的数据进行调控；对网页应用程序的JavaScript访问的数据源进行唯一命名，若还包括多个子访问，则将唯一命名的数据源作为访问对象，并记录访问日志，添加与当前登录用户所属角色相关的固定筛选条件，若有问题，可以通过后台控制台或系统日志文件内容查看生成的HQL语句。

[0026] 根据所述的基于角色和资源的用户数据读写安全权限控制方法，其中通过资源权限定义表实现表和字段级权限控制具体包括：通过对数据库表或持久化实体的资源权限定义表中指定角色与持久化实体的授权关系，以及增删改查四个选项分别控制对应角色针对指定数据库表的增删改查权限控制，同时，还可以采用正则表达式定义对应角色针对指定数据库表的可访问字段或采用排他方式的不可访问字段清单。

[0027] 根据所述的基于角色和资源的用户数据读写安全权限控制方法，其中使用服务层接口对任何对数据库的增删改查进行监控具体包括：对于指定数据库表记录的增删改操作，通过对应的实体类增删改事件前定义的方法实现记录级权限控制。

[0028] 根据所述的基于角色和资源的用户数据读写安全权限控制方法，其中对应用程序访问数据库的角色权限、数据源及查询对象对访问时返回的数据进行调控包括：创建记录级权限控制表实现记录级读取权限控制，通过数据源作为唯一标识，并通过固定过滤条件属性，对指定表的行级数据过滤。

[0029] 根据所述的基于角色和资源的用户数据读写安全权限控制方法，其中工单数据权限控制包括：工单管理员角色权限，包括增加工单管理员角色，工单管理员角色用于负责流程的发布和更新、上传和下载、工单配置及工单调度；工单新增权限，包括工单公共主表和私有主表记录的新增，根据工单的功能项执行单权限控制；工单内容查阅权限，用于指定工单内容的查询通过调用接口实现，根据输入的单号查阅权限；工单内容修改权限，指定工单主细表内容的更改和删除；工单附件的操作权限，用于使用多个控制器对指定工单附件的上传、更新和删除。包括对工单管理员角色、工单新增权限工单内容查阅权限、工单内容修改权限及内容的操作权限执行对应权限安全控制

[0030] 根据所述的基于角色和资源的用户数据读写安全权限控制方法，其中工单内容修改权限包括：S81，通过查询实体定义表，判断要操作的实体资源是否为工，主表和工单明细

表;S82,若是工单主表,则根据SQL语句,将当前用户和工单号作为筛选条件查询该工单是否为当前用户的待办工作;S83,通过工单号查询流程实例唯一标识查找对应流程变量,根据变量的值判定当前用户是否有对应的更改或删除权限。

[0031] 根据所述的基于角色和资源的用户数据读写安全权限控制方法,其中报表权限控制具体包括:在BIRT报表请求头部增加用户关键字,通过用户账号和当前日期进行加密,报表服务器端通过拦截器进行解密,然后查询报表权限定义表判定是否有权对资源进行访问;对于记录级权限控制,若要启用,报表必须带用户账号参数,数值为当前用户账号,拦截器会将用户账号参数数值与用户关键字解密后获得的当前用户账号进行比较,若不一致,则不允许访问指定报表。

[0032] 本发明的技术方案还包括一种用于执行上述任意所述方法的基于角色和资源的用户数据读写安全权限控制系统,其特征在于,该系统包括:应用程序权限控制模块,用于对应用程序前后端的数据库表级、字段级及记录级数据执行对应的安全权限控制;工单数据权限控制模块,用于对工单管理员角色、工单新增权限、工单内容查阅权限、工单内容修改权限及内容的操作权限执行对应权限安全控制;报表权限控制,用于在报表文件中添加权限认定,用于对访问和/或修改的对象进行判定,根据判定结果执行访问控制。

[0033] 本发明的有益效果为:可以利用正则表达式强大的自定义匹配性灵活定义各种复杂的字段或报表筛选条件;可以实现灵活多变的表级、字段级和记录级全方位矩阵式权限控制;资源权限定义表或记录级权限控制表中只要针对某一数据库表或数据源有任一权限定义,则其他所有非授权角色都无权访问该资源;工单权限可以通过上述统一的资源权限控制,再加上工单所对应流程定义中变量和人工授权日志信息进行灵活的辅助控制;Web API接口可在平台级别统一实现针对各种数据库表的表级、字段级和记录级全方位矩阵式权限控制;可以在平台级别统一实现报表的权限控制;在服务器后台通过统一的服务层接口实现各种权限判断逻辑,杜绝不同途径、各种入口下的权限控制漏洞。

