一种面向云计算的任务—角色访问控制模型*

黄 毅[1,2]，李肯立[1]
（1. 湖南大学，长沙 410004；2. 湖南科技职业学院，长沙 410118）

摘 要：针对云计算模式下用户访问安全的问题，简单分析了基于角色和任务的访问控制模型的内容，提出了一种基于云计算的任务—角色模型。该模型通过对角色和权限进行分类，有效地解决了访问控制模型中的管理权限问题，使得云计算服务商的权限分配得到了进一步改进。分析结果表明，该访问控制模型可以进一步提高客体频繁访问的效率。

关键词：云计算；访问控制；角色；任务
中图分类号：TP393 **文献标志码**：A **文章编号**：1001-3695(2013)12-3735-03
doi:10.3969/j.issn.1001-3695.2013.12.056

Model of cloud computing oriented T-RBAC

HUANG Yi[1,2], LI Ken-li[1]
(1. *Hunan University*, *Changsha* 410004, *China*; 2. *Hunan Vocational College of Science & Technology*, *Changsha* 410118, *China*)

Abstract: Based on problems of user access security in the cloud computing models, this paper made simple analysis of the content of task-role-based access control model and offered a model of cloud computing oriented T-RBAC, in which permissions and roles were classified, users were granted permissions by assigning them roles that have those permissions. This greatly simplified management of permissions in the access control models and further improved permission allocation of cloud computing service providers. The analysis results show that this access control model can further improve the efficiency of user frequent access.

Key words: cloud computing; access control; role; task

0 引言

云计算在互联网中的应用越来越广泛，它提供了大型数据存储和计算服务，为网络资源共享提供了便利，突破了传统的 PC 机网络共享的边际。在云计算为人们提供方便的同时，网络安全也是不可忽视的问题，如密码技术、用户身份认证等。在这些技术中，访问控制技术是信息安全领域中一类非常重要的技术，它实现了用户数据机密性和隐私保护的重要手段[1~4]。文献[5]描述了在进行云计算访问控制时采用的算法，进一步提高了访问控制效率。文献[6,7]提出了一种改进型的任务—角色模型，该模型针对访问控制模型进行了改变，效率得到了一定的提高，但总体表现不稳定。文献[8~10]从组、属性和角色的角度出发进行阐述，有效降低了角色管理的复杂度。本文首先介绍了访问控制模型的内容，然后根据云计算的特点，对访问控制模型进行了改进，构建了一个改进型的任务—角色访问控制模型。

1 访问控制研究

在访问控制模型中，其核心的是授权策略的制定，主要是用于确定主体对客体访问能力的规则的制定，控制模型中采用主体、客体、访问这三个部分组成，它决定了授权策略制定水平的高低以及灵活性。在云计算环境下，用户需要访问的资源越来越多，这就要求云计算服务商提供的资源种类和安全性也越来越高，访问控制模型在云计算环境中显得尤为重要[11]。

1.1 基于角色的访问控制

基于角色的访问控制(RBAC)是一种访问控制技术，它在用户和访问权限之间引入角色的概念，这样保证将用户和权限之间进行分离，从而可以进一步保证用户和访问权限的安全，提高用户访问的灵活性。RBAC 中的用户、角色、访问权限之间关系如图 1 所示，RBAC 模型的结构如图 2 所示。RBAC 模型对主体特征的描述非常详细，缺少对客体特征的描述，不适合在分布式的系统中应用。

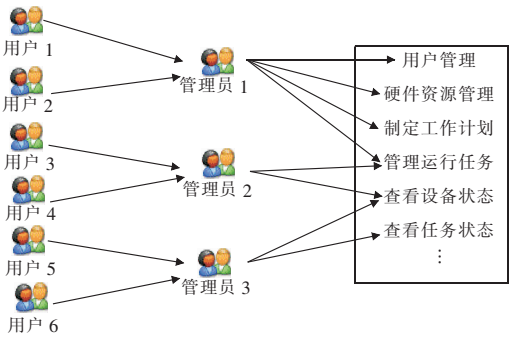

图 1 用户、角色、访问权限示例图

1.2 基于任务的访问控制

基于任务的访问控制模型(TBAC)是一种新的安全模型，它采用工作流的特性，从任务的角度出发，将任务分为建立任

收稿日期：2013-02-23；**修回日期**：2013-04-09 **基金项目**：国家自然科学基金资助项目(61133005)

作者简介：黄毅(1976-)，男，讲师，硕士，主要研究方向为信息安全、云计算(hnhuangyi2013@163.com)；李肯立(1971-)，男，教授，博导，主要研究方向为并行分布式处理、计算机仿真、地震数据处理与可视化、生物计算技术.

