第 37 卷 第 24 期
Vol.37 No.24

计 算 机 工 程
Computer Engineering

2011 年 12 月
December 2011

• 软件技术与数据库 •　　文章编号：1000—3428(2011)24—0050—02　　文献标识码：A　　中图分类号：TP309

基于 UCON 的分布式数据库安全模型

翟志刚，王建东

(南京航空航天大学计算机科学与技术学院，南京 210016)

摘　要：针对分布式数据库系统中已发布数据难以控制的问题，结合基于角色访问控制模型(RBAC)和使用控制模型(UCON)的特点，提出一种基于 UCON 的分布式数据库安全模型。将分布式数据库分为服务器端和客户端，服务器端采用 UCON 策略，客户端采用 RBAC 策略。分析结果表明，该模型能有效控制分布式数据库系统中的数据。

关键词：分布式数据库；访问控制；使用控制；易变性；持续性

Secure Model of Distributed Database Based on UCON

ZHAI Zhi-gang, WANG Jian-dong

(College of Computer Science and Technology, Nanjing University of Aeronautics & Astronautics, Nanjing 210016, China)

【Abstract】 In distributed database systems, controlling usage of data after it had been released to a different control domain from its provider becomes an important security issue. Aiming at this problem, this paper analyses the characteristics of Role-based Access Control model(RBAC) and Usage Control model(UCON), and proposes a novel secure model of distributed database based on usage control technology. It gives the composition and definition by using different access control policies on server-side and client-side. Analysis result shows that this model can be used as an effective solution for usage control enforcement in distributed database systems.

【Key words】 distributed database; access control; usage control; mutability; continuity

DOI: 10.3969/j.issn.1000-3428.2011.24.016

1　概述

近年来，分布式数据库系统(Distributed Database System, DDBS)的研究成为计算机技术最活跃的研究领域之一[1]。随着 DDBS 的推广和普及，如何保证 DDBS 的安全也越来越得到重视。DDBS 面临的安全问题具有独特性，尤其是其动态开放性的特点，使得传统的访问控制技术不再适用于分布式数据库系统。文献[2]描述了 DDBS 安全领域中的自主安全策略，但没有给出解决安全问题的方案。文献[3]尝试使用 RBAC 模型来构建分布式系统，使用特权映射的方法使不同的系统保护不同的客体集合，以此保证 DDBS 的安全。

目前应用广泛的角色访问控制模型(Role-based Access Control model, RBAC)表达力较强，优点很多，但是仍旧是基于封闭式环境的，对分布式环境下属性的易变性以及决策的持续性并不提供支持，在描述 DDBS 方面存在较多困难。而使用控制模型(Usage Control model, UCON)概念的提出，为解决这些问题提供了一个很好的思路。UCON 模型是作为下一代访问控制模型被提出的[4]，它具有极强的表达能力，通过不同的配置，可以表达不同的安全策略。在 UCON 模型的完备性和安全性都得到较完整的证明后[5]，学者的研究方向开始转向其应用。文献[6]分析了访问控制和使用控制的区别，探讨了如何在分布式环境下当数据发布以后保证数据的安全。文献[7]给出一个体系结构和 SELinux 的强制访问控制执行机制，并验证了该框架在解决分布式使用控制安全问题上是有效的。文献[8]则实现了一个分布式网格系统中的 UCON 授权子模型。

上述研究成果已经比较丰富，但对于分布式数据库系统来说，用户数量动辄数十万，单独实施 UCON 策略非常困难，因为每次的访问请求都检查决策的 3 个组件，其可行性较差，导致已发布的数据难以控制。为此，本文结合 RBAC 模型和 UCON 模型的优缺点，提出一种新的分布式数据库：RUCON 模型。笔者将 DDBS 分为 2 个部分：服务器部分和终端部分。在终端部分主要实施 RBAC 策略，保证用户身份的获得；在服务器部分主要实施 UCON 策略，保证使用决策的安全。

