李德泉,阮宇智,杨润芝,等. 基于 RBAC 的气象多维数据权限管理模型的建立. 应用气象学报,2012,23(5):614-623.

基于 RBAC 的气象多维数据权限管理模型的建立

李德泉[1)]　阮宇智[1)]　杨润芝[1)]　马廷淮[2)*]

[1)](国家气象信息中心,北京 100081)　[2)](南京信息工程大学,南京 210044)

摘　要

在传统的基于角色访问权限管理(RBAC)模型基础上结合气象数据自身特点及共享服务中的权限控制需求,提出了一种符合气象资料管理特点的多维度权限管理模型。该模型充分考虑了气象数据进行资源共享时资料分类众多、层次化结构复杂、检索粒度不同等特点,有针对性引入了客体维度概念和更灵活的权限管理机制,较好地满足了气象部门数据共享服务系统建设的需求。该方案作为全国综合气象信息共享平台(CIMISS)数据服务权限控制模型的前期试验研究,构建一个多维数据权限管理原型系统用于数据访问控制。作为通用性模型,该模型可以延伸用于气象数据服务类系统应用,对确保数据库的信息安全、防止用户越权访问数据、保障管理信息系统的正常运行具有重要意义。

关键词: RBAC; 权限管理模型; 客体多维; 数据共享

引　言

权限管理是信息系统的重要环节,一个好的权限管理系统是成功的信息系统的重要因素,能更好地保护和使用本部门的信息资源,提高部门内信息系统的安全性。权限管理(access control)是指通过管理技术手段,允许被授权用户访问系统中特定对象或资源,同时拒绝非授权用户的访问服务。权限管理通常包括 3 个要素,即主体(subject)、客体(object)及权限(privilege)。其中,主体是指任何主动发出访问请求的实体,通常指系统用户,也可以是任何主动发出访问请求的程序、进程、服务等;客体是指所有受访问控制保护的信息资源实体,通常可以是被调用的程序、进程,也可以是要存取的数据、文件、目录等信息。例如,系统某个功能进程、某个 Web 页面、数据库中某个表中的记录等;权限是指主体对客体的执行特定操作的能力或特权,常见的如读、写、执行等。权限管理的技术要点就是切合主体、客体的自身特点,依据主体对客体的操作行为划分出不同的权限,设计一种权限判定机制,确保主体只能在其被赋予的权限范围内访问客体。

目前,国内外访问权限管理研究的重点仍然集中在自主访问权限管理(DAC, discretionary access controls)、强制访问权限管理(MAC, mandatory access controls)和基于角色的访问权限管理(RBAC, role based access controls)上。其中,基于角色的访问权限管理是目前公认的解决大型企业或部门的统一资源访问控制的有效方法[1-8]。

近些年,随着气象业务向纵深发展,气象系统内部以及民航、水利、农业等相关行业的气象数据共享需求不断增长,各类气象数据共享服务类业务信息系统迅速发展[9-18]。由于气象数据共享系统在技术实现手段上较多采用关系型数据库方式存储数据,共享网站方式服务,因此权限管理系统也多采用 RBAC 权限管理方案。

一方面,随着气象综合观测系统发展,进入共享服务的气象数据资料种类不断增加;另一方面,用户对数据服务需求也越来越延伸到策略层面,对数据的访问或获取逐步希望精确到要素级别;此外,气象

2011-11-10 收到, 2012-05-30 收到再改稿。

资助项目:国家气象信息中心 2010 年度青年科技基金项目"多维度权限控制模型的设计与开发"

* 通信作者, E-mail: thma@nuist.edu.cn

部门对内外用户的数据获取范围有相关规定予以界定[①②],并且这些规定也在不断修订完善,这些变化都要求投入使用的业务系统的权限管理必须能灵活适应这种趋势,而传统 RBAC 在管理上的粗放粒度、灵活性不足的劣势也逐步体现。因此,建立一个能灵活应对气象行业数据共享发展趋势的权限管理模型,对提高气象信息系统服务质量、系统安全性和业务系统整合效果都具有积极的推动作用。

1　权限管理模型的气象业务需求

权限管理机制的设计,通常与该部门的作业流程、安全策略存在紧密关联。其中,权限授予、管理的过程,必须要符合业务上作业流程的需求,并考虑本部门的组织层次结构和权责的区分。依据不同的职责,授予用户完成任务的最小权限需求。同时,应构建完善的权限管理机制,用以区分读取、修改、删除等对数据操作的行为。而由此产生的信息系统安全记录,可以作为信息安全管理的依据,从而有利于与信息系统的安全过程管理。

