基于工作流用户权限管理模型的研究与设计

蒋 永[1],蒋玉明[1],彭思达[2]
(1.四川大学 计算机学院,四川 成都 610065;
2.77680部队57分队,西藏 林芝 860501)

摘 要:为了能够适应多用户协同工作以及用户权限动态分配的需求,并满足企业越来越精细的明确分工,保证企业信息化平台协调业务工作的方便快捷。首先从用户权限管理的主要形式进行统计描述,并分析了早期用户权限的实现形式;在对比一般应用系统的用户权限管理形式的基础上结合企业级信息管理系统的管理形式着重从工作流系统中用户的分类设计与角色分配进行研究;主要针对用户权限的灵活管理与随着业务需求变化而动态分配进行分析研究与设计;最终实现了用户权限动态分配的设计模式。

关键词:工作流;信息系统;用户管理;动态分配
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)01-0161-04

Research and Design of User Rights Management Model Based on Workflow

JIANG Yong[1], JIANG Yu-ming[1], PENG Si-da[2]
(1. Computer College, Sichuan University, Chengdu 610065, China;
2. Detachments 57, Troops 77680, Linzhi 860501, China)

Abstract: In order to be able to work well together as well as multi-user dynamic allocation of user rights requirements, and meet the growing refinement of a clear division of labor to ensure that enterprise information platform for the coordination of operational work of the convenient and quick. First, it describes the main form of user rights management, and analyses the realization forms of early user rights. Then, on the basis of contrasting with the form of general application management system of user rights and combining enterprise-class information management system's managing models, emphasize researching the classification design and the role allocated of users in workflow system. And then it mainly researches and designs the flexible management of user rights and dynamic allocation with the changing needs of business. Finally, it successfully realizes the design patterns of user rights dynamic allocation.

Key words: workflow; information system; user management; dynamic allocation

0 引 言

对信息资源的合理利用和正确使用,对人力资源的合理分配以及相关人员之间协同工作是每一个管理应用系统要综合考虑的。对信息资源分类、保证信息资源的安全使用、对于人力资源的合理分配及其角色任务的定位,并根据不同的角色任务赋予不同的享有控制不同信息资源的权限等管理方面的要求越来越高。同时随着ERP,CRM,SCM,EAM等应用系统在企业里的推广,各种应用系统的使用用户也越来越多,所牵涉的业务逻辑也越来越复杂,对人力资源的合理分配及协同工作的力度要求也越来越高,对各类信息安全访问与利用以及相关人员的操作权限的要求也越来越严格。尤其在基于工作流的管理信息系统中,对各类信息资源的访问与控制更要划分清楚,对用户权限及相关人员的管理也变得越来越复杂。

1 工作流

工作流技术是一种能将业务流程表述为信息数据并对其加以管理和执行的软件技术。工作流系统是由自动化控制系统发展而来的,信息资源的流转是通过工作流引擎作为平台自动进行的。工作流技术是工作流管理系统的核心技术,它监督、控制和协调业务过程和计划,并对工作和信息流程、资源的利用和投入进行预先跟踪。按照工作流管理联盟(Workflow Manage-

收稿日期:2008-04-20
作者简介:蒋 永(1982-),男,四川乐山人,硕士研究生,研究方向为数据库理论与设计;蒋玉明,教授,硕士生导师,研究方向为CRM、ERP、SCM及数据库理论与设计。

ment Coalition, WFMC)的定义,工作流是一类能够完全或者部分自动执行的业务过程,它根据一系列过程规则,能够使文档、信息或任务在不同的执行者之间传递与执行,实现组织成员间的协调工作并达到业务过程流动的最终期望目标[1]。

工作流系统的基本目的是处理案例[2]。处理案例就是对某一特定业务过程的执行过程,此过程只是部分或者全部交由工作流系统来执行而已。工作流一般代表了办公环境的工作过程,包括若干定义完善的活动和它们之间的连接关系。在这一系列的工作流业务过程中,包含了流程的启动和终止、活动的详细描述、活动的规则和次序、参与用户的执行权限和要求、相关应用程序和数据[3]。