2　RUCON 模型结构

RUCON 模型结构如图 1 所示。

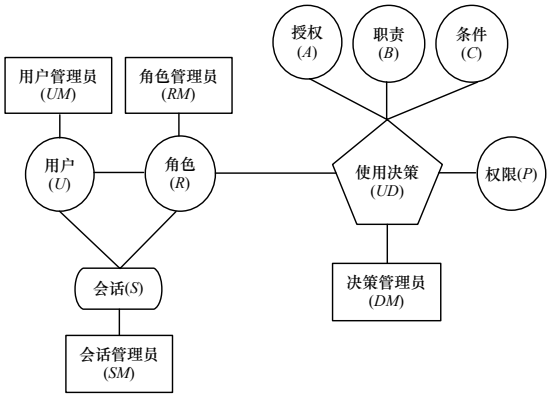

图 1　RUCON 模型结构

在该模型中，用户管理员管理数据库中的用户列表，他同角色管理员结合在每次会话中使用户获得相应的角色，即获得用户的激活角色集；会话管理员帮助维护多个会话，在每个会话当中把用户的激活角色集映射给用户。每次会话开

作者简介：翟志刚(1977－)，男，博士研究生，主研方向：访问控制技术，数据库技术，信息安全；王建东，教授、博士生导师

收稿日期：2011-07-11　**E-mail：**zhaizhigang@nuaa.edu.cn

始时，会话管理员要检查用户的查询历史，依照查询历史判断角色的授予是否执行。当用户要求数据时，UCON 组件开始起作用。决策管理员首先检查是否给予当前角色对于当前客体的权限，如果预先授权存在，则执行；如果预先授权不存在，则不授予；同时检查决策中是否有授予权限的要求。在操作前和操作中都要检查角色职责和对相应数据的权力。当用户的角色满足职责谓词要求的时候，授权才执行。在决策前还要检查当前系统的条件，判断系统条件是否一致，在事务要求提交以后系统条件仍要继续进行检查。如果所有这些决策处理都被检查过了，那么执行用户的请求，否则给予拒绝。

一次完整的用户访问数据过程如下：当一个用户想使用分布式数据库中的数据时，他必须首先通过一个安全会话登录，并提供之前包含他的会话的历史。这个过程由 RUCON 中的会话管理员组件管理。会话管理员允许用户去参与已经存在的会话。一旦会话创建，则初始化访问分布式数据库的进程，分布式数据库访问数据源(存储在分布式数据库中的数据对于用户来说是透明的，用户不必知道数据具体存放在什么位置)，同时决策管理员检查获得相应资源需要的预先授权。如果这个预先授权已经被授予，则进程装载需要的数据，这个过程必须要满足职责谓词，同时还必须检查系统条件是否一致，如果检查结果不一致，则终止进程。

获得预先授权的进程此时开始执行，如果这个进程在执行过程中还有一些属性值需要更新，则决策管理员参照决策管理的判断，检查相应的属性值是否允许修改，也就是说要检查是否满足使用决策的职责属性和条件属性；如果满足条件，进程继续；如果执行以后系统不再具有一致性，则授权被终止或者进程直接停止。

3　RUCON 模型定义

定义 1(名称域 N) $N=\{n|\text{LegalString(string } n)=\text{true}\}$，其中，LegalString(string n)是名称域检验函数。

定义 2 $RUCON=\{U, ATT(U), R, SM, DM, O, ATT(O), P, Q, A, B, C\}$，其中，$U$ 是用户集合，$U=\{u|u\in N\}$；$ATT(U)$是用户属性集合，$ATT(U)=\{(R_u, R_u')|R_u, R_u'\in R\wedge R_u'\subseteq R_u\}$，$R_u$ 是用户的角色属性集合，$R_u\rightarrow 2^R$；R_u'是用户的激活角色属性集合，即用户在一次会话中激活的角色属性集合，$R_u'\rightarrow 2^R$；R 是角色集合，$R=\{r|r\in N,\ r\in ATT(U)\vee r\in ATT(O)\}$；$SM$ 是会话管理员，$SM=\{sm|sm\in N\}$；DM 是决策管理员；O 是客体集合，$O=\{o|o\in N\wedge U\subseteq O\}$；$ATT(O)$是客体属性集合，$ATT(O)=\{R_o|R_o\in R\wedge R_o\rightarrow 2^P\}$；$P$ 是权限集合，$P=\{p|p=(o,\ q),\ o\in O\wedge q\in Q\}$；$Q$ 是权力集合，$Q=\{read, write, add, delete, update, append\}$；$A$ 是授权；B 是职责；C 是条件。

