基于Web的工作流细粒度授权框架

肖 威,程文青,许 炜
(华中科技大学 电信系,湖北 武汉 430074)

摘 要:基于Web环境下的工作流系统面临复杂的数据安全管理难题。Web环境下的授权资源种类繁多、差异性大,需要控制模型具有较细的授权粒度,以保证工作流系统管理的安全性和灵活性。文中分析传统授权模型,结合Web系统基于表单的特点,提出一种由表单模型、授权模型、流程模型构成的工作流细粒度授权框架。并对该方案进行描述,给予实现。

关键词:工作流;授权;细粒度;Web;XML
中图分类号:TP311.5 **文献标识码**:A **文章编号**:1673-629X(2006)12-0240-04

A Web-Based Workflow Authorization Architecture with Fine Granularity

XIAO Wei, CHENG Wen-qing, XU Wei
(Electronics and Information Dept., Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract: One of the most challenging problems in large distributed workflow management system is the complexity of security administration. The complex kinds of resources in the Web requires the fine granularity authorization to guarantee the security and agility of workflow management system. This paper compares merits of the general authorization models in the Web-based workflow environment, combines the characteristic that Web is based on form, gives a new Web-based workflow authorization architecture with fine granularity which is assembled by form model, authorization model and flow model, and presents an instance of the system at last.

Key words: workflow; authorization; fine granularity; Web; XML

0 引 言

工作流技术通过分离过程逻辑与功能逻辑,极大提升了系统灵活性,越来越多的行业都将其业务建立于工作流管理系统(WorkFlow Management System, WFMS)[1]之上。Web方式作为最普遍的网络应用方式,被很多企业信息管理系统所采用。如何在Web环境下,保证工作流系统的授权访问的安全性成为关注的热点。目前存在很多访问控制模型,主流解决方案是基于角色的访问控制模型(RBAC)[2]和基于任务的访问控制模型(TBAC)[3]。

RBAC模型根据管理中相对稳定的职权和责任来划分角色,角色成为访问控制中访问主体和受控对象之间的桥梁。RBAC模型的缺点在于不限制权限的应用时间、次数,不考虑系统的上下文环境,导致被授权用户拥有权限与实际要求不符,容易产生安全隐患。文献[4~6]扩充RBAC模型的约束机制,解决了RBAC模型在工作流环境下的动态约束问题。

TBAC模型从应用和企业级的角度来考虑和解决安全访问控制问题,在任务处理的过程中提供动态的权限管理。在TBAC中,主体所拥有的访问权限并不是静态的,而是随着所执行任务的上下文环境发生变化。

但在基于Web的工作流环境下,上述两种访问控制模型都不完全适用。Web环境下的授权资源种类繁多、差异性大,需要访问控制模型具有较细的授权粒度,以满足授权管理的安全性和灵活性。而RBAC/TABC模型将授权资源假设为无差别的,未考虑授权资源的差异性,因此两者的授权粒度控制在任务级别,在细粒度的授权及授权粒度灵活调整方面,未能很好地满足Web环境下工作流的授权需求。为此,笔者提出一种全新的细粒度授权框架解决上述问题。

1 细粒度授权框架建模

文中提出的基于Web的工作流细粒度授权框架以XML描述的表单模型、流程模型、授权模型协同完成细粒度的工作流授权。其中,基于层次化资源对象模型的表单模型描述资源信息,维护与实际授权无关的资源集合;授权模型维护授权信息;基于授权规则的流程模型定义流程走向信息。

1.1 表单模型

1.1.1 层次化资源对象模型

对授权资源的灵活管理是细粒度授权框架的重要内容,细粒度的权限判断与授权资源关系密切。在资源的种类繁多的情况下,如何将资源信息抽象为一个通用模型十

收稿日期:2006-03-24
作者简介:肖 威(1981-),男,湖北十堰人,硕士研究生,主要研究方向为电子商务,工作流。

分重要。

授权粒度表示某一个角色所能够赋予权限的纵深程度。在工作流的执行过程中,授权粒度可以控制对某些资源对象的操作,也可能控制对某些对象的某些具体部分进行操作,即授权粒度需要细化到资源对象的具体组成部分。因此,授权粒度管理的核心在于对资源对象的管理,根据实际应用场景抽象为层次化的对象模型。层次化的资源对象的形式化描述如下:

用 $RO = \{ro_1, ro_2, \cdots, ro_p\}$ 表示资源对象类型集,其中资源对象类型依赖关系如下:$ro_1 \subset ro_2 \cdots \subset ro_p$。用 $O_i = \{O_{1(i+1)}, O_{2(i+1)}, \cdots, O_{j(i+1)}\}$ 表示资源对象,其中对象 O_i 是某个对象类型 ro_i 的实例;$O_{j(i+1)}$ 是对象 O_i 第 j 个组成部分,是对象类型 ro_{i+1} 的实例。对任意资源对象 O_i,可以用树型结构表示(见图 1)。

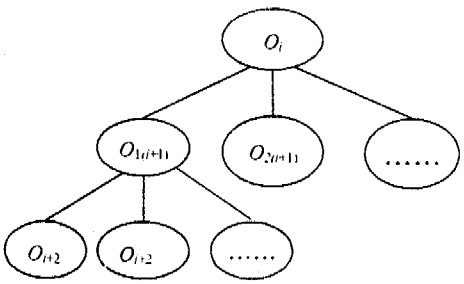

图 1　层次资源模型

显然,对于资源对象 O_i,可以用更小的资源对象类型 ro_{i+2} 表示为 $\{(O_{11(i+2)}, O_{12(i+2)}, \cdots, O_{1j(i+2)}), (O_{21(i+2)}, O_{22(i+2)}, \cdots, O_{2j(i+2)}), \cdots, (O_{j1(i+2)}, O_{j2(i+2)}, \cdots, O_{jj(i+2)})\}$。对资源对象 O_i 的访问授权转化为 O_i 的子类型对象集合的的访问授权。文中对层次资源模型的授权约束如下:资源对象 $O_{j(i+1)}$ 是资源对象 O_i 的组成部分,若对 O_i 有访问权限,则对 $O_{j(i+1)}$ 拥有访问权限。因此,通过对 O_i 的子类型对象集合进行授权,即完成对 O_i 细粒度的授权操作;同理,对 O_i 的父类型对象授权也实现对 O_i 的授权操作。通过调整授权对象的描述类型的高低级别,可以对授权粒度实现灵活控制。

层次资源对象模型的建立,将复杂的系统资源对象转化为结构有序的树型结构,增强了对资源对象的描述能力,极大简化了资源管理的复杂性,为工作流的细粒度授权奠定了基础。

1.1.2　表单信息建模及 XML 描述

根据层次化资源对象模型,框架将基于 Web 的工作流系统资源对象类型分为模块、表单、表单项三种。各资源类型的定义如下:

1) 表单项:工作流授权的最小单位,在 Web 系统中表现为页面控件。

2) 表单:工作流授权的基本单元,在 Web 系统中表现为待填写、处理的页面,用户对工作流的处理过程即该页面在多个用户之间传递、填充数据的过程;一系列表单项组成有特定业务意义的表单。

3) 模块:系统应用功能的抽象与聚集,是系统授权的最大单元;相似功能的一系列表单组成模块。

其中,表单作为核心资源类型,是工作流中传递信息的载体。在基于 Web 的工作流实现系统中,表单作为工作流中传递信息的载体,负责向客户端显示界面(UI),但表单本身无法携带任何信息。本框架采用 XML 描述表单模型,可以表达更多的信息,提升灵活性。表单模型包括表单层次信息、控件类型、映射信息和操作类型信息,各部分定义如下:

(1)表单层次信息:定义表单模块、表单、表单项的从属关系,分别用 module,form,item 标签表示。

(2)控件信息:指明此表单项的类型及主要属性,例如单行文本框、单选框等,以及对应的内容、显示风格。因为表单是以 HTML 的格式呈现的,文中的表单项类型限于标准 HTML 的显示类型。