2 系统用户权限管理

对于信息资源的利用、对于一个应用型的信息系统来说不同的用户角色应该享有不同的用户权限,对不同的信息资源具有不同的访问和控制权限。在越来越庞大的信息管理系统中,对用户权限的管理以及角色的分类提出了更高的要求。为了使企业级信息管理系统能够满足企业业务越来越复杂的需求,就需要设计出功能齐全且方便用户使用,对用户权限管理灵活自由的管理系统。

2.1 用户权限管理的主要形式分析

应用系统的模式主要分为 B/S 模式和 C/S 模式。不管基于什么模式设计的信息管理系统都离不开用户权限管理。在早期的信息管理应用系统中,对用户权限的管理并不那么随意,其实现的用户权限管理也相当的简单,对于系统特定的业务需求也很少能够通过动态的设置相应的用户访问控制权限。用户权限管理的形式相当有限,主要表现为以下几种形式:

1) 简单的基于 Web 系统的用户权限管理形式。这种形式的应用在系统生成时就只定义了两类用户:系统管理员和普通系统用户。只需要通过简单的 session 设置或者用户类型判断来获得到用户相应的访问控制权限。

2) 普通 CS 模式系统和 BS 模式系统的用户权限管理形式。系统用户一般也分为两类:超级用户和普通用户。但是这里的普通用户又可以分为不同的等级,可以拥有不同的访问权限和处于不同的角色。但是这些用户角色和访问权限是在设计系统的时候就设计好的,不能随着业务需求的变化而随意改动。

3) 企业级 MIS 系统用户权限管理形式。用户权限管理已经趋于一个子系统,在系统中已经不再是一个功能模块的地位。在企业级的信息管理系统中已经引入了组织机构和相关岗位等的划分。这就使得对用户的管理更趋合理化更趋灵活性,而且还能随着业务需求的变化而改动和设置对应的用户角色权限。

4) 工作流系统中用户权限管理形式。工作流系统中的用户可以说是没有分级别的,因为用户权限是根据组织机构和工作任务来设置,即是一种 TBAC 模式[4]。它是以岗位角色来对用户进行分类的。由于它的应用目的是为了处理案例,所以它的用户权限管理也与相应的业务过程有关,分配要相当灵活方便才能真正满足工作流中自动流转提交等业务节点活动的办理。文中将进行这方面的研究与设计实现。

2.2 系统用户分类研究

为满足工作流系统业务过程的顺利自动流转及其相关业务职能的自动执行,工作流中用户与组织机构及相关岗位是紧密联系在一起的。根据工作流系统业务流转过程,不同的工作任务对应了不同的组织角色,而完成这些任务操作的不同角色对应的用户又具有不同的业务权限,这就提出了对用户进行分类来管理的要求。但仅从用户的角度来分类又不能满足工作流业务过程管理的需求,更不能像普通的应用系统那样仅把用户分为不同的级别并为不同的级别赋予不同的操作权限。如图 1 所示,简单展现了早期的用户权限分配管理,这种分配是趋于固定的,很难能够对用户权限进行动态分配管理,但是这种形式的权限分配管理在现在企业级应用系统中同样保留了下来。

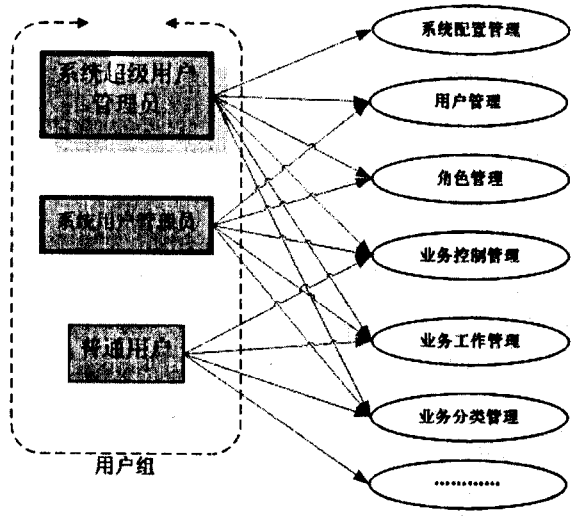

图 1 早期用户权限分配图

* 系统超级用户管理员。

整个系统拥有最高权限的用户一般只有一个,这就是系统超级用户管理员。他要负责对系统进行初始化设置及业务应用的配置设置、添加删除系统用户管理员、业务控制管理和业务工作跟踪等,即拥有全部系