针对气象数据访问权限管理来说,客体主要指气象数据资源。传统的 RBAC 访问控制方式在应对气象部门需求的权限管理方面存在不足,其中最重要的问题就是应对精细授权力度较困难。不同用户的访问层次不同,对于具体到控件级别的权限管理,传统模型实现困难。此外,气象部门数据资源存在分类方法多样、层次结构多样等行业特点,传统模型没有针对此特点的解决方案,必须对原有模型进行改进。气象数据共享业务具有以下特点:①虽然目前气象部门针对数据访问授权还呈粗放式管理特点,但是数据访问策略灵活调整以及细粒度的访问控制将是未来趋势,尤其是数据共享平台和云服务不断投入运用后,为精确控制用户访问数据行为,对数据访问须细化至字段级。即数据权限管理最小粒度到数据的字段。②气象数据资料的特点是种类繁多,数据层次多样,各个层次结构相互制约,共同构成对用户访问权限的业务限定。按照气象行业标准,气象数据资料分 14 大类[19],每个大类又细分许多小类,共计 1000 余种数据形式,数据共享系统可以按照分类组织数据提供服务;同时,根据气象局现有规定,数据共享服务系统必须将数据资料按公开程度分为多个级别并做针对性服务[②]。显然这些现有的以及未来可能还会新增的各种业务制度、规范从不同角度出发对数据进行分类,共同组成一个框架对数据共享服务进行交叉限定,表现出复杂的层次结构,并间接提高了数据共享权限管理的难度,这也是本模型重点解决的问题。

因此,在基于角色的访问控制的基本思想上,对 RBAC 模型进行了改进和扩展,并引入了用户组、客体维的概念,设计出一个较为通用、高效和方便的权限管理模型——多维数据权限管理模型。

2　多维数据共享权限管理模型

2.1　模型框架

基于角色的访问权限管理(RBAC)包括 3 个实体:用户(user)、角色(role)和权限。其中,用户就是系统的使用者,是可以访问系统中的数据或资源的主体。角色是指具有相同权限的一类用户或组织,在系统使用中代表一种权利、资格和责任。引入角色概念的目的是为实现用户和权限的逻辑隔离。权限与角色关联,角色再与用户关联。用户和角色之间是多对多的关系,一个用户可以被赋予若干角色,一个角色也可以被赋予若干个具体用户。同样,角色和权限之间也是多对多的关系,一个角色可以具有多项权限,一个权限也可以赋予多个不同的角色。系统定义各种角色,每种角色可以完成一定的职能,不同的用户根据其职能和责任可以被同时赋予不同的角色,一旦某个用户成为某角色的成员,通过他所具有的角色的权限来判断其可访问的系统资源和对系统资源可以进行的操作[1-2]。

RBAC 的描述如下:u:user 用户;r: role 角色;P:privilege 权限。

某个用户 u 对某个资源 o 具有的权限记为 $P(u,o)$,则有如下关系:

$$P(u,o) = P_r(r(u),o)。\tag{1}$$

式(1)中,$P_r(r(u),o)$是通过用户 u 所赋予的角色 r 对资源对象 o 的权限。

本文提出的多维权限管理模型是在 RBAC 模型的基础上,引入用户组,并针对数据资源不同分类这一情况特别增加了客体维元素,从而形成了新的数据资源权限管理模型,如图 1 所示。

①中国气象局.气象资料共享管理办法(中国气象局第 4 号令).2001.

②中国气象局.涉外提供和使用气象资料审查管理规定(气发[2007]382 号).2007.

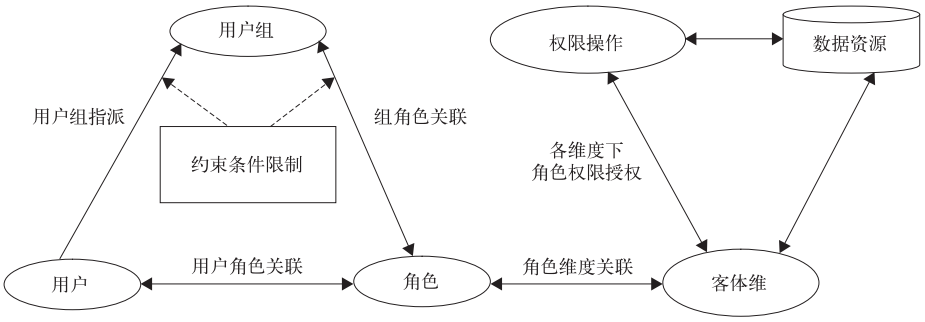

图 1 多维数据资源权限管理模型

Fig. 1 Multi-dimensional role access control model for data resource

从图 1 可以看到，传统 RBAC 仅包括用户、角色、约束条件和权限操作等元素，本模型增加了用户组和客体维两类元素。

2.2 用户组

用户的组织层次关系往往通过组来实现。一般将具有某种共同权限的人员构成一个用户组。一个新权限赋予某个用户组，就相当于赋予组内每个用户。同时，用户组与用户组之间也可具有层次关系，上层组的拥有权限大于下层组，同一分支的用户组的权限之间具有包含关系，即上级通常拥有下级的权限，以确保上级对下级工作进行监督管理。上层组权限可看成是其分支上所有下层各组的权限之和。同时规定，同层用户组之间不存在权限包含关系，不同分支的用户组之间也不存在权限包含关系。

2.3 客体型和客体维

引入客体维的概念，主要为了解决这一问题：数据资源共享时，当数据资源具有多重属性情况下，如何实现在不同属性维度上对数据进行权限有效控制。每个气象数据资源往往拥有多个属性，而属性往往具有一定业务涵义，例如是否对专业气象服务付费、质量情况、所属区域、要素属性、站点属性等（图 2）。