(3)映射信息:维护表单项数据与后台数据库的映射,用 bean 标签表示。框架引入业务逻辑类进行维护,以减轻表单项与后台数据库的耦合。

(4)操作类型信息:定义表单每个表单项的显示规则,即该表单项是否可见(visible 标签)、是否允许修改(modify 标签)。操作类型信息可以灵活地定义表单在不同权限下的显示样式,是细粒度权限控制的关键。

表单模型的定义代码片断如下:

```
<! -功能模块定义->
<module name="" id=""></module>
<! -表单定义->
<form name="" id="">
  <! -表单项定义 ->
  <item name="productName" type="text" style="" bean
="com.wf.qulity.bad" visible="" "modify="" ">
  </item>
  .....
</form>
```

1.2　授权模型

授权模型定义工作流中流程节点的授权信息,由角色信息、表单编号和表单项操作类型信息组成。每个节点的授权信息形成一个授权模板,授权模板对应唯一表单模型。

XML 定义的授权模型示例如下:

```
<! -授权模型定义->
<auth id="" >
 <form id="" module_auth="" form_auth="">
  <item name="productName" visible="true" modify=
"false"></item>
  .....
 </form>
</auth>
```

其中,form 标签对应表单模型,属性 module_auth 定义模块级别的授权信息,form_auth 定义表单级别的授权

信息，item 标签对应表单模型中的表单项，属性 visible，modify 定义表单项的授权信息。当 module_auth，form_auth 属性值为 false，则授权控制到表单项，表现为表单项是否可见、是否允许操作，完成粒度到表单项的授权；当 module_auth 属性值为 false 且 form_auth 属性为 true，则权限控制到表单级别，表单项一律认为可见、可编辑；当 module_auth 属性为 true，则权限控制到模块级别。这种表单模型、授权模型结合的方式，可灵活地调整权限粒度，提高表单模型的充用性，降低系统授权的管理难度。

1.3 流程模型

流程模型是授权框架的核心，它将表单模型和授权模型结合起来，通过活动和业务授权规则，完整准确地描述一个完整的工作流程。

活动是流程模型的基本单元，定义流程在运转过程中所涉及的所有表单和表单之间的时间承接关系，并定义每个表单节点在流程运行过程的授权模型信息。活动分为简单活动、复杂活动和流程活动三种。简单活动表示信息的产生及操作，关联表单模型和授权模型。复杂活动用于建立顺序、并行、条件选择等流程控制信息。流程活动用于管理流程状态，包括挂起、重复、恢复和结束等状态。

业务授权规则是流程模型的核心环节。由于活动间存在业务逻辑约束，导致流程授权与业务逻辑关系紧密。如，某制造型企业的质检流程规定，废品率在 5% 以下由制造组长审阅，废品率在 5% ～10% 由制造课长审批，超过 10% 由经理审批。因此，在细粒度授权框架中，需对业务逻辑统一定义，实现动态授权机制，确保授权的准确性。业务授权规则是对其资源主体状态的判断或约束。业务授权规则可以抽象为(规则类型、资源主体、规则描述)三元组。规则类型包括计算、选择和行为三种，定义如下：

1) 计算规则：包括逻辑计算和数学计算，如规则“订单金额 =(订购数量 × 订单价格 + 样品费用) * 汇率”。计算规则是业务授权规则的基础，支持计算规则的嵌套。

2) 选择规则：选择规则与程序设计中的 if/else if/else 语句类似，描述流程的分支情况，需要调用逻辑计算规则或数学计算规则。前文的质检流程即为选择规则的典型应用。