统权限和功能设置权限。

* 系统用户管理员。

系统用户管理员与超级用户管理员比,他所拥有的权限就没有超级用户管理员权限高。他就只能添加删除普通用户,修改自身信息,进行业务控制,工作流跟踪等功能。

* 系统普通用户。

由图 1 可以看出,系统普通用户拥有最低权限,在应用系统中的操作也很有限。只能完成与业务有关的相关任务控制、业务跟踪等。

在工作流系统中为满足复杂多变的业务需求对这种分类形式需要做更加全面的扩展工作。为此可以考虑在工作流系统中使用与组织机构相关的用户分类形式。这样可以根据业务的实际需求和企业或单位的组织机构及其对应的岗位来对用户进行的分类。如图 2 所示,用户的分类不再限于依据用户拥有权限的等级分类,而是针对用户所处不同组织机构、岗位和相应需要完成的任务来划分对应的拥有的系统职责权限。这样对用户进行分类和管理既容易实现用户权限的继承,又便于用户权限的扩展和自由分配。

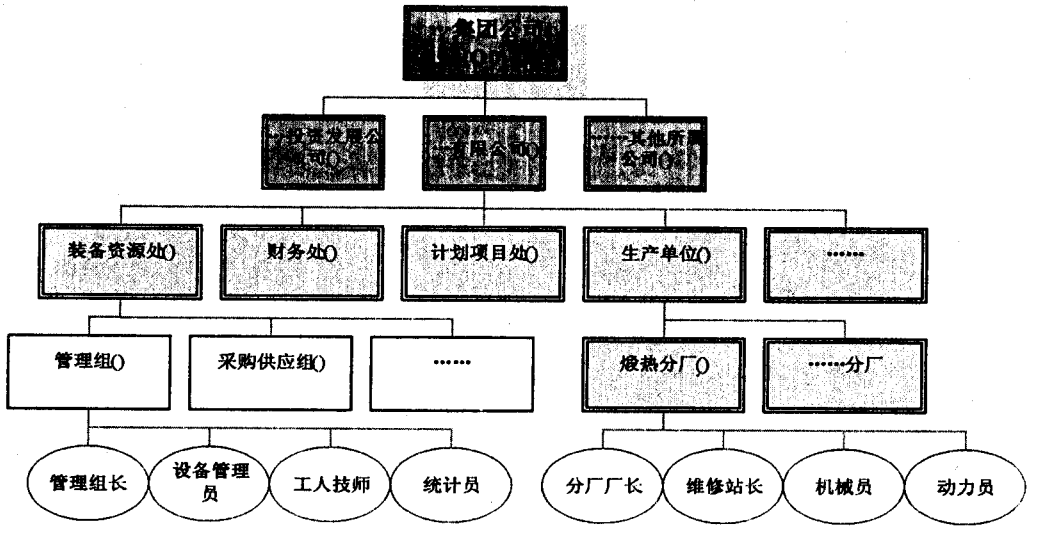

图 2　组织机构树图

3　用户权限分配管理的分析与设计

尤其是在业务过程流转即工作任务转交的时候,要使系统能够清楚将工作任务转向何处,转交给何人并以何种方式传送及下一步要完成何种任务或者该工作流程已经完成到什么程度,达到了什么样的效果。所有这些信息资源都要反映在系统里面,并以友好的界面表示形式展现给相应用户。同时也反映出,在设计系统时、在设计用户权限管理时需要考虑的细节很复杂,必须从工作流程的业务需求出发全面满足各个业务逻辑的控制需求。