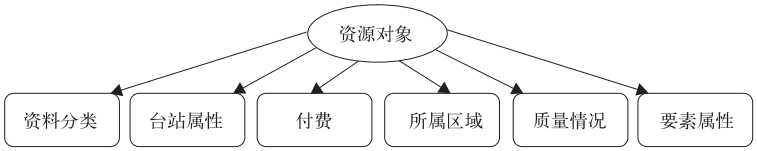

图 2 气象数据资源的多个属性示例

Fig. 2 Multiple properties of data resource

更进一步，这些属性又往往会作为权限判定的条件。例如，对“辽宁省的付费用户是否可以读取吉林省地面数据中国家基准站的温度字段”权限判定。判定条件中，用户需检查是否具有“辽宁省”、“付费”2 个角色，资源属性分为“地面类数据、区域（吉林省）、站点（国家基准站）、要素字段（温度）、付费”等判定条件，权限检查是否为“读”。

由此，将每个属性（或资源类型）定义为一个客体属性维（以下简称客体维）。每个资源都可以在每个客体维上描述对其的权限。对某一资源对象的权限操作，和该权限操作所在的客体维有关。分配角色权限，实现权限操作和角色之间的关联关系映射，必须涉及权限操作、资源和客体维 3 个要素。在此，特别强调，不同的客体维不允许相交。如果一个新属性与已有属性相交，那么必须将新属性与已有属性合并，以确保每个属性类型信息的独立性。

通过进一步分析还可看到，因为 RBAC 中对资源的权限管理是通过角色来传递的，也就是说在每个客体维上都可以定义一个角色在此维上对资源拥有某些权限。这个角色赋予某个用户的话，该用户就在此维上拥有了一定的权限。不同维上的角色相当于一个维角色分量，这些维角色分量组成一个集合，来共同表示出对资源拥有权限的一个完整角色。因此资源多个属性上权限问题就转化为资源的多个客体维问题，进而转化为角色的多维问题。判定一个用户对一个具有多个属性的资源的权限，就是判定在每个属性维度上这个用户被所赋予的维角色分量对该资源属性所拥有的权限。

下面利用图 3 来说明多维模型下将角色分解成相互独立的各属性维度上的维角色分量的直观意义。

图 3 中,假设某气象数据资源具有付费、台站两种独立属性,实线显示角色继承关系。如果设置一个角色在气象数据资源的这两种属性的任何可能情况下进行访问,则这个角色可能会是众多节点中的某一个,进行权限管理比较复杂。而如果设定付费、台站两种客体维,则权限判断可以在两个维度上分别进行,每个维度上的权限判断复杂度明显降低。可以看出,在付费客体维上,存在付费用户、免费用户两个维角色分量,在付费属性的权限层级结构上,付费用户继承免费用户的权限;在台站客体维上,存在台站用户、国家级站用户、省级站用户、区域站用户等多个维角色分量,在台站属性的权限层级结构上,区域站用户继承省级站用户权限,同时省级站用户继承台站用户权限。实际上,二维情况下所有角色的集合其实就是两个客体维上维角色分量的笛卡尔积。

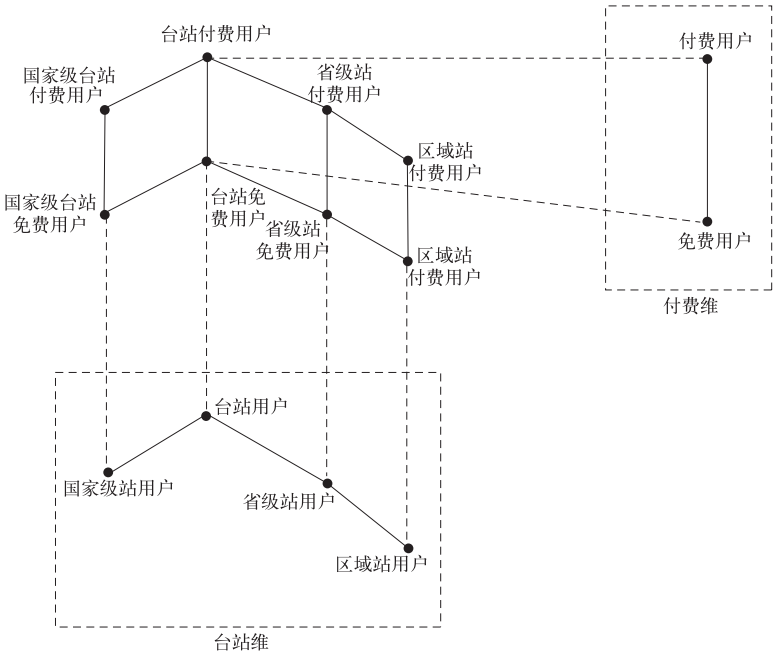

图 3　客体维的直观意义

Fig. 3　Concept of target object dimension

从图 3 可以看到,引入客体维并分解维角色分量的优势:存在多属性维度情况下,可以将角色定义与管理的复杂度降低。多属性维度情况下,如果直接实现对整个角色集的管理较困难,且属性维度越多越复杂,角色总数越多。但是,引入客体维并分解成维角色分量后,只需要角色集在每个客体维上的投影(维角色分量)进行管理即可。这样,整个复杂的角色集在不同维度上被分割为不同的相对较简单的角色集,并且每个维度上仍然可以使用 RBAC 模型进行权限管理。

