

可扩展 workflow 模型的信访业务协同处理系统

韩坚华, 李 黎, 杨安宸, 赵 锐

HAN Jian-hua, LI Li, YANG An-chen, ZHAO Rui

广东工业大学 计算机学院, 广州 510006

Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China

E-mail: gzhanjianhua@163.com

HAN Jian-hua, LI Li, YANG An-chen, et al. Cooperative petition processing system based on extensible workflow model. Computer Engineering and Applications, 2009, 45(16): 219-221.

Abstract: According to the needs of customized business workflow and information accessed security, an extensible and dynamic cooperative processing workflow model is put forward. By using this as a cord model, users can develop various additional sub models to meet their business processing requirements, such as different kinds of activities, business processing logic, rules and procedures. These sub models then form a workflow model, which can achieve information accessed security control. Using the extensible and dynamic cooperative processing workflow model, the authors develop a petition letters cooperative processing system, which introduces a dynamic workflow management technology, a workflow accessed control and coordinated processing methods based on roles and tasks, and authority monitoring control. After more than three years of use, it is proved that the system has application advantages, compared with similar systems in the market, in system maintenance, cooperative processing and monitoring control.

Key words: petition service processing system; workflow model; cooperative processing; access control

摘 要: 根据可定制业务流程和信息安全访问控制的需求, 提出了一种可扩展动态工作流的协同处理模型。用户可以按照任务处理环节的需求以工作流子模型为核心定制任务中的活动类型和业务处理逻辑, 定制各种附加子模型的业务知识与规则, 并将基于角色和任务的访问控制运用于模型中, 实现安全访问控制的工作流建模。利用该模型, 研发了信访业务协同处理系统, 介绍了系统的动态工作流管理技术、基于角色和任务的工作流访问控制与协调处理方法、以及基于任务授权控制的监控机制。三年多的应用情况证明, 该系统在系统维护、协同处理、以及监控异常方面, 具有应用优势。

关键词: 信访业务系统; 工作流模型; 协同处理; 访问控制

DOI: 10.3778/j.issn.1002-8331.2009.16.064 **文章编号:** 1002-8331(2009)16-0219-03 **文献标识码:** A **中图分类号:** TP311.5

1 引言

随着计算机应用系统的业务处理流程趋于分布式、异构性和自治性的特征, 基于 workflow 技术的分布式协同业务处理系统在业务协同处理过程中的协调性、适应业务需求变动的可扩展性、工作流访问控制的安全性和发现异常、解决异常的监控机制方面, 提出了更高的要求。为提高工作流模型的可扩展性以适应业务变动的需求, 文献[1]采用业务逻辑与管理逻辑相分离的方法来抽象工作流管理系统中各子模型的内容, 提出了一种呈动态工作流管理的、可定制和可扩展业务需求的、具有发现异常和解决异常监控机制的协同处理模型, 但在协同处理的协调性、工作流安全访问控制方面, 尚未给出相关的研究与总结工作。

本文将改进与完善协同业务处理系统的建模分析, 构建一种基于角色和任务的信息安全访问控制、可扩展动态工作流的协同处理模型, 介绍该模型在研发信访业务系统中的应用实

例。系统三年多的应用情况证明, 其研发成果取得了很好的效益。

2 可扩展动态工作流的协同处理模型

2.1 可扩展动态工作流模型的建模方法

从工作流管理联盟 WFMC 提出的工作流管理系统参考模型^[2], 以及对一般业务流程的抽象可知, 业务过程可由一组活动, 以及活动之间的相互关系、过程的起始/终止条件、活动的执行/转移条件、活动的参与者、资源及应用程序等元素组成, 这是构成工作流模型的最小集合(图 1)。

建立可定制和可扩展需求的工作流处理模型, 需要将协同业务相关领域知识与系统框架分离, 构建趋近于与领域无关的、但又能为定制具体的协同业务工作流提供共性支持的系统框架。分析图 1 的元素组成, 业务过程是由一系列活动按照一定的路由逻辑关系(顺序、分支、汇合、循环等)组合而形成的,