3) 行为规则：行为规则是用于描述前两个规则难以描述的业务授权规则。

流程模型用 XML 描述，由流程引擎来进行实例化执行。流程模型的代码片段如下：

```
<! - 变量及常量定义 - >
<variables>
    <var name = "sum" type = "int" value = "com. wf. qulity. sum"/>
    <var name = "bad" type = "int" value = "com. wf. qulity. bad"/>
</variables>
<! - 条件定义，conditions 的条件一旦被满足，则执行相应流程 - >
<if>
    <conditions name = "checkQulity" >
        <condition name = "cond1" > bad/ sum&lt; = 0. 05</condition>
    </conditions>
    <action name = "制造组长审阅" role = "" form = "" auth = "" />
</if>
<elseif>
    <conditions name = "checkQulity" >
        <condition name = "cond1" > bad/ sum&lt; = 0. 10</condition>
    </conditions>
    <action name = "制造课长审阅" role = "" form = "" auth = "" />
</elseif>
<else>
    <action name = "经理审阅" role = "" form = "" auth = "" />
</else>
```

1.4 细粒度授权框架

系统中的表单模型、授权模型、流程模型均用 XML 描述并存储在数据库中。用户需要处理某个流程节点时，首先根据业务授权规则验证流程走向的正确性，然后解析流程文档中的表单模型号，获得并解析数据库中的表单模型，获得表单中每个表单项控件及其与具体数据库表的映射信息，自动完成数据映射；同时根据用户的角色信息，调用授权模型中对表单每个具体控件的操作类型信息，将表单模型信息与授权模型信息匹配，就可以知道当前用户对表单每个控件所具有的权限(隐藏、只读、编辑)，从而生成一份包含业务数据、符合权限的 XML 格式的表单文件。此时生成的 XML 文件只包含了表单要显示的内容，还需要有一个样式表文件。这里采用 XSL 样式表定义语言，将表单的显示格式在 XSL 文件中预先定义好，然后在 XML 表单中直接调用。通过上述的两个匹配过程和 XSL 定义，即可以实现对用户权限的细粒度控制。

2 系统实现

2.1 系统框架结构

如图 2 所示，整个系统主要包括五个模块：流程定义、表单定义、授权定义、工作流引擎及工作流数据库。流程定义模块用来对流程进行建模，将业务过程表示成计算机可读的定义，从而使业务过程能被工作流执行服务执行；表单定义模块用来创建 XML 表单，在该模块里定义好的表单将和流程定义模块中定义的流程结合起来进行处理；授权定义模块用以维护流程模型对表单模型的授权信息；工作流引擎是整个系统的核心，它用来激活并解释流程的定义，执行业务授权规则，对运行中的流程进行监控，同时负责和客户端的交互；工作流数据库用来存储流程定义、

表单定义、表单业务数据和当前运行流程实例等数据。

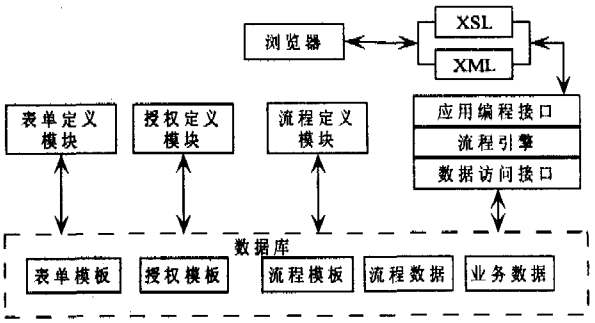

图 2　细粒度授权系统架构图

为降低授权操作难度,系统提供简单、易用的定制工具,将表单模型、授权模型、业务规则、流程模型定义四种功能集成。定制工具的程序流程如图 3 所示。通过定制工具,可以实现 XML 格式的流程文档的可视化编辑,极大减小了流程定义和维护的工作量。