附图说明

[0034] 图1所示为根据本发明的总体流程图;

[0035] 图2所示为根据本发明的系统框图;

[0036] 图3所示为根据本发明实施方式的权限流程图流程图;

[0037] 图4所示为根据本发明实施方式的VRPT模块接口架构图;

[0038] 图5所示为根据本发明实施方式的报表查阅权限判定处理流程图。

具体实施方式

[0039] 以下将结合实施例和附图对本发明的构思、具体结构及产生的技术效果进行清楚、完整的描述,以充分地理解本发明的目的、方案和效果。

[0040] 需要说明的是,如无特殊说明,当某一特征被称为“固定”、“连接”在另一个特征,它可以直接固定、连接在另一个特征上,也可以间接地固定、连接在另一个特征上。此外,本公开中所使用的上、下、左、右等描述仅仅是相对于附图中本公开各组成部分的相互位置关系来说的。在本公开中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义。此外,除非另有定义,本文所使用的所有的技术和科学术语

与本技术领域的技术人员通常理解的含义相同。本文说明书中所使用的术语只是为了描述具体的实施例，而不是为了限制本发明。本文所使用的术语“和/或”包括一个或多个相关的所列项目的任意的组合。

[0041] 应当理解，尽管在本公开可能采用术语第一、第二、第三等来描述各种元件，但这些元件不应限于这些术语。这些术语仅用来将同一类型的元件彼此区分开。例如，在不脱离本公开范围的情况下，第一元件也可以被称为第二元件，类似地，第二元件也可以被称为第一元件。本文所提供的任何以及所有实例或示例性语言(“例如”、“如”等)的使用仅意图更好地说明本发明的实施例，并且除非另外要求，否则不会对本发明的范围施加限制。

[0042] 本发明的技术方案通过专门针对数据库表或持久化实体的资源权限定义表中指定角色与持久化实体的授权关系，以及CRUD四个选项分别控制对应角色针对指定数据库表的增删改查权限控制，同时，还可以采用正则表达式定义对应角色针对指定数据库表的可访问字段或采用排他方式的不可访问字段清单，进行更细化的字段级权限控制；通过记录级权限控制表统一定义指定角色针对HQL数据源及其子数据源中记录集的固定过滤条件和判定顺序，固定过滤条件包括服务器后台通过Web请求会话信息中的当前登录用户作为过滤条件，并且与用户自定义其他条件是“与”的关系，进而实现复杂、灵活、基于当前登录用户、Web前端不可更改的记录级读取权限控制；对于指定数据库表记录的增删改操作，通过对应的实体类增删改事件前专门定义的方法实现记录级权限控制；通过在报表权限定义表采用正则表达式定义指定角色可访问报表或采用排他方式的不可访问报表清单，来定义报表的权限控制；在报表请求中增加加密过的当前登录用户账号信息，报表服务对该信息进行解密，然后将用户账号和报表名作为参数通过Web请求验证该用户是否有指定报表的查阅权限。对于报表的记录级权限控制，若要启用，报表必须带当前登录用户账号作为参数，报表服务的拦截器会将该参数数值与报表请求中解密后获得的当前用户账号进行比较，若不一致，则不允许访问指定报表；通过工单流程变量和人工授权日志信息，在特定工单中授权流程中各人工节点任务处理人及其转让人、代理人、代办人或协办人等工单实际处理人和工单待阅接收人有查阅或操作指定工单相关数据的权限；

[0043] 图1所示为根据本发明的总体流程图。具体包括：应用程序权限控制，包括对应用程序前后端的数据库表级、字段级及记录级数据执行对应的安全权限控制；工单数据权限控制，包括对工单管理员角色、工单新增权限、工单内容查阅权限、工单内容修改权限及内容的操作权限执行对应权限安全控制；报表权限控制，包括在报表文件中添加权限认定，用于对访问和/或修改的对象进行判定，根据判定结果执行访问控制。