务、执行任务、完成任务三个部分。TBAC 结构如图 3 所示。在 TBAC 结构中，主体和客体之间引入任务层来实现权限的分解，可以对权限分配表进行简化，使得主体在执行任务中获得客体的访问权限，任务结束之后权限就被消耗完成了，防止了主体对客户的权限的永久拥有。但是 TBAC 结构中，由于没有对客体任务明确地说明，不支持被动访问控制。

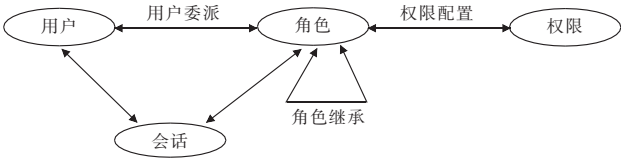

图 2 RBAC 基本结构

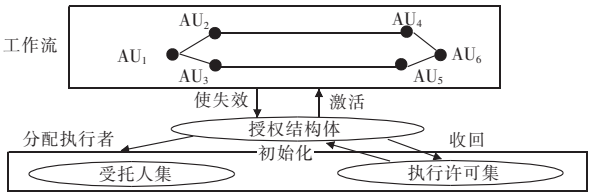

图 3 TBAC 模型

1.3 任务—角色的访问控制模型

该模型(T-RBAC)结合 RBAC 和 TBAC 两者的优点，通过将角色、权限、任务进行结合，从而实现对访问权限的管理。这样做的目的是为了在执行任务时，用户才能拥有与之相关的权限，可以进一步保证授权与任务的同步[12]。但该模型具有以下缺点[13]：

a)任务分配。在工作流处理的过程中，系统直接处理的对象不一定都是可执行的任务，也就是说，在系统中，任务不全是数据对象，有些任务仅仅是用来管理与监督它们的任务，这样做的目的是便于计算机系统能够更好地进行管理，因此在模型中需要对任务进行进一步的分类。

b)角色分配。在模型中，角色之间分为高级角色和一般角色，在实际应用的过程中，很多的任务都是通过相应的角色来完成的，在高级角色和一般角色之间存在某种传递关系，但是由于这种关系的存在，使得传递的范围无法进行控制，这就导致任务之间的分配关系存在一定的模糊性。在该模型中，需要对角色进行一定的控制。

c)时间有效性。在访问控制中，每一个任务的执行时间具有一定的限制性，如果超出设定时间，就必须自动地挂起该任务或者删除任务，否则会进一步拖延下一个任务的运行时间。

d)资源有效性。系统中最重要的是资源的合理使用，每一个任务使用资源的数目有限，在规定的时间下，每一个任务如果没有合理的使用资源，很容易操作死锁。

2 基于任务—角色的云计算访问控制

在云计算中，云计算服务提供商管理着数据的计算和存储，它扮演着最终数据掌握者的角色。存储在云端的数据主体经常频繁访问数据库，这样给系统的权限管理带来了一定的难度。在 TRBAC 模型中，通过角色的概念来进行管理，从而使得管理层次更加清楚，云计算中的主体对于客体的权限有着明显的角色属性区别。在云计算访问控制中，云服务器都是最重要的角色，它具有最高的访问权限，对于客体拥有最高的访问控制权限。本文首先在云计算中的服务端中进行角色分类，根据访问客体的要求分配不同的访问角色，在任务分配的权限阶段，对权限进行不同的分类，从而可以进一步解决主体对于客体访问过程产生的效率低和频繁访问的问题。

2.1 基于任务—角色云计算访问控制模型

任务—角色访问控制模型(T-RBAC)是在角色模型的基础上结合任务模型的特点，将权限通过任务分配给角色，从而实现了动态管理，在 T-RBAC 模型中，任务节点的实例分配给角色，从而获得权限，用户获得对客体的访问权限通过角色来获得，结合云计算模式下的用户访问特点，基于云计算模式下的任务—角色访问控制模型描述如下：