因此,在本文提出的多维模型下,一个角色其实是多个资源客体维上的维角色分量共同组成的。设 d 为客体维数,则任意一个角色 R 都可以表示为

$$R=(r_1,r_2,\cdots,r_d)。\qquad(2)$$

在各个客体维上,资源的层次结构可能各不相同。例如,数据资源在站点属性客体维上,会依据站点所属级别建立层次结构,如图 4 所示。但在所属区域属性维上,则会依据数据采集所在的地域位置形成另外完全不同的层次结构。

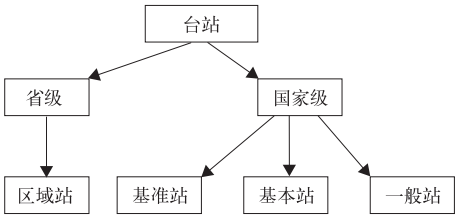

图 4　站点属性层次结构

Fig. 4　Hierarchy of station property for data source

2.4 多客体维权限判定模型

为形式化描述模型，本文采用四元组〈客体维，用户，资源，权限〉的形式定义用户在某个客体维约束条件的情况下，对资源的具有处理权限。该四元组的具体使用含义：如果在权限表中存在四元组〈D,U,O,P〉，则用户 U 在客体维 D 下，对于资源 O 具有权限 P。

在维度 D 下，如果可以推导出某个用户 U 对某个资源对象 O 具有的权限 P 的四元组集合记为 $P(\langle D,U,O,P\rangle)$，$P_u(\langle D,U,O,P\rangle)$ 是通过对用户 U 直接授权所确定的对资源对象 O 的具有 P 权限的四元组集合。$r(U)$ 表示用户 U 所赋予的角色 r。$g(U)$ 表示用户 U 所直接所属的用户组 g。

$P_r(\langle D,r(U),O,P\rangle)$ 是通过用户 U 所赋予的角色 r 对资源对象 O 的具有 P 权限的四元组权限集合。$P_g(\langle D,H_{\text{down}}(g(U)),O,P\rangle)$ 是通过用户 U 直接所属的用户组 g 及 g 之下所有直接或间接用户组而获得的对资源对象 O 的具有 P 权限的四元组权限集合。

$H_{\text{down}}(x)$ 函数获得在关于变量 x 的层级树形结构中，所有属于 x 分支及其以下的所有子分支上的变量组成的集合。与之相对应的，$H_{\text{up}}(x)$ 函数获得在关于变量 x 的层级树形结构中，所有属于 x 节点及其之上的所有父节点（直至包含根节点）的变量组成的集合。

则有如下关系：

$$P(\langle D,U,O,P\rangle) = P_u(\langle D,U,O,P\rangle) \cup P_r(\langle D,r(U),O,P\rangle) \cup P_g(\langle D,H_{\text{down}}(g(U)),O,P\rangle)。 \quad (3)$$

即 P 是 P_u,P_r,P_g 3 个集合的并集，即用户所属角色拥有的权限和用户本身及所在的用户组拥有的权限之和。

用户权限判定是在多个维度 D 下，在给定用户 U、资源 O 和权限 P 的前提下，判定用户 U 是否具有权限执行能力。

设客体维数目为 d。则在约束条件满足情况下，在某一个客体维 $D_i(i=1,\cdots\cdots,d)$ 下，用户 U 对资源在该客体维上的分量 O_i 的权限判定函数为

$$f_i(D_i,U,O_i,P) = \begin{cases} \text{True}, \{\langle D_i,U,O_i,P\rangle\} \subseteq P(\langle D_i,U,O_i,H_{\text{up}}(P)\rangle), \\ \text{False}, \{\langle D_i,U,O_i,P\rangle\} \not\subset P(\langle D_i,U,O_i,H_{\text{up}}(P)\rangle)。 \end{cases} \quad (4)$$

式(4)中，

$$P(\langle D_u,U,O,P\rangle) = P_u(\langle D_i,U,O_i,P\rangle) \cup P_r(\langle D_i,r_i(U),O_i,P\rangle) \cup P_g(\langle D_i,H_{\text{down}}(g(U)),O_i,P\rangle)$$

其中，$r_i(U)$ 是通过用户 u 所赋予的角色 r 在客体维 i 上的角色分量。$H_{\text{up}}(P)$ 是通过权限层次结构产生一个权限集合，该集合不仅包含权限 P 自身，也包含拥有该权限 P 的所有上层权限。

式(3)得出的结果中，True 表明具备权限，False 表明不具备权限。

式(3)是针对某一客体维所做的权限判定。在存在多个客体维情况时，多维权限判定用四元布尔函数 $F_{\text{md}}(D,U,R,R)$ 表示，True 表示有执行权限，False 表示没有执行权限。公式如下：

$$F_{\text{md}}(D,U,O,P) = f_1(D_1,U,O_1,P) \wedge f_2(D_2,U,O_2,P) \wedge \cdots \wedge f_d(D_d,U,O_d,P)。 \quad (5)$$

