

CT-RBAC: 一种云计算环境下的访问控制模型

常玲霞, 王凤英, 赵连军, 贾永新, 程 震

(山东理工大学 计算机学院, 山东 淄博 255049)

摘 要: 云计算的开放性、共享性等特点, 使云计算环境下的访问控制比传统环境下的访问控制更加复杂. 为了保证访问过程中云用户以及云服务器上数据的安全性和可靠性, 提出了一种云计算环境下的访问控制模型 (CT-RBAC). 划分了云服务器上数据和云用户的安全级别, 引入了任务情景集, 从 5 个角度来实现访问控制策略, 最后给出了云用户访问云端数据的实现流程. 分析结果表明 CT-RBAC 具有明显的优点. 该方案提高了客体拥有者对云服务器的监控能力, 保证了云环境下数据的安全性和可靠性, 并且具有较好的灵活性.

关键词: 云计算; 访问控制; CT-RBAC; 安全级别; 任务情景集; 监控能力

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2014)06-0152-06

CT-RBAC: An Access Control Model in Cloud Computing

CHANG Ling-xia, WANG Feng-ying, ZHAO Lian-jun, JIA Yong-xin, CHENG Zhen

(College of Computer Science and Technology, Shandong University of Technology, Zi'bo 255049, China)

Abstract: The characteristics of cloud computing such as openness, sharing, make the access control more complicated in cloud computing than it in traditional environment. In order to guarantee the security and reliability of cloud users and the data on the cloud server in the accessing process, this paper put forward an access control model named CT-RBAC in cloud computing. This scheme divided the security level of the data on the cloud server and cloud users, and introduced the set of task situation, what's more, it achieved the access control policy from five aspects. Finally, it gave out the implementation process of cloud users access the data in the cloud. The analysis results indicate that CT-RBAC has its obvious advantages. This scheme improves the monitoring ability of the object owner to the cloud server, guarantees the security and reliability of data, and ensures the well flexibility.

Key words: cloud computing; access control; CT-RBAC; security level; task situation; monitoring ability

1 引言

云计算是在分布式处理、并行计算和网格计算的基础上发展起来的一种新兴计算模式^[1]. 它把大量存储资源、计算资源和软件资源连接在一起, 形成了一个巨大的共享虚拟资源池为远程计算机用户提供 IT 服务. 云计算的快速发展带来了服务方式的改变, 但同时也带来了许多新的安全挑战. 目前, 很多云服务提供商都不能有效保证其服务的安全性. 安全问题的频繁发生不仅阻碍了云计算技术的快速发展, 也给云用户带来了许多顾虑, 而访问控制技术

是解决安全问题的一个重要途径.

2 相关问题及研究现状

2.1 云计算中的安全问题

传统环境下的数据可以受到局域网的保护, 而云计算环境下的数据存储云端, 由于云计算系统的规模巨大、虚拟化、开放性等特点, 使其面临的安全问题更为严峻^[2], 数据的安全性更难保证^[3]. 如何保证用户的数据不被非法访问和泄露是云计算环境下亟待解决的两个重要问题. 此外, 还存在云服务器并不对客体拥有者的数据丢失等安全问题负责; 客

收稿日期: 2013-07-26; 修回日期: 2013-09-17

基金项目: 山东省科技发展计划(2013GGX10116); 山东省自然科学基金(ZR2011FL013); 山东省高校科技计划(J13LN274)

体拥有者对云服务器的依赖程度过大,对所属客体的管理控制能力减弱等问题.虽然加密技术能够提高数据存储和传输过程中的安全性和可靠性,但使管理过程变得复杂.建立私有云也能够提高数据的安全性,但费用较高,也不能有效发挥云计算的灵活性和弹性等特性.因此迫切需求一种适合于云计算环境下的访问控制方案来解决这些问题.

2.2 访问控制

访问控制是保护用户数据安全,防止信息泄露的重要手段^[4].它可以保障合法用户访问和使用授权内的网络资源,防止非法用户的侵入或者合法用户的不慎操作造成破坏^[5].目前已有的典型访问控制模型主要有自主访问控制模型(DAC)、强制访问控制模型(MAC)、基于角色的访问控制模型(RBAC)^[6]以及基于任务的访问控制模型(TBAC).其中RBAC和TBAC模型是现在常用的两种模型.RBAC引入了角色的概念,分离了主客体,简化了管理,并且易于扩展,但对角色授权管理时没有考虑执行的上下文环境,只适用于角色结构严谨的企业内部访问控制^[7].TBAC是一种动态授权的主动安全模型,仅在任务执行时主体对客体才具有权限,一旦任务结束就释放权限.但TBAC模型没有分离角色和任务,不支持角色的层次等级,也不支持被动访问控制,授权管理复杂,很难单独模型化,适用于事务管理系统、工作流、分布式处理以及多点访问控制的信息处理^[8].

目前,针对云计算环境下的访问控制,国内外学者在已有的访问控制模型的基础上进行了研究,提出了一些访问控制模型.LI等^[9]对SaaS平台下的RBAC模型进行了改进,解决了云计算环境下部分访问控制问题,但没有考虑访问控制过程中的上下文环境.朱养鹏等^[10]提出的SaaS平台权限管理模型能够保证用户的数据安全,但其定义的租户,租户用户,租户角色等概念,复杂化了角色之间的层次关系.赵明斌等^[11]提出的基于RBAC的云计算访问控制模型,提高了云计算环境下数据的安全性和灵活性,但忽略了云服务提供商的可信性,对用户数据的安全构成了威胁.林果园等^[12]提出的基于行为的云计算访问控制安全模型保证了云服务器中数据的安全性和保密性,但模型中“上读、下写”的特性降低了

它的可用性.Tang等^[13]把云环境下的用户划分为普通用户和资源所有者,由资源所有者授予用户访问相应资源的权限,增加了资源所有者的管理负担.洪澄等^[14-15]提出的云存储密文访问控制,保证了数据的机密性,但增加了管理成本和负担.