定义 1 用户。网络中的企业客户或者个人客户，他们是由云计算服务商提供的客户，可以独立访问系统中的数据或者资源。

定义 2 角色。在云计算中，访问任务的一组集合。

定义 3 角色分类。针对任务性质的不同进行分类，可以提高客体访问主体的效率，为权限分类提供一定的参考。

定义 4 权限。在云计算中访问资源的许可范围。

定义 5 权限分类。在云计算中，根据不同的用户访问要求，权限分类需要对用户的访问权限进行一定的分类，根据 Permission→Users 建立有效的权限分类。

定义 6 会话。用户在激活云计算服务商的授权角色之后，通过分配的角色建立映射，取得会话过程。

定义 7 会话用户。Sessions→Users，在云计算中，用户需要访问云计算服务商提供服务时，创建的会话 S。

定义 8 会话的角色集合 Roles。Sessions→2^R 表示会话 si 到角色集合 Roles 的映射，SA 表示当前的角色集合被激活的角色。

定义 9 任务。在云计算中，根据云计算服务商中提供的不同服务，对任务进行不同的分类。有些任务是可以根据功能进行分类，也可以根据服务类型进行分类。

定义 10 角色继承。在云计算中，很多任务的执行者可能会具有相同的权限，比如在同一个用户中的不同客户访问同一个数据库，为了避免相同权限的重复设置，角色可以继承其他的角色，从而可以具有属性和权限，避免了角色的重复设置。

定义 11 时间控制。设置任务的执行时间，用于保证云计算中任务的合理运行时间，从一定程度上约束角色和任务的活跃性。

定义 12 资源控制。在云计算中，容易出现不同的用户争夺同一使用资源的情况，对任务和角色设置资源控制来保证云服务商的正常运行，以避免死锁情况的发生。

基于云计算改进的任务—角色访问控制模型的基本结构如图 4 所示。

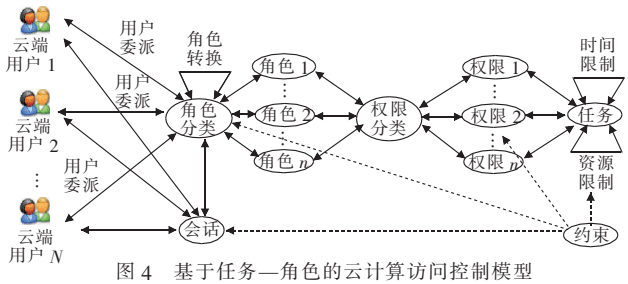

图 4 基于任务—角色的云计算访问控制模型

2.2　任务—角色的云计算访问控制需求

在云端存储数据需要具有更高的访问控制,控制需求主要是由客户和数据保密两个方面来组成。在云计算中,数据的访问主要是由云服务提供商和访问者两个部分组成,其中,访问者主要分为外部访问者和内部访问者。不同的数据访问对应的权限是不同的,云计算服务商进行数据的管理和维护,通常访问的权限仅限于对数据库的操作。外部访问者的访问权限对数据的操作多集中在数据的读取上,内部访问者的访问权限主要是企业内部的访问级别的设定。从数据保密的角度出发,由于云计算中服务器的存在,数据的访问控制根据不同的安全等级来设置不同的访问权限,客体可以通过服务器来设置公开的信息,而更加机密的信息可以由客体创建来进行。

2.3　任务—角色的云计算访问控制管理

云计算中的访问控制主要分为以下几个方面来进行管理:

a)客体的用户管理。在云计算环境下,外部访问者是对数据库进行读操作和查询操作,内部访问者的角色是员工的层次管理,在 T-RBAC 模型中,通过任务来进行权限分配,通过为客体访问者创建任务实例,从而将用户管理和权限分配工作的效率提高。由于客体所有者向云计算提供商定时地激活数据,可以从一定程度上防止供应商随意访问数据的权限,从而进一步保护了用户的数据。

b)数据管理。数据的安全性管理对于云端服务器和用户来说都是非常重要的,数据安全过程都是采用密钥系统进行加密存储。加密的目的是通过对客体安全等级的设置来进行数据的分级管理,将数据按照重要性的不同进行分级,进一步细化了安全等级。

c)任务和角色管理。任务和角色的分类细化了访问控制的安全等级。系统根据主体的访问请求来进行任务和角色的分类。依托对任务的访问控制管理,将角色分为私有、监督、工作流、活动四类。系统中根据主体的访问请求启动相应的角色,通过对角色的分类,从而实现细粒度的管理。这样做的好处是保证任务的时间属性来消除客体获得权限的无限制的等待,以免导致数据安全出现隐患。