综上所述，可以看出本模型具有以下特点：①利用用户组增强组织机构管理，降低了系统权限管理的复杂度。②通过引入客体维实现对数据资源各种属性、类型及分类管理方法的抽象，支持在不同的资源属性进行不同的权限操作。也就是说，本模型中，权限操作与资源所属的资源类别、所具备的不同属性密切相关。③引入客体维简化了整个角色集的管理，并在理论上可以支持角色集在不同维上由不同的管理员负责管理该维上的角色。④分配角色权限，实现权限操作和角色之间的关联关系映射时，必须指定客体维、资源、操作权限。

2.5 模型的动态权限管理

作为 RBAC 模型的扩展，本模型中每个角色的继承关系都要求是一个绝对偏序关系，不能继承自己的子类，满足反对称性和传递性，防止产生继承循环。这是模型进行用户权限动态管理的前提。

本模型中用户权限的动态管理其实是通过角色的动态管理实现的。尤其在模型引入客体维后，角色的动态管理的重点就变成客体维及其上的维角色分量的角色继承关系的动态管理。以下简要说明角色的添加和删除，客体维的添加和删除，某个客体维上分量之间的角色继承关系的变更。

本模型下,添加一个角色时,必须指明待添加角色在当前已有客体维集合下的每个维角色分量。这些维角色分量的取值范围已经存在(因为在增加一种数据资源的新属性时,要求其维角色分量不能为空集,即至少包含一个该属性客体维度上权限最低的角色)。

删除一个角色时,必须先删除该角色在当前已有客体维集合下的每个维角色分量后,才能删除角色。

增加一个客体维时,必须同时建立维角色分量集合,该集合至少包含一个该属性客体维度上权限最低的角色。然后,针对当前已有的整个角色集中的每个角色,指定其在该客体维上的维角色分量。删除一个客体维时,必须先删除当前整个角色集中的每个角色在该维度上的维角色分量后,才能删除该客体维。

客体维上角色分量之间继承关系的变更,除了在该维度内部进行继承关系变更外,还会影响整个角色集。例如,在某个客体维上,在添加了一个新角色形成新的维角色继承关系后,可能根据需要进一步确定当前整个角色集中的每个角色在该客体维上的维角色分量是否更新为新增加的这个角色分量。在删除一个维角色分量形成新的维角色继承关系后,必须根据新的继承关系,指明由其父类或子类作为新的取值,将所有具有该分量的角色进行更新。

3　权限管理系统的设计与实现

3.1　系统结构

根据多维权限判定模型,构建了一个具备完整权限管理功能的原型系统并验证运行,该系统作为重点工程项目"全国综合气象信息共享平台(CIMISS)"的数据共享权限控制前期试验性系统,对登入平台的数据共享服务用户进行数据访问权限管理。

采用多维权限管理模型的数据访问权限管理系统的一般性框架如图 5 所示。

框架分用户与组的建立、权限授予、用户条件验证(如输入信息合法性验证、身份认证、资源和权限层次性完整性验证)、权限判定等部分。在这个框架中,主体发出的任何请求都要首先经过条件验证对请求进行判断,条件验证拒绝不合法的用户和没有申请权限的用户。在得到申请的用户中,在对各种权限进行操作时,会遇到各种权限问题再进行权限判定。

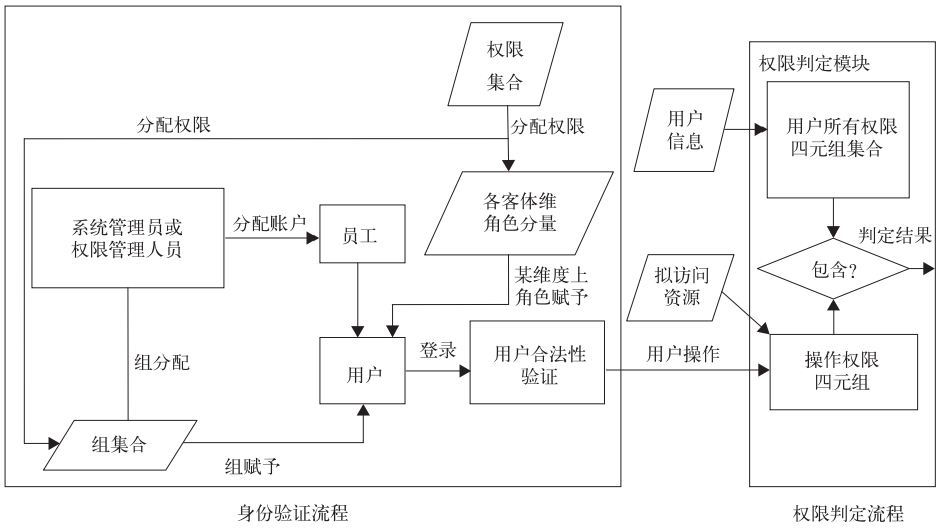

图 5　数据访问权限管理系统框架

Fig. 5　Framework of multi-objective dimension access controls

在 CIMISS 原型系统具体应用中,通过用户输入信息、权限管理数据库、用户条件验证组件、资源权限判定组件实现权限管理框架,实现数据资源访问权限管理流程。

①用户登录时输入用户名和密码或其他身份认证手段(例如认证卡认证、生物识别技术认证),用户输入信息提交给用户条件验证组件,该组件首先调用其输入合法性检查模块验证,对输入的用户名和密码或者其他输入信息进行合法性检查,只有验证为合法的信息才能进入下一步,否则报错终止执行。如果验证结果为合法的格式输入,则进入该组件的身份有效性认证模块。