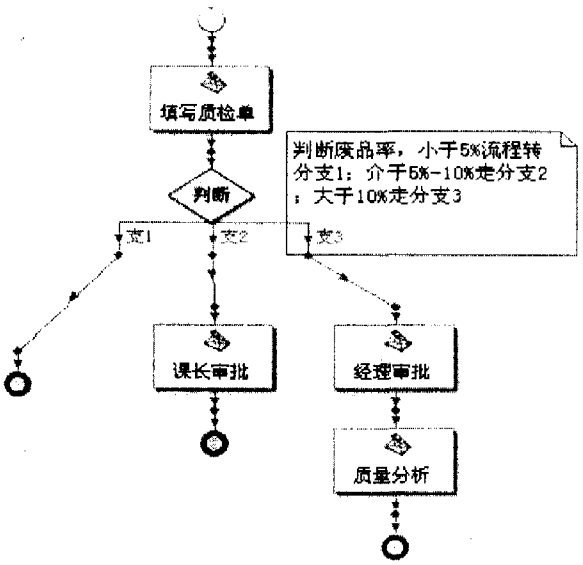

图 3　业务规则定制工具

2.2　性能优化

系统在实现时,考虑到 XML 解析时资源消耗大的缺点,进行了一系列的性能优化工作,从而大大降低了程序对计算机资源的依赖性,减少了冗余计算,适时释放了内存空间,其具体优化策略如下:

(1) 流程引擎的解析算法优化。

根据流程模型、授权模型、表单模型中的自定义标签的规律进行解析优化,保证基本数据解析操作的高效。

(2)XML 表单预处理。

针对系统中动态表单、静态表单并存的情况,在表单定义阶段将无动态业务授权逻辑的静态表单预先生成并存入数据库的特定表。在流程执行时无需动态创建即可获得 XML 表单,极大降低系统运行时的计算量。

(3)流程文档缓存。

当同一流程有多个实例被激活时,重复解析同一流程文档将导致效率低下。系统采用缓存技术,将已解析流程文档用关键字标识,缓存在系统内存中;系统激活同流程的实例时,则从缓存中获取已解析的流程文档,从而大大减少系统的内存消耗。

3　结束语

针对基于 Web 的工作流对授权模型的细粒度、灵活性的要求,提出一种工作流细粒度授权框架。框架通过表单模型、授权模型和流程模型的协同工作,较完善地解决了工作流授权的细粒度问题,具有一定的可扩展性、重用性和灵活性。在下一步的研究工作中,准备进一步完善流程模型的描述能力,同时优化系统执行性能,以适应复杂的企业流程需求。

参考文献:

[1] 范玉顺 . 工作流管理技术基础[M].北京:清华大学出版社,2001.

[2] Sandhu. Role-based Access Control models[J]. IEEE Computer, 1996,29(2):38-47.

[3] Bertino E, Bonatti P A, Ferrari E. TRBAC: A temporal role-based access control model[J]. ACM Transactions on Information and System Security,2001,4(3):191-223.

[4] 黄　建,卿斯汉, 温红子.带时间特性的角色访问控制[J].软件学报,2003,14(11) : 1944-1954.

[5] 王小明,赵宗涛,郝克刚.工作流系统带权角色与周期时间访问控制模型[J].软件学报,2003,14(11):1841-1848.

[6] Thomas R K, Sandhu R. Task-based authentication controls (TABC):A family of models for active and enterprise-oriented authentication management [C]//In: Proc of the IFIP WG1113 Workshop on Database Security. London : Chapman & Hall,1997:166-181.

(上接第 239 页)

参考文献:

[1] 程　光,龚　俭,丁　伟.基于抽样测量的高速网络实时异常检测模型[J]. 软件学报,2002,13(4):594-599.

[2] Yang Xiang,Zhou Wanlei,Chowdhury M. A Survey of Active and Passive Defense Mechanisms against DDoS Attacks[R]. Australia:Deakin University,2004.

[3] Bellovin I J. Pushback:Router-Based Defense Against DDoS Attacks[C]//In Proceeding of Network and Distributed System Security Symposium. San Diego, USA:[s.n.],2002.

[4] Mohiuddin S, Hershkop S, Bhan R, et al. Defending against a Large Scale Denial of Service Attack[C]// In Proceedings of the 3rd Annual IEEE Information Assurance Workshop. New York:United States Military Academy West Point,2002.

[5] Li M, Chi C. Decision Analysis of Statistically Detecting Distributed Denial-of-Service Flooding Attacks[J]. International Journal of Information Technology and Decision Making,2003,2(3):397-405.