[0044] 图2所示为根据本发明的系统框图。具体包括：应用程序权限控制模块，用于对应用程序前后端的数据库表级、字段级及记录级数据执行对应的安全权限控制；工单数据权限控制模块，用于对工单管理员角色、工单新增权限、工单内容查阅权限、工单内容修改权限及内容的操作权限执行对应权限安全控制；报表权限控制，用于在报表文件中添加权限认定，用于对访问和/或修改的对象进行判定，根据判定结果执行访问控制。

[0045] 图3所示为根据本发明实施方式的权限流程图流程图。其大体流程如下所示：

[0046] 1)通过资源权限定义表实现表和字段级权限控制。通过专门针对数据库表或持久化实体的资源权限定义表中指定角色与持久化实体的授权关系，以及CRUD四个选项分别控制对应角色针对指定数据库表的增删改查权限控制，同时，还可以采用正则表达式定义对

应角色针对指定数据库表的可访问字段或采用排他方式的不可访问字段清单，进行更细化的字段级权限控制。

[0047] 2)对任何数据库表的数据执行增删改都必须通过统一的服务层接口。对于指定数据库表记录的增删改操作，通过对应的实体类增删改事件前专门定义的方法实现记录级权限控制；

[0048] 3)Hibernate的HQL和SQL语句暂时只实现查询功能，对任何数据库表的数据读取都必须通过该入口。新增记录级权限控制表实现记录级读取权限控制，通过数据源字符串作为唯一标识(若HQL中含有子查询，还会用到子数据源)，固定过滤条件属性用于实现指定表的行级数据过滤，例如：对于emploree角色，访问MsgInfo资源的固定过滤条件属性值为“receiverUserCode＝'{CurrentUserCode}'or receiverUserCode is null”。

[0049] 4)在api/hql对应控制器方法调用的服务程序中，以Web请求体作为输入，通过当前用户所属角色、数据源字符串和子数据源字符串遍历记录级权限控制表，若有固定过滤条件属性，则在生成的HQL中每个from数据源对应的where(没有要加)后增加固定过滤条件内容(注：其中的{当前用户编码}命名参数要替换为当前会话对应用户的UserCode)作为默认首要过滤条件，原有条件括起来用and连接，若当前用户所属角色同时拥有多种角色，以没有过滤条件为优先，或按照排序号顺序采用第一个符合条件的固定过滤条件内容。若所有定义的记录都不匹配，则不允许HQL读取数据，向Web前端返回错误。对于与当前登录人相关的诸如所属部门、所管项目等的筛选，也是按照当前登录人关联筛选。

[0050] 5)对于Web前端的JS文件只需要将数据源字符串唯一命名(如：datasource:'MsgInfo myBBSMsg')，若有子查询，只需要其from数据源(如：select myReadBBSMsg.readTime from MsgInfo myReadBBSMsg where…)在对应数据源下的同一HQL语句中唯一。然后，在记录级权限控制表新增记录，添加与当前登录用户所属角色相关的固定筛选条件，若有问题，可以通过后台控制台或系统日志文件内容查看生成的HQL语句。

[0051] 图4所示为根据本发明实施方式的VRPT模块接口架构图，图5所示为根据本发明实施方式的报表查阅权限判定处理流程图。根据图4和5，具体描述如下：在报表请求头部增加USER_KEY，通过登录账号和当前日期进行加密，报表服务器端通过拦截器进行解密，然后查询报表权限定义表判定是否有权对资源进行访问。

[0052] 对于记录级权限控制，若要启用，报表必须带登录账号参数，数值为当前用户账号，拦截器会将登录账号参数数值与用户关键字解密后获得的当前用户账号进行比较，若不一致，则不允许访问指定报表。

[0053] 本发明的技术方案还提供了一种替代方案。具体包括：若不用本技术方案，用户可以将BIRT报表嵌入业务系统应用程序，与业务系统应用程序深度集成和绑定，API接口可根据客户实际需求专门定制开发，Web页面改用服务器端动态网页自动生成等技术实现，这种方式的不足之处或劣势也很明显。