②在验证输入信息的合法性后，进入用户条件验证组件身份有效性验证模块，在模块中，系统会进入用户信息数据表(Users)，通过调出用户信息表的用户名和口令验证是否是合法用户。只有合法用户才能登录进入系统。如果用户的输入信息与用户信息数据库表中的存储信息一致，则通过身份验证。否则报错返回。

③经过身份验证并检查动态约束条件许可和配置文件正常等必备运行条件后，用户条件验证组件完成工作，将用户信息传递给资源权限判定组件。

④资源权限判定组件通过用户信息表以及用户角色映射关系表(UserRoles)获得登录用户所属的角色，根据用户组信息表及用户组角色映射关系表(GroupRoles)获得当前用户由所属组的角色而获得的角色，再根据客体维角色表(SubRoles)确定用户每个角色在各个客体维下的客体维角色分量，再根据客体维角色权限设置表(DimensionRoles)确定用户在各个客体维下的所有权限记录，这样就构成各个维度下用户所属角色、所属组权限集合与用户自身权限集合之和，其表现形式是四元组〈dimension，user，resource，right〉的一组数据库记录集合。

⑤如果用户通过菜单或其他操作对数据资源进行某个访问权限操作，则根据资源的 ID 查询其是否包含在上一步生成的权限四元组集合中，若包含，则表示用户有权访问，资源权限判定组件返回通过权限过滤许可标志。

⑥通过资源权限判定组件的权限过滤许可后，用户就可以按照该权限访问数据资源。通过这样一个流程形成了一套较完整的气象数据资源共享系统的权限管理方法。

3.2 数据库表结构

为了实现多维模型下对用户访问的控制，需要在权限数据库中建立数据表。实现基于角色的权限管理模型，需要创建用户表、用户组表、角色表、权限表、用户到角色映射关系表、用户组到角色映射关系表、角色到权限映射关系表等多个数据表。本模型引入多维概念，因此增加一个客体维表。

用于气象数据共享访问的多维权限管理模型的实体关系(E-R)如图 6 所示，相关说明见表 1。需要指出的是，为方便说明，图 6 中各实体仅列出部分关键属性，在实际应用中，实体的属性值会有所增加。