基金项目: 广东省科技计划项目(No.2003C101013, No.2007B060401007)。

作者简介: 韩坚华(1955-), 女, 副教授, 主要研究领域为分布式协同软件、智能控制。

收稿日期: 2009-01-22 修回日期: 2009-03-02

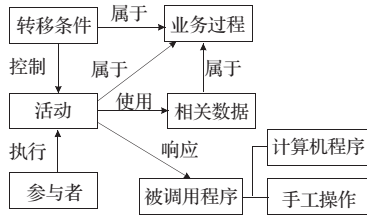


图1 业务流程元素及关系

活动元素是 workflow 处理的核心，而其他元素是活动中的主体、客体或反映活动之间关系的实体，将每个实体对应一个(对象)模型，进行业务逻辑与管理逻辑的分离，在处理具体的业务流程时，再按照业务逻辑定制每一种活动类型、活动中所对应的执行者、触发规则/转移条件、资源、调用的应用程序等属性/方法，并填入到对应的(对象)模型中，就形成了以活动模型为核心，以用户/角色模型、规则模型、资源模型、信息模型等作为附加模型的可扩展动态工作流的建模方法(图2)。

2.2 分布式协同处理的协调模型

在业务过程的基本活动中，没有包括分布式协同处理中需要附加的一些活动，这些活动的协调方式有：任务参与者之间相互合作/交流的对等方式；任务主管部门与参与者之间执行督查/反馈的主从方式；为任务中的参与者提供协同处理信息的辅助方式。这些活动的执行有助于促进任务参与者之间的协同工作，将组成基于任务的协调模型(图2)。

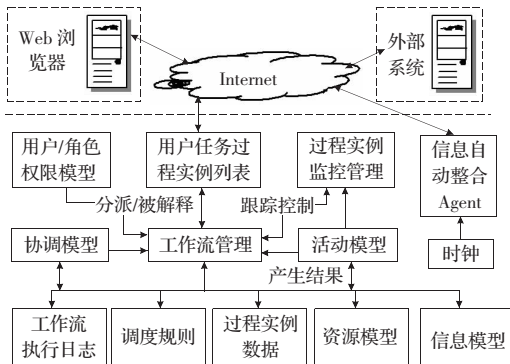


图2 可扩展动态工作流的协同处理模型

2.3 发现异常、解决异常的监控处理机制

跨组织的协同工作难免会遇到一些难以预测的异常发生。因此，处理模型还需要有监控管理机制，通过完整地保存构成任务执行过程的实例数据，为可视化跟踪任务执行中的演变流程、状态以及对工作流程进行纠错提供处理依据。

2.4 基于角色和任务的信息安全访问控制机制

在跨组织的协同业务处理流程中，为保证每个活动只有经过授权的用户才能执行，工作流模型的安全访问控制机制需要结合基于角色和基于任务的两种访问控制模式的优势：对任务处理流程的每一个活动，采用基于角色的访问控制方法，将活动与参与者绑定一起，根据参与者的角色权限，限制其活动中的数据访问区域和操作类型，实现独立于任何过程实例的静态约束(图3^[3])；对涉及过程实例执行历史的模型(如：已完成的工作流活动、协调模型、监控机制等)，采用基于任务的访问控制方法^[4]，其访问控制策略将随着任务的演进而改变授予用户权限的时效性，按过程实例的上下文环境进行信息安全访问控制的动态约束。

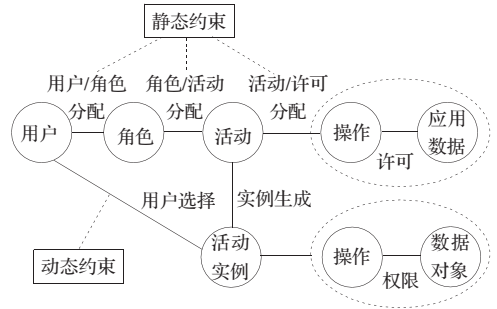


图3 基于角色和任务的工作流访问控制

2.5 信息资源的自动整合机制

在一些分布式协同业务处理中，系统的数据不再是一个信息孤岛，利用(时间、工作流状态、异常、交互等^[5])事件驱动形成代理的行为基础，可以将地理位置分散的、通过 Internet/Intranet 互联的各异构系统之间进行的业务处理作为事件的发生，通过定义事件的合成规则和双方的授权控制，实现信息资源的自动整合处理。

3 基于动态工作流协同处理模型的信访系统

基于以上构建的模型，研发了一个跨部门之间处理市民的来信、来访以及来自网上、呼叫中心的信件，自动与 12319 系统、监察系统整合信息资源，为市民提供查询信件处理结果，并接收其反馈意见的信访系统。