[0054] 应当认识到，本发明的实施例可以由计算机硬件、硬件和软件的组合、或者通过存储在非暂时性计算机可读存储器中的计算机指令来实现或实施。方法可以使用标准编程技术-包括配置有计算机程序的非暂时性计算机可读存储介质在计算机程序中实现，其中如此配置的存储介质使得计算机以特定和预定义的方式操作——根据在具体实施例中描述

的方法和附图。每个程序可以以高级过程或面向对象的编程语言来实现以与计算机系统通信。然而，若需要，该程序可以以汇编或机器语言实现。在任何情况下，该语言可以是编译或解释的语言。此外，为此目的该程序能够在编程的专用集成电路上运行。

[0055] 此外，可按任何合适的顺序来执行本文描述的过程的操作，除非本文另外指示或以其他方式明显地与上下文矛盾。本文描述的过程(或变型和/或其组合)可在配置有可执行指令的一个或多个计算机系统的控制下执行，并且可作为共同地在一个或多个处理器上执行的代码(例如，可执行指令、一个或多个计算机程序或一个或多个应用)、由硬件或其组合来实现。计算机程序包括可由一个或多个处理器执行的多个指令。

[0056] 进一步，方法可以在可操作地连接至合适的任何类型的计算平台中实现，包括但不限于个人电脑、迷你计算机、主框架、工作站、网络或分布式计算环境、单独的或集成的计算机平台、或者与带电粒子工具或其它成像装置通信等等。本发明的各方面可以以存储在非暂时性存储介质或设备上的机器可读代码来实现，无论是可移动的还是集成至计算平台，如硬盘、光学读取和/或写入存储介质、RAM、ROM等，使得其可由可编程计算机读取，当存储介质或设备由计算机读取时可用于配置和操作计算机以执行在此所描述的过程。此外，机器可读代码，或其部分可以通过有线或无线网络传输。当此类媒体包括结合微处理器或其他数据处理器实现上文步骤的指令或程序时，本文的发明包括这些和其他不同类型的非暂时性计算机可读存储介质。当根据本发明的方法和技术编程时，本发明还包括计算机本身。

[0057] 计算机程序能够应用于输入数据以执行本文的功能，从而转换输入数据以生成存储至非易失性存储器的输出数据。输出信息还可以应用于一个或多个输出设备如显示器。在本发明优选的实施例中，转换的数据表示物理和有形的对象，包括显示器上产生的物理和有形对象的特定视觉描绘。

[0058] 以上，只是本发明的较佳实施例而已，本发明并不局限于上述实施方式，只要其以相同的手段达到本发明的技术效果，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。在本发明的保护范围内其技术方案和/或实施方式可以有各种不同的修改和变化。

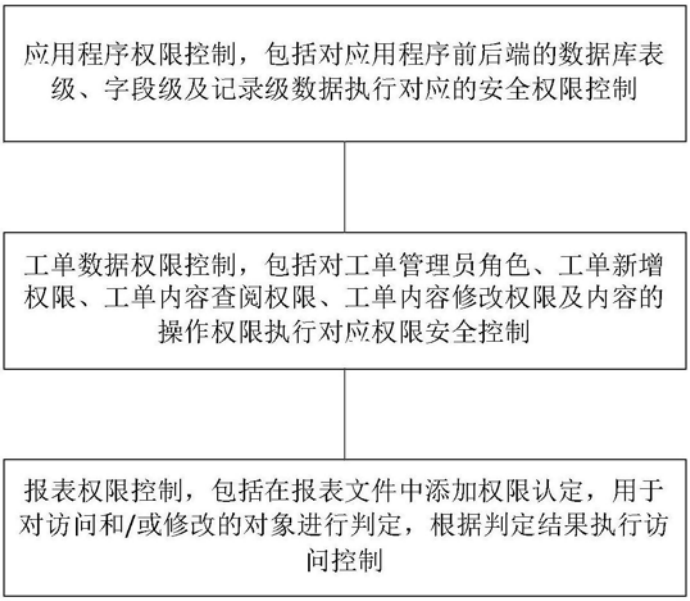

应用程序权限控制，包括对应用程序前后端的数据库表级、字段级及记录级数据执行对应的安全权限控制
工单数据权限控制，包括对工单管理员角色、工单新增权限、工单内容查阅权限、工单内容修改权限及内容的操作权限执行对应权限安全控制
报表权限控制，包括在报表文件中添加权限认定，用于对访问和/或修改的对象进行判定，根据判定结果执行访问控制