在基于工作流的系统设计中必不可少的支持工作流引擎的工具就是与工作流引擎紧密联系的建模工具。工作流业务过程的跳转及业务工作的转交都是靠工作流引擎预先定义好的规则来自动执行的[5]。但是这些规则是可以通过相应的建模工具建立满足特定业务需求的相应模型并发布相应的资源信息来确定的。如图 3 所示,这些就是模型里面定义对应于相应业务流程的职责权限,这些职责权限可以在模型中自由添加与删除以满足特定业务的需求。有了这些职责权限,就可以动态地分配给特定的用户,这里的用户是与特定的组织结构和业务流程相关的。

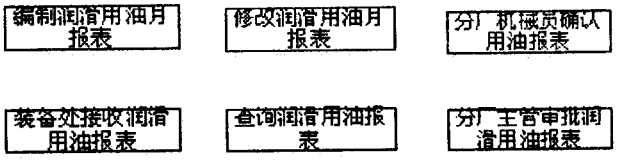

图 3　职责权限视图

再从图 4 所示的工作流系统中的一个业务流程来看,每一个业务节点对应一项业务工作,同时又对应一个特定的组织机构岗位。这样一看就不难发现:这样的设计就把组织机构岗位、相应业务工作和职责权限一一对应起来了。而每一个组织结构和岗位又对应了多个实施业务工作的人员,也就是用户。只需要把每个业务节点对应的职责权限分配给对应岗位的某个人员,那么这个人员就拥有了执行该业务工作的权限,而且只有分配到了权限的人员才能执行,即使相同岗位的人员,若没有分配权限他就不能执行该业务工作。这样一来就通过组织机构及岗位的不同把用户分成了不同的类别,使得不同的用户具有了只有权限差别而没有级别差别的用户权限管理形式,同时还把相同的业务工作通过不同的组织机构及对应的人员而区分开来。这样才真正实现了工作流流程顺利流转。