定义 3 授权管理定义

(1)决策前角色分配

$Authorized\_constant\_R(sm,\ r)\Rightarrow SetActive\_R(sm)\in Assigned\_R(sm)$

其中，$SetActive\_R$：$sm\rightarrow 2^{Ru'}$；$Assigned\_R$：$sm\rightarrow 2^{Ru}$

$allowed(u, o, r)\Rightarrow\exists\, role\in R_u,\ \exists\, role'\in R_u', role\geqslant role'$

(2)决策前权限分配

$allowed(u, o, r)\Rightarrow Authorized\_constant\_R(sm, r)\wedge(id(u), r)\in ACL(o)$

其中，id：$U\rightarrow N$；ACL：$O\rightarrow 2^{N\times Q}$

$allowed(u, o, r)\Rightarrow R_u'\cap R_o\neq\varnothing$

(3)决策中授权分配

$onA(ongoing\text{-}authorizations)$：决策中授权谓词

$allowed(u, o, r)\Rightarrow$true

$stopped(u, o, r)\Leftarrow\neg\ onA(u, o, r)$

定义 4 职责管理定义

(1)决策前职责定义

$preB$：预先职责谓词

$allowed(u, o, r)\Rightarrow preB(u, o, r)$

(2)决策中职责定义

onB：执行中职责谓词

$allowed(u, o, r)\Rightarrow onB(u, o, r)$

M：信用度账户集合；$Credit$：$U\rightarrow M$；$Value$：$O\times R\rightarrow M$

$allowed(u, o, r)\Rightarrow credit(u)\geqslant value(o, r)$

$updates(credit(u))$：$credit(u)=credit(u)-value(o, r)$

定义 5 条件管理定义

(1)决策前条件定义

$preC$：预先条件谓词

$allowed(u, o, r)\Rightarrow preC(u, o, r)$

(2)决策中条件定义

onC：决策中条件谓词

$allowed(u, o, r)\Rightarrow$true

$stopped(u, o, r)\Leftarrow\neg\ onC(u, o, r)$

4　RUCON 模型的表达能力

本文通过实现 DAC 策略、MAC 策略和 RBAC 策略，来验证 RUCON 模型的表达能力。

(1)DAC 策略的实现

id: $U\rightarrow N$，一对一的映射

ACL: $O\rightarrow 2^{N\times R}$

$ATT(U)=\{id\}$

$ATT(O)=\{ACL\}$

$Allowed(u, o, r)=>(id(u), r)\in ACL(o)$

(2)MAC 策略的实现

L：满足支配关系“$\geqslant$”的安全级

$Clearance$: $U\rightarrow L$

$Classification$: $O\rightarrow L$

$ATT(U)=\{clearance\}$

$ATT(O)=\{classification\}$

$allowed(u, o, read)=>clearance(u)\geqslant classification(o)$

$allowed(u, o, write)=>clearance(u)\leqslant classification(o)$

(3)RBAC 策略的实现

用户角色集 R_u、激活角色集 R_u'、权限角色集 R_o 定义如前，则有如下规则：

$allowed(u, o, r)=>\exists role\in R_u', \exists role'\in R_o, role\geqslant role'$

$allowed(u, o, r)=>R_u\cap R_o\neq\varnothing$

对于 RBAC 中的职责分离原则、最小特权原则、抽象原则等，RUCON 中定义与 RBAC96 模型相同，本文不再赘述。

5　结束语

本文讨论了 UCON 模型在建立分布式数据库系统安全模型中的应用，提出一种基于 UCON 的分布式数据库安全模型。该模型可支持丰富的策略决策、支持属性的易变性和决策的持续性。分布式系统的动态性使其访问控制的问题较为复杂，下一步工作将研究授权的自动执行与撤销以及职责问题。

(下转第 54 页)