3.1 面向对象的动态工作流建模技术

信访业务中，构成信件处理流程的基本活动有：信件的提交、编辑、审核、转发、受理、转错回退、办结等，组成了工作流的活动模型。信件的处理允许在参与部门之间经过多级转发和协同处理，反映了工作流活动之间相互连接的路由结构。参考图4，可以将组成任务过程的各处理环节(活动)看作对象，也可以将连接活动之间的路径描述成对象。再参考图1，图1中只反映了组成活动的元素，没有反映连接活动的路由关系。针对信件的路流转路由和参与部门难以预先确定，并存在重组处理流程的需求，本系统将活动作为组成工作流的对象，活动中的元素作为活动对象的属性或方法，并把反映路由关系的属性纳入到活动对象中，形成关系数据库中所描述的活动在信件处理过程实例中的数据结构：

信件受理号、信件类型、活动标识、转发时间、处理期限、指派部门、处理意见、承办部门、处理标识/状态、回复指派部门标识、回复信访办标识、回复日期、……。

每个信件的处理流程犹如一张包含树状结构和网状结构的双向动态链表，每个活动对象相当于链表中的一个节点，其属性中的活动指派部门与承办部门构成了活动之间的相互连接(路由)关系(图4)。

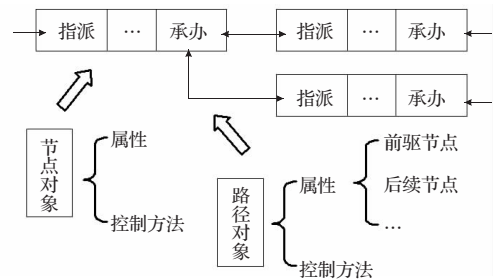


图4 活动之间的相互连接(路由)关系

在信件处理流程中,按活动的承办者设计任务的分解和分配,通过为每个承办者创建一个相互独立的活动实例,绑定活动中用户的职责与权限,使多个参与部门在协同处理同一信件的同时处理环节时,都有各自的活动实例,活动对象可以根据调度规则和自身的属性值(如:承办部门及对应的角色,活动标识,处理状态)来激活自身的活动,在执行中通过访问相关的附加模型来修改自身的属性值,确保处理数据的完整性。

3.2 工作流访问控制与协调处理方法

系统中,一个用户可以授权多个不同的角色,同一个角色可以拥有多个用户,组成信件处理的每个工作流活动可以由多个角色的用户来完成,一个角色也可以分配完成工作流中的不同活动。从用户的职责权限以及信访业务某些敏感数据的安全性出发,系统为管理员提供了定制用户的角色分配、定制角色的权限许可的功能(用户/角色权限模型),在执行活动中,角色对应的权限可以细化为对某个字段数据的操作处理,即对应为二元组(应用数据,操作)。

3.2.1 基于角色和任务的工作流访问控制模型

系统中,基于角色和任务的工作流访问控制管理方法如下:

定义 1 用户集合: $U=\{u_1, u_2, \dots, u_n\}$; 角色集合: $R=\{r_1, r_2, \dots, r_n\}$; 活动集合: $A=\{a_1, a_2, \dots, a_n\}$; 活动中的权限许可集合: $P=\{p_1, p_2, \dots, p_n\}$, 其中: P 中的每一个元素 $p=(d, o)$ 代表对应用数据 d 进行 o 操作。

定义 2 用户 u 所分配的角色集合用 $roles(u)$ 表示; 角色 r 所分配的活动集合用 $activities(r)$ 表示; 活动 a 中的权限许可集合用 $permissions(a)$ 表示。

活动中对应的静态约束规则包括:

(1) 同一用户不能属于冲突的角色, 表示为 $\forall u \in U, |roles(u) \cap CR| \leq 1$;

(2) 同一活动不能分配冲突的角色, 表示为 $\forall a \in A, |activities^{-1}(a) \cap CR| \leq 1$;

(3) 同一活动不能分配冲突的权限许可, 表示为 $\forall p \in P, |permissions(a) \cap CP| \leq 1$;

(4) 用户所授权的角色在活动中的资源配置为 $P=(roles \circ activities \circ permissions)(u)$ 。

任务过程实例中对应的动态约束规则包括:

(1) 完成活动实例的用户属于对应活动的分配角色, 表示为 $\forall a \in A, a_i$ 的用户 $u \in (activities^{-1} \circ roles^{-1})(u)$;