4　用户权限管理的动态分配

将前面的图 2、图 3、图 4 和下面图 5 综合起来看,很容易发现在权限分配的时候不是将职责权限直接划

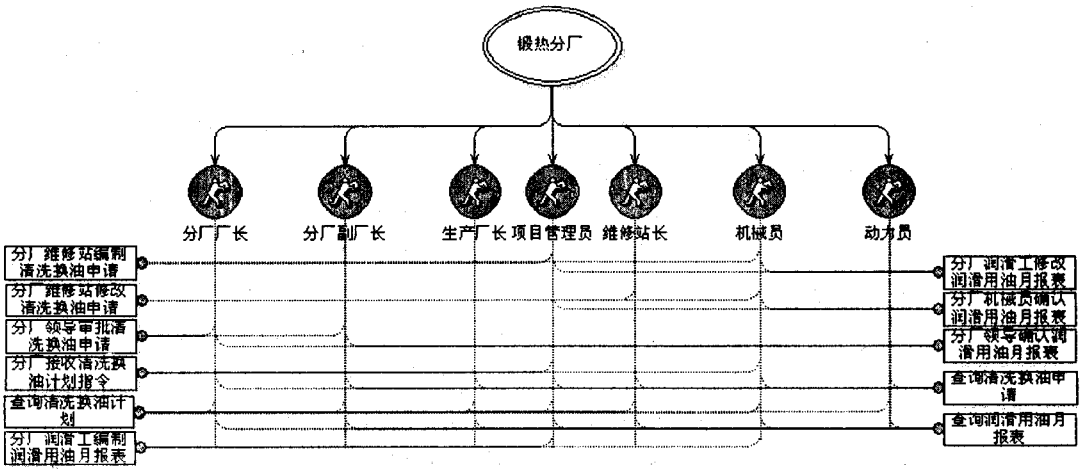

图 5 权限分配视图

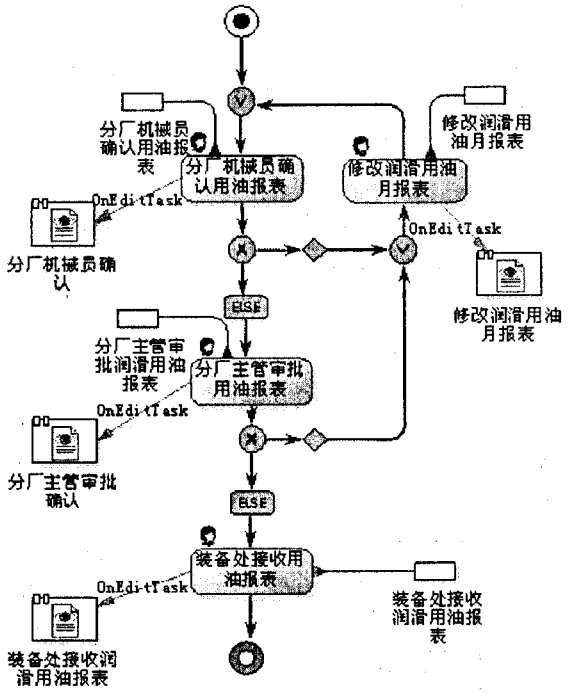

图 4 业务流程视图

分给每个用户，而是为每个职责权限指定了执行该职责任务的组织机构岗位，也就是说有关系统里面所有业务工作任务的执行权限必须同相应的岗位对应。前面介绍到用户是通过组织机构及岗位来进行分类，确切的是通过岗位来将不同的用户进行区分，同时也将业务工作职能进行了良好的区分。也就是为了既要保证不让用户执行未授权的任务又要保证授权用户顺利地执行已经授权的任务[6]。如图 5 所示，在模型设计里面只需要将特定职责权限同特定的岗位通过从属关系联系起来，这样就能实现处于哪些岗位的人员可以执行哪些业务工作，哪些业务工作只能由哪些岗位的人员来执行。还有就是每个岗位都可能有多人，每个岗位同时也可能拥有执行多个业务工作的职责权限。当用设计的模型向工作流引擎发布了相应的模型配置信息以后，进入系统用系统超级用户管理员身份就能为每一个岗位添加相应的人员，同时还能查看每个岗位所要执行的业务工作，并进一步为每个职责权限分配相应岗位下的执行人员。

从前面几张图还可以看出，模型可以随着业务需求的变化而改动，对职责权限设计也可以随着需求而改变，而这种改变对组织机构、岗位和人员不会产生任何影响，但是却可以自由调整人员所拥有的职责权限。就算组织机构、岗位及人员都有较大的变化，也不会对系统造成很大的影响，因为只需要在模型里面修改好了发布到工作流引擎，通过系统超级用户管理员的添加设置相应的职责权限就能实现相应的业务需求。由此可见，这样就很方便地实现了用户权限管理的动态分配。

5 结束语

主要介绍了用户权限管理的形式及用户的分类形式，以及基于工作流系统的用户权限管理思想和设计实现思路。对满足各种业务工作需求的各类用户权限管理进行了研究与设计，达到了用户权限的自由调整和动态分配的要求。基本适应了工作流业务自动跳转与工作任务自动转交后业务职责的动态分配要求。

参考文献：

[1] Hollingsworth D. Workflow Management Coalition - The Workflow Reference Model [S]. The Workflow Management Coalition Specification Document Number TC00 - 1003 Document Status - Issue 1.1, 1995.

[2] Wilvander A, Hee K. Workflow Management - Models Methods and Systems[M]. Massachusetts, London, England: The MIT Press, 2002.

[3] 李永立. 基于 J2EE 的工作流及其在 ERP 系统中的应用

（下转第 171 页）

文档夹或文档组、单个文档或应用对象(如电子邮件或日历项目)。

3.3.3 恢复时间应用集成

在进行恢复时,CDP解决方案能够识别出该应用的先前历史中最优化或最重要的恢复点。这类应用集成是完全自动的,也是可扩展的。

3.3.4 数据库连续保护

CDP解决方案一般都支持常见数据库环境(如Oracle或SQL)的连续保护。支持的意思是该解决方案经过了厂商的全面测试和认证,而且还会向用户提供相关文档内容。

3.3.5 库架构

大多数CDP解决方案是将任何数据的变化存储在单独的地点,形成存储库架构,而且这种存储库是局域网、广域网或存储区域网上明确的专用节点。

3.3.6 库复制

一些CDP解决方案还提供将CDP库复制到另外一个远程库的能力。这样就能够提供更高的灵活性,防止主CDP库可能出现损坏或丢失对恢复能力产生影响。

3.4 CDP发展方向

随着CDP应用范围的扩大和人们认知的深入,CDP技术将会作为在线数据的重要保护手段而独立开辟一条新的通道。其发展方向概括为三点:

第一,CDP的连续和系统保护范畴将继续延伸,从目前基于微软的各类操作系统平台延伸到更多企业级所采用的UNIX平台。

第二,在精细点恢复的技术上,拉杆式日志恢复技术将使精细点的恢复超越最近的快照点。该技术将为一些高端的、以秒级错误恢复为目标的用户带来真正的数据保护方案。

第三,继续完善历史数据的存档机制、在线数据和离线数据的分级保护体系。可利用在线多时间点数据在后台自动提取的serverless备份技术,将近期各时间点数据在不影响应用的情况下存档到VTL虚拟带库中或者存档到物理磁带库中,从而实现数据的离线保存能力和长时间历史数据的保管。

4 结束语

今后,人们的信息系统将面临着越来越多的人为的或自然的不确定因素的威胁,因此,融合现有技术,不断发展新技术,构建更加安全、可靠的数据容灾系统,已经成为当今世界共同关注的课题。

参考文献:

[1] 崔可升,王玉春.建设容灾系统的几点思考[J].计算机系统应用,2003(7):26-29.

[2] 王树鹏,云晓春,余翔湛,等.容灾的理论与关键技术分析[J].计算机工程与应用,2004(28):54-58.

[3] 李兆玉,韦世红,李　鹏.容灾系统的建设方案研究[J].重庆邮电学院学报:自然科学版,2005(4):35-37.

[4] 杜　宁,姚玉坤,黄　伟.浅析基于SAN的容灾实现[J].山东通信技术,2006(2):9-11.

[5] 胡　勇,罗维荣.容灾备份技术架构浅析[J].电子政务,2006(9):15-16.

[6] 妙全兴,武海鹰.一种高性价比的网络容灾与高可用集群的设计[J].微机发展(现更名:计算机技术与发展),2003,13(9):41-42.

[7] Benjamin B, Shao M. Optimal Redundancy Allocation for Information Technology Disaster Recovery in the Network Economy[J]. IEEE Transactions on Dependable and Secure Computing, 2005, 3:262-267.

[8] 颜　军.CDP带来存储新气象[N].计算机世界报,2006-04-03(12).

(上接第164页)

[D].青岛:中国海洋大学,2005.

[4] 云辽飞.基于角色的访问控制技术在统一设备管理中心系统中的应用[D].西安:西安电子科技大学,2007.

[5] 范玉顺.工作流管理技术基础[M].北京:清华大学出版社,2001.

[6] 杨冬梅,张亦军.基于角色的工作流模型研究与应用[J].电脑开发与应用,2006(11):22-24.

(上接第167页)

on Trusted Computing[C]//Proceedings of the Fifth International Conference on Machine Learning and Cybernetics. Dalian:[s.n.],2006:2776-2781.

[4] 魏　乐,叶剑新,黄　健.可信计算的初步研究[J].科技资讯,2007,13:166-167.

[5] 肖　曦,韩　军,汪伦伟.可信计算平台关键机制研究[J].信息工程大学学报,2007,8(2):217-220.

[6] 靳蓓蓓,张仕斌.可信计算平台及其研究现状[J].长春大学学报,2007,17(2):45-49.

[7] Smith S W. Trusted Computing Platforms: Design and Applications[M].冯登国,徐　震,张立武,译.北京:清华大学出版社,2006:148-151.

[8] 邢启江,肖　政,侯紫峰,等.一种基于TPM芯片的计算机安全体系结构[J].计算机工程,2007,33(15):152-154.

[9] Price A. More Secure Computing[EB/OL]. 2006. http:\\www.trustedcomputinggroup.org\TCGBackgrounder_revised_amp_oct_17_06.pdf.