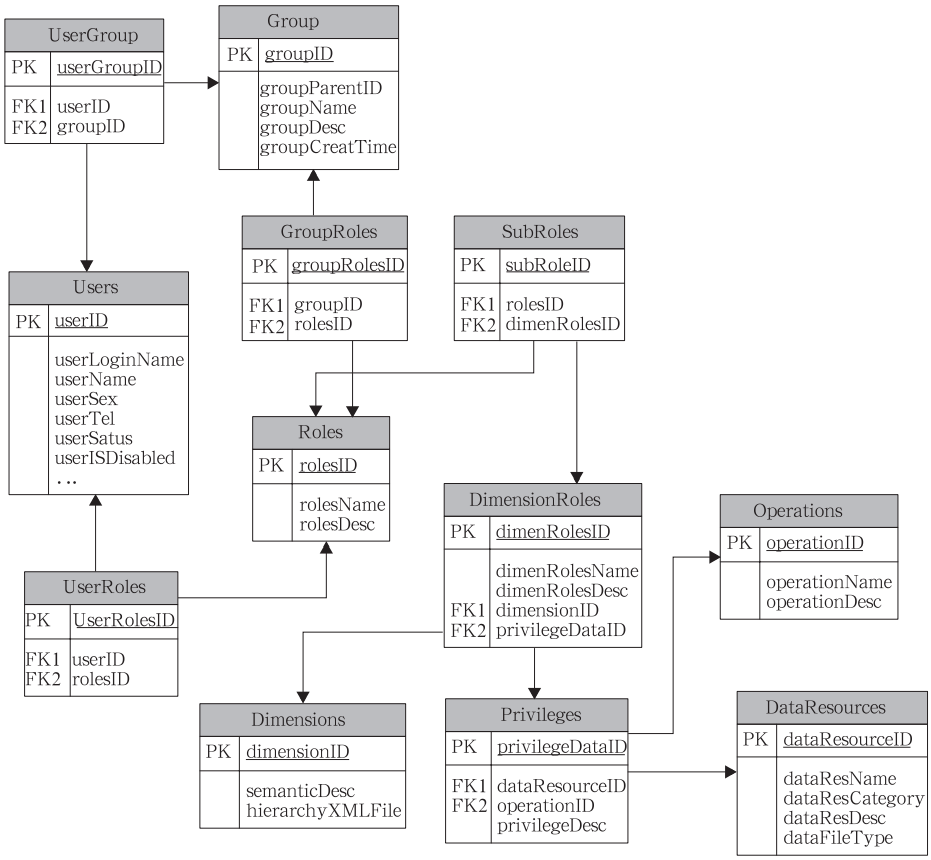

图 6 多维权限管理的 E-R 模型

Fig. 6 E-R model of multi-objective dimension access controls

权限管理数据库中共包括多个数据表,E-R 图显示了这些数据表之间的关系。表 1 对图 6 中数据表及重要字段进行简要介绍。

表 1　权限管理数据库表说明

Table 1　Description of the rights management database

数据表名称	说明	重要字段
Users	记录系统用户基本信息	userID: 用户 ID groupID: 所属的群组 ID
Roles	记录角色信息	rolesID: 角色 ID rolesName: 角色名称 rolesDesc: 角色描述
UserRoles	存储用户和角色的关系数据	UserRolesID: 用户-角色关联 ID
Groups	记录用户所属群组信息	groupID: 群组 ID groupName: 群组名称 groupParentID: 上级节点群组 ID
UserGroup	存储用户与群组的关系数据	UserGroupID: 用户-群组关联 ID
GroupRoles	存储部门与角色的关系数据	GroupRolesID: 群组-角色关联 ID
SubRoles	各个客体维角色分量与角色对应表	subRoleID: 角色-维角色分量关联 ID
DimensionRoles	存储每个维度的角色与权限的关系数据	dimenRolesID: 维角色分量 ID dimenRolesName: 维角色分量名称 dimensionID: 所属维的 ID
Privilege	记录对数据资源的具体权限	privilegeDataID: 权限值 ID privilegeDesc: 权限描述
DataResource	记录数据资源具体信息,名称、类别、地址等	dataResourceID: 资源 ID dataResName: 资源名称 dataResCategory: 资源类型 dataFileType: 资源文件类型
Operations	记录具体的操作信息,例如增加、修改等	operationID: 具体操作 ID operationName: 操作名称
Dimensions	记录客体维的定义信息	dimensionID: 所属维的 ID semanticDesc: 维应用场景描述 hierarchyXMLFile: 客体维层次结构 XML 文件

4　小　结

本文在具体分析了基于角色的权限管理的原理及气象数据共享系统权限管理设计目标的情况下,提出面向气象数据共享服务的一种通用的权限管理模型——多维数据共享权限管理方案,除增加用户组权限管理方法外,该模型有针对性引入客体维度概念,面向气象数据资料多种资源类型、多种属性类型的特点,设计了更灵活的权限管理机制和计算方法。该方案作为全国综合气象信息共享平台(CIMISS)数据服务权限控制模型的前期试验性研究,构建原型系统进行验证,并将作为 CIMISS 中数据共享系统的数据统一权限管理功能的关键部件,与其他模块进一步结合,实现业务应用。引入多维模式后的权限管理,简单实用,不仅提高服务系统应对实际业务变化的灵活性,简化了数据授权与维护的管理程序,间接提升数据的安全性及管理效率,而且其具有较强的气象部门通用性和服务特点,对确保数据库的信息安全,防止用户越权访问数据,保障管理信息系统的正常运行具有重要作用。

致　谢:本文工作得到国家气象信息中心熊安元、邓莉等的大力协助和支持,在此表示感谢。

参 考 文 献

[1] Sandhu R S, Coyne E J, Feinsteinh L, et al. Role-based access models. *IEEE Computer*, 1996, 29(2): 38-47.

[2] Crook R, Ince D, Nuseibeh B. Modeling access policies using roles in requirements engineering. *Information and Software Technology*, 2003, 45(14): 979-991.

[3] 杨柳,危韧勇,陈传波. 一种扩展型基于角色权限管理模型(E-RBAC)的研究. 计算机工程与科学, 2006, 28(9): 126-128.

[4] 胡林平. PDM 系统中权限管理方法的研究与应用. 航空计算技术, 2007, 37(1): 84-87.

[5] 刘建圻,曾碧,郑秀璋. 基于 RBAC 权限管理模型的改进与应用. 计算机应用, 2008, 28(9): 2449-2451.

[6] 朱磊,周明辉,刘天成,等. 一种面向服务的权限管理模型. 计算机学报, 2005, 28(4):677-684.
[7] 陈琛,陈学广,王煜,等. 一种基于改进 RBAC 模型的 EIS 权限管理框架的研究与实现. 计算机应用研究,2010,27(10):3855-3858.
[8] 何云强,李建凤. RBAC 中基于概念格的权限管理研究. 河南大学学报:自然科学版, 2011,41(3):308-311.
[9] 仪清菊,高梅,接连淑,等. 网络与气象信息共享研究. 应用气象学报,2001,12(1):127-128.
[10] 王国复,徐枫,吴增祥. 气象元数据标准与信息发布技术研究. 应用气象学报,2005,16(1):114-121.
[11] 吴焕萍,罗兵,王维国,等. GIS 技术在决策气象服务系统建设中的应用. 应用气象学报,2008,19(3):380-384.
[12] 祝婷,李湘. WMO 信息系统中气象元数据的设计与实现. 应用气象学报,2012,23(2):238-244.
[13] 马渝勇,徐晓莉,宋智,等. 省级气象信息共享系统的设计与实现. 应用气象学报,2011,22(4):505-512.
[14] 王国复,李集明,邓莉,等. 中国气象科学数据共享服务网总体设计与建设. 应用气象学报,2004,15(增刊):10-16.
[15] 周峥嵘,王琤,何文春. 分布式气象元数据同步系统的探索研究. 应用气象学报,2010,21(1):121-128.
[16] 高峰,王国复,喻雯,等. 气象数据文件快速下载服务系统的设计与实现. 应用气象学报,2010,21(2):243-249.
[17] 高峰,王国复,孙超,等. 后台管理模式在数据共享平台中的应用. 应用气象学报,2011,22(3):367-374.
[18] 苗传海,卢娟,张凯,等. 省级公众气象信息服务业务系统. 气象与环境学报,2008,24(5):48-51.
[19] QX/T 102-2009. 气象资料分类与编码. 气象行业标准(QX), 2009.