图1


应用程序权限控制模块
工单数据权限控制模块
报表权限控制

图2

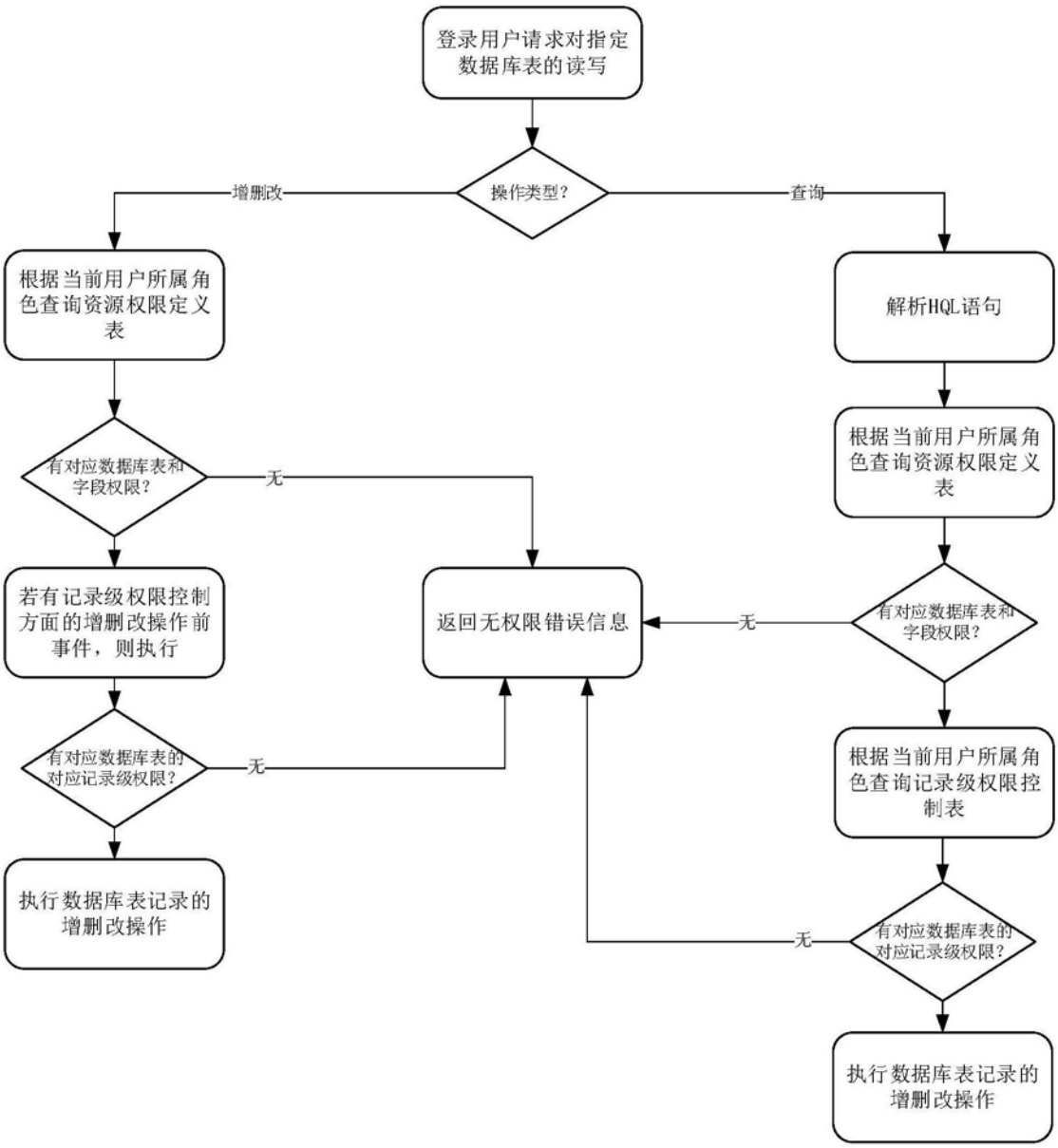

登录用户请求对指定数据库表的读写
操作类型?
增删改
查询
根据当前用户所属角色查询资源权限定义表
解析HQL语句
有对应数据库表和字段权限?
无
根据当前用户所属角色查询资源权限定义表
若有记录级权限控制方面的增删改操作前事件，则执行
返回无权限错误信息
无
有对应数据库表和字段权限?
有对应数据库表的对应记录级权限?
无
根据当前用户所属角色查询记录级权限控制表
执行数据库表记录的增删改操作
无
有对应数据库表的对应记录级权限?
执行数据库表记录的增删改操作