2.4　任务—角色的云计算访问控制的逻辑描述

在本文的访问控制模型中,云计算服务提供商没有最高权限,客体访问请求由客体所有者和云计算服务商来进行共同的处理访问请求,通过角色分类和权限分类来进行任务的管理。假设某一个云计算服务商(cloud-services)有主体 S 请求对客体 ob 执行 op 操作,将主体角色的访问请求分解为不同的任务进行操作,然后对这些任务进行分配资源。假设 S_N 表示不同的客体,Time_N 表示任务 i 使用时间额度,Source_N 表示任务 i 使用的资源数。其中 N 为$\{1,2,\cdots,i\}$。

a)用户 x_i 向服务器访问的过程:

(a)用户 x_i 向服务器发送访问请求;

(b)服务器检查客体的权限表,验证客户 x_i 的访问权限,如果合法就返回授权证书,反之,拒绝访问;

(c)服务器向 x_i 发送证书;

(d)x_i 向服务器发起访问请求;

(e)x_i 向 T-RBAC 组建申请任务,模型根据权限表中分配的不同进行角色分类,T-RBAC 根据角色的不同,进行授权的分类。

b)用户访问服务器逻辑表达:

S_N,Time_N,Source_N
flag = false;
for $S_i \in$ As
if(as, T) $\in$ Perssion[n] and $r \in$ roles[n]
　for s_i at Perssion[i] and r_i at roles[i]
　if(at = false)
　　flag = false
　　break;
　else
　　flag = true
　end if
　if flag = true
　 if $S_{\text{timei}} \leqslant \text{Time}_i$ and $S_{\text{sourcei}} \leqslant \text{Source}_i$
　　云计算客体访问主体服务器资源
　end if
end if

3　结束语

云计算环境下访问控制安全已经成为了当前的研究热点,本文所描述的访问控制模型从控制的角度出发,从而进一步地保护系统的安全以及云计算中的客户信息的安全,T-RBAC 模型能够利用云端服务器,通过角色和权限的分类,使得客体所有者既能满足分布式访问控制的要求,同时又能对角色管理进行分层,采用 T-RBAC 模型构建了面向云计算模型,解决了访问控制中的用户管理、数据管理和任务及角色管理问题。但该模型目前存在的一些问题需要进一步的讨论,有待于进一步的深入研究。

参考文献:

[1] CHOW R. Controlling data in the cloud: outsourcing computation without outsourcing control[C]//Proc of ACM Workshop on Cloud Computing Security. New York: ACM Press, 2009: 85-90.

[2] 李凤华,苏锟,史国振,等. 访问控制模型研究进展及发展趋势[J]. 电子学报,2012,4(4):805-813.

[3] 韩道军,高洁,翟浩良,等. 访问控制模型研究进展[J]. 计算机科学,2010,37(11):29-33.

[4] 陈全,邓倩妮. 云计算及其相关技术[J]. 计算机应用,2009,29(9):2562-2566.

[5] 孙国梓,董宇,李云. 基于 CP-ABE 算法的云存储数据访问控制[J]. 通信学报,2011,32(7):145-152.

[6] 陈泉冰,王会进. 一种改进的基于任务—角色的访问控制模型[J]. 暨南大学学报,2010,31(1):29-34.

[7] 韩若飞,汪厚祥. 基于任务—角色的访问控制模型的研究[J]. 计算机工程与设计,2007,28(6):800-807.

[8] 张斌,张宇. 基于属性和角色的访问控制模型[J]. 计算机工程与设计,2012,33(10):3807-3811.

[9] 费洪晓,陈炯,邓小鸿,等. 面向资源所有者访问控制模型的设计与实现[J]. 计算机应用与软件,2012,29(6):26-29.

[10] 于春生,聂晶. 基于组和角色的工作流权限访问控制模型[J]. 计算机应用,2011,31(3):778-780.

[11] 马强,艾中良. 面向云计算环境访问控制模型[J]. 计算机工程与设计,2012,33(12):4487-4492.

[12] 雷建云,洪帆,蒋天发. 基于角色的安全工作流动态访问控制模型[J]. 东北大学学报:自然科学版,2008,29(3):387-390.

[13] 孙军红,王新红. 一种分布式环境下基于角色的控制模型[J]. 计算机工程与应用,2011,47(23):84-87.