Privilege Management Model Based on RBAC for Meteorological Data Resource Service

Li Dequan[1)] Ruan Yuzhi[1)] Yang Runzhi[1)] Ma Tinghuai[2)]

[1)] (*National Meteorological Information Center*, *Beijing* 100081)

[2)] (*Nanjing University of Information Science & Technology*, *Nanjing* 210044)

Abstract

In recent years, Role-Based Access Control (RBAC) is apopular privilege management model at home and abroad, which has a distinct advantage than the other traditional access control technologies such as MAC and DAC. The basic principle of RBAC introduces the concept of role endued with authority between user and privilege, and user is also endued with role.

However, RBAC still has its limitations when it comes to applications in meteorological department of CMA with fine-grained data access control, and distinct definition. To meet the growing demand for data sharing, a novel access control management model must be built.

According to the requirements and characteristics of meteorological data sharing, a model is proposed for a general solution of data-sharing privilege management and multi-dimensional data-sharing privilege management, which is improved from RBAC model.

As a shared data resource, meteorological data have a large number of classifications, with a complex hierarchical structure, and very fine particle size of retrieving. In consideration of these comprehensive characteristics, this model introduces the concept of targeted object dimensions in RBAC on the basis of more flexible rights management mechanisms and calculation formula, which improves the security and flexibility of the data sharing services to meet the needs.

This model decomposes the fine-grained access privilege of sources by object dimension, and realizes access control of different levels from coarse-grained to fine-grained. The model can authorize directly not only the role but also the user, which greatly improves the flexibility and scalability. The model has been developed as re-pilot study in China Integrated Meteorological Information Sharing System (CIMISS),

which is the key project and the practical application of operational systems involved in the meteorological department. A prototype system is built to verify this model. Its deployment is helpful to manage the data retrieving and information access, and simplifies data authorization, maintenance management process, and improves data security. The model supports general security framework of the meteorological database information services, which prevents unauthorized user to access data. As a result, high stability and good security of the simple privilege management model are achieved, and security management information systems based on this model will play an important role in the meteorological data service in the future operations.

Key words: RBAC; privilege management model; multi-objective dimension; data sharing

《应用气象学报》征稿简则

《应用气象学报》(双月刊)是大气科学理论与应用研究的综合性学术期刊,主要刊登反映新理论与新技术在大气科学中的应用,以及大气科学理论与实践相结合,应用于各个有关领域的研究论文、业务系统和研究简报;国内外大气科学与应用气象科学发展中的新动态与新问题的探讨与评论;国内外重要学术会议或研究、业务活动的报道;气象书刊评介。

投稿要求和注意事项:

1. 论点明确、文字精炼。摘要请按文摘四要素(目的、方法、结果、结论)撰写,列出 3～8 个关键词,作者姓名请附汉语拼音,所在单位请附中、英文全名、地名、邮编。要求中文摘要为 200～400 字,英文摘要为 500 个单词左右(并请附对应的中文译文)。

2. 插图请插入文中适当位置,要求准确、清晰、美观。图中物理量、单位请勿遗漏,中、英文图题及说明写在插图下面。表格请采用三线表形式,并列出中、英文表题。

3. 参考文献请择主要的列入,并请按文中引用顺序标号。期刊书写格式:作者. 文章题目. 刊名,年,卷(期):起止页. 专著书写格式:作者. 书名. 译编者. 出版地:出版社,出版年:起止页.

4. 计量单位请按《中华人民共和国法定计量单位》列出,已废止的单位请换算成法定计量单位。

5. 科技术语和名词请使用全国自然科学名词审定委员会公布的名词。外国人名和地名,除常用者外请注原文。

6. **网上投稿(http://qk.cams.cma.gov.cn)请同时寄送全体作者签名的《承诺书》(请网上自行下载)。**稿件自收到之日起,将在 6 个月内决定刊用与否,来稿一经刊登,酌情收取版面费,并酌付稿酬。

7. 文中的数字及符号必须清楚无误,易混淆的外文字母、符号,请标注文种,大、小写,正、斜体,黑、白体,公式中的上、下标。

8. 本刊已加入“中国学术期刊(光盘版)”、“万方数据——数字化期刊群”和“中文科技期刊数据库”。本刊所付稿酬包含光盘稿酬和刊物内容上网服务报酬。凡向本刊投稿的作者(除事先声明外),本刊视为同意将其稿件纳入此两种版本进行交流。

欢迎投稿。投稿请登录 qk.cams.cma.gov.cn。

地址:中国气象科学研究院《应用气象学报》编辑部,邮政编码:100081; 电话:(010)68407086,68408638; 网址: qk.cams.cma.gov.cn; E-mail:yyqxxb@cams.cma.gov.cn, yyqxxb@163.com。