图3

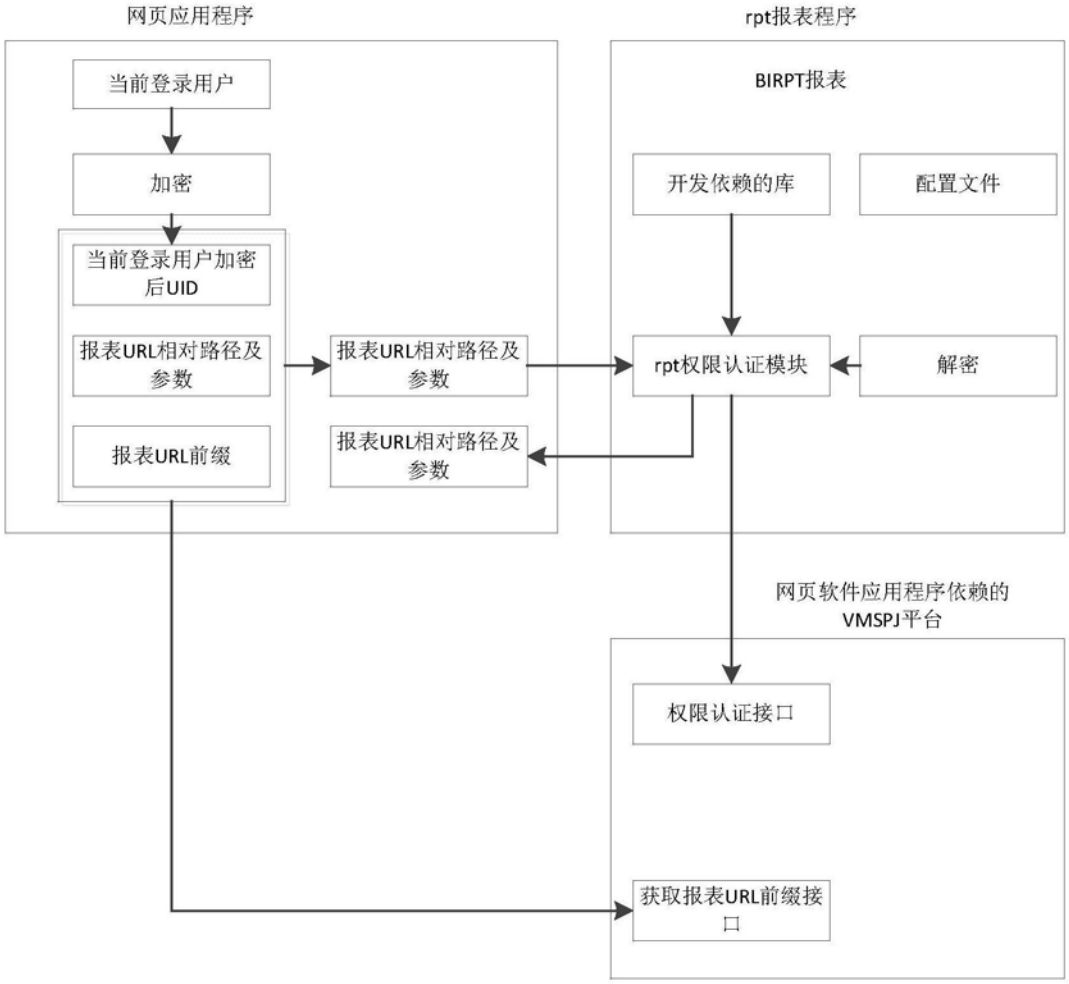

网页应用程序
当前登录用户
加密
当前登录用户加密后UID
报表URL相对路径及参数
报表URL前缀
报表URL相对路径及参数
报表URL相对路径及参数
rpt报表程序
BIRPT报表
开发依赖的库
配置文件
rpt权限认证模块
解密
网页软件应用程序依赖的VMSPJ平台
权限认证接口
获取报表URL前缀接口