(2) 在形成相互衔接的工作流活动中, 随着任务的演进将改变用户权限的时效性, 若当前正在处理的活动实例为 a_i , 则前面的过程活动实例 a_1, a_2, \dots, a_{i-1} 的权限许可失效, 表示为 $\forall a \in A, a_i \in P \Rightarrow permissions(a_i) \rightarrow \bigcup_{j=1}^{i-1} \neg permissions(a_j)$ 。

3.2.2 基于角色和任务的工作流访问控制与协调处理方法

因为信访业务流程中有些处理环节的参与部门必须推迟到过程实例执行时才能确定, 所以系统在信件流程的处理上, 采用了基于角色和任务的动态工作流访问控制管理方法, 对信件处理流程的每一个活动, 按承办者对应的角色权限, 实现活动中资源配置的静态控制; 对信件的流转操作, 交由当前环节的承办部门, 并结合信件的处理状态和过程实例的上下文环境共同决定下一环节参与部门的用户集, 实现对用户的活动类型和路由选择的动态约束, 使处理结果的下一个活动自动在参与

者之间传递, 形成一系列相互衔接的工作流。

系统中, 构成信件处理任务的协调活动有: 向上级默认反馈处理意见, 催办、督办信件, 参与部门之间交流处理意见, 信访人对办结信件的反馈意见等, 其协调活动实例的生成规则采用基于任务的授权控制方法, 即根据信件处理流程的历史记录、信件的处理状态和处理期限等绑定活动的参与者或用户集(如: 信件受理号、活动标识、承办部门、内容、……)。对贯穿于整个信件处理流程始终的协调活动(如: 对反复咨询或重复投诉的关联信件, 通过建立 1-M 实体关系的关联信件模型, 形成每组关联信件中第一封关联信件与同组其他关联信件的一对多关系, 在关联信件的每一个处理活动中都为参与者提供相互链接的关联信件处理详情的列表显示操作, 以作为重复办案的参考依据), 自动绑定在用户任务列表所对应信件的基本活动中, 从而在处理信件时, 有利于任务参与者之间、主管部门与参与者之间的相互交流和协同工作。

3.3 基于任务授权控制的监控处理机制

系统把信件处理流程中每一个活动的处理记录都保存在数据库中, 构成完整的过程实例数据, 以信件处理的起始结点开始进行深度遍历与广度遍历相结合的搜索方法, 为用户提供基于任务的可视化跟踪信件的整个处理流程、处理状态(信件转办的链条数和参与部门的先后次序, 影响信件处理进度的部门), 并可以根据用户权限的时效性对工作流程进行纠错的功能。对信件处理流程的纠错或重组将保留处理痕迹。

3.4 基于事件驱动的信息资源自动整合平台

设计了专门的 Agent 来实现异构系统之间进行的分布式工作流活动。如: 基于交互事件自动接收来自呼叫中心的信件; 基于时间事件自动访问 12319 系统中由政府部门处理的信件; 基于时间事件自动为全程监控业务流程的监察系统发送信件处理过程的实例数据。

3.5 用户身份认证与应用程序相分离的登录方法

对处理信件的后台系统, 采用了数字化 CA 认证技术与 AD 目录服务绑定的 Windows 基本验证相结合的用户身份认证方法, 其认证过程的处理逻辑与应用程序相分离, 用户身份认证方法的更改不会影响到系统程序。

3.6 信访业务报表系统

可按用户指定的时间间隔生成各种反映信访方式、信件类型、问题分类、问题属地分布等数据的 (Excel 格式) 统计报表。

4 结束语

基于模型研发的信访系统在区政府信息网上不间断运行了三年多时间, 已应用在 70 多个职能部门中, 系统维护方便。实际应用情况证明了研发的系统能够很好地满足信件处理流程中跨部门之间协同处理的需求、以及信息安全访问控制的需求。

本系统与同类系统相比, 在应用上具有以下优势:

(1) 采用双向动态链表结构保存信件流转与处理过程的实例数据, 为参与部门提供基于任务的可视化跟踪信件处理中的演变流程、处理状态以及对工作流活动纠错的功能, 方便发现异常和解决异常。

(2) 在关联信件(反复咨询或重复投诉的信件)的处理流程中, 自动提供对以往关联信件进行处理的历史记录, 为重新办案和科学办案提供参考依据。