图4

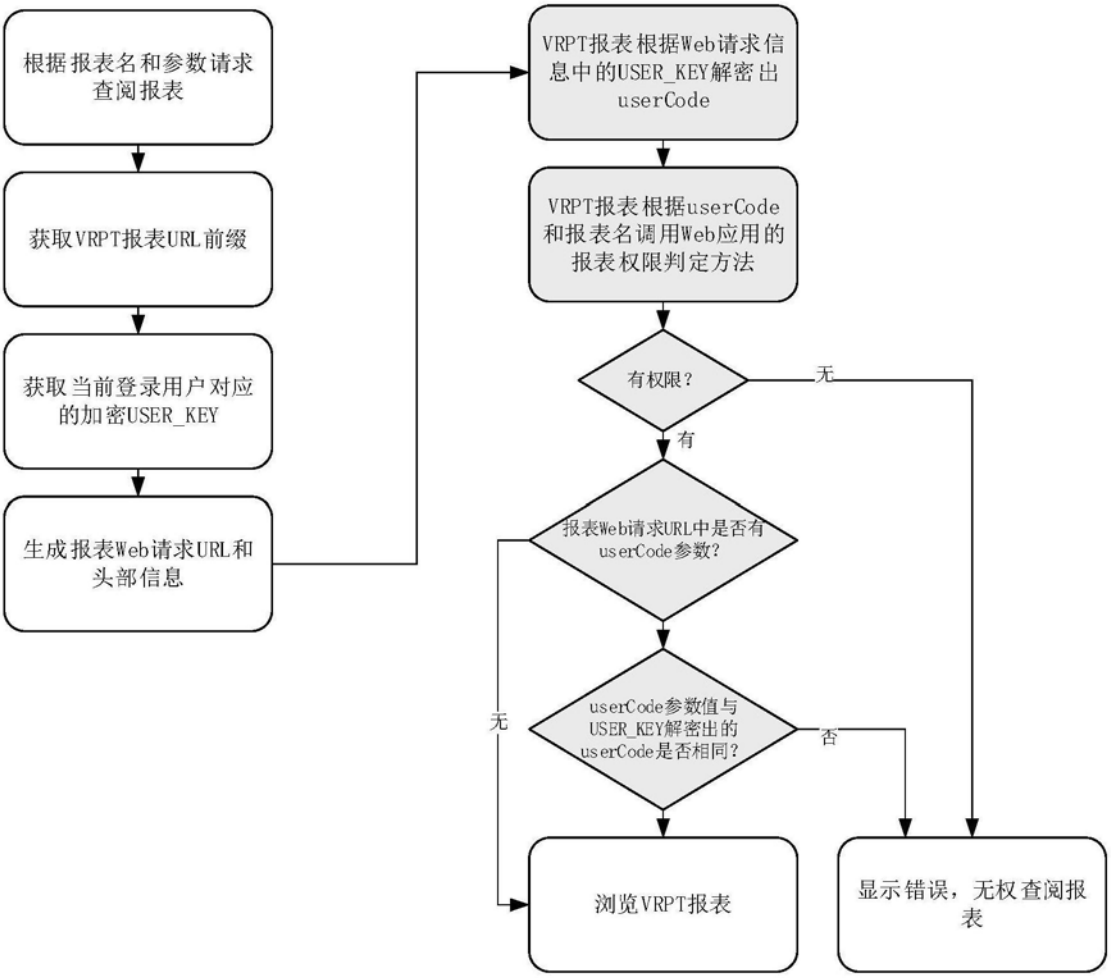

根据报表名和参数请求查阅报表
获取VRPT报表URL前缀
获取当前登录用户对应的加密USER_KEY
生成报表Web请求URL和头部信息
VRPT报表根据Web请求信息中的USER_KEY解密出userCode
VRPT报表根据userCode和报表名调用Web应用的报表权限判定方法
有权限?
无
有
报表Web请求URL中是否有userCode参数?
无
userCode参数值与USER_KEY解密出的userCode是否相同?
否
浏览VRPT报表
显示错误，无权查阅报表

图5