本文在TBAC和RBAC模型的基础上,提出了一种云计算环境下的访问控制(CT-RBAC)模型.该模型主要保持了RBAC分离了主客体、便于管理、易于扩展的特点以及TBAC动态授权的优点,也结合了MAC根据安全属性强制性决定一个主体是否可以访问某个客体的特点,能够在一定程度上避免机密信息的意外泄漏.此外,该模型考虑了对角色授权管理时的上下文环境,既支持主动访问又支持被动访问.

3 CT-RBAC 模型

3.1 CT-RBAC 模型的架构

CT-RBAC模型主要是在RBAC和TBAC的基础上进行了改进和扩展,模型主要由云用户,角色,任务,权限,云客体等元素组成.CT-RBAC模型的架构如图1所示.

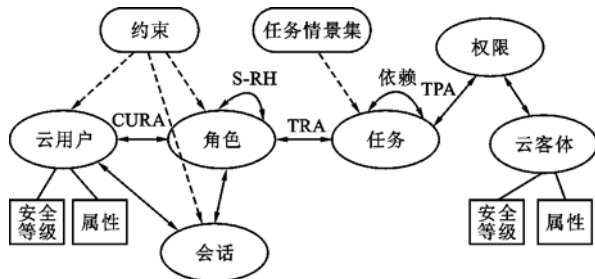


图1 CT-RBAC模型

3.2 CT-RBAC 模型中的组成元素及元素间的关系

模型的形式化定义如下:

云用户集: $CU = \{cu_i \mid i = 1, 2, \dots, m\}$, 云用户是访问云服务器上资源的用户.

云客体集: $CO = \{co_i \mid i = 1, 2, \dots, n\}$, 云客体是云服务器上的资源,如图片、音乐、视频等.

安全级别: $SL = \{H, M, L, \dots\}$, 云用户以云客体的安全级别,本文中取高(H)、中(M)、低(L)三个级别.

属性集: $A = \{a_i \mid i = 1, 2, \dots, n\}$, 云用户或者云客体自身所拥有的一些特性.如云用户的姓名、部

门、职位等信息,云客体的名称,大小,所属的客体拥有者等信息.

角色集: $R = \{r_i \mid i = 1, 2, \dots, n\}$, 角色是云用户可以执行的操作的集合.

任务集: $T = \{t_j \mid j = 1, 2, \dots, n\}$, 任务是云用户需要处理的操作, 是能够区分的动作, 一个任务可以分割成若干个子任务.

权限集: $P = \{p_i \mid i = 1, 2, \dots, p\}$, 权限是云用户对云客体进行操作的能力, 包括读、写、执行、虚拟资源调度等.

会话集: $S = \{s_i \mid i = 1, 2, \dots, s\}$, 会话是云用户与所激活角色之间的一种映射.

约束集: $C = \{c_i \mid i = 1, 2, \dots, q\}$, 访问控制过程中对相应指派规则所作的限制条件.

任务情景集: $TS = \{ts_i \mid i = 1, 2, \dots, u\}$, 任务情景是任务执行时的安全信息, 包括时间状态、环境状态和监控信息.

依赖: 任务之间具有的一些相互依赖关系.

S-RH: 角色之间的一些继承关系.

CURA: $CURA \subseteq R \times CU$, 角色到云用户的分配关系.

TPA: $TPA \subseteq P \times T$, 权限到任务的分配关系.

TRA: $TRA \subseteq R \times T$, 任务到角色的分配关系.

4 CT-RBAC 访问控制策略

4.1 管理策略

云计算环境下的访问控制不仅需要保障数据的安全可靠性, 也需要保持云计算的开放性. 本方案的访问控制策略参考了文献[8], 在文献[8]的基础上进行了充分的扩展和改进. 这里主要从以下 5 个角度来实现云计算环境下的访问控制管理策略. 具体如下:

(1) 用户管理

由于本地用户数量有限, 并且用户属性一般不会发生变化. 与本地用户不同, 云计算环境下的云用户数量跟属性是都动态变化的, 如何实现对云用户的有效管理是访问控制管理中的一个重要问题.

为了实现对角色的分类授权管理, 把云计算环境下的用户划分为客体拥有者、云服务器、云用户三类. 客体拥有者根据客体的重要程度来划分它的安

全级别(本文中取高、中、低三个级别)再将所属的客体上传到云服务器上, 并且授予云服务器对其的管理权限, 因此相应云客体的安全级别与客体的安全级别是一样的. 云服务器负责管理和维护云客体.

(2) 任务管理

CT-RBAC 中, 任务把角色和权限关联起来, 因此对任务的管理是至关重要的. 任务是随着云用户的变化而变化的, 需要保证同一云用户在不同条件下的任务执行状况是不同的.

①任务分类: 为了简化对任务的管理, 从两个角度对任务进行分类. 从任务的权限是否具有可继承性的角度把任务分为可继承权限的任务和不可继承权限的任务. 监管类和活动批准类任务是可继承权限的任务, 私有类任务和工作流类任务是不可继承权限的任务. 另外, 从应用的角度把任务分为工作流类(W 类)任务和非工作流类任务(NW 类)任务. 其中, W 类任务是主动访问控制, NW 类任务是被动访问控制.

②任务情景集: 为了确保某任务只能在特定的系统环境中并且由特定角色的云用户执行, 这里引入了任务情景集, 它包含了任务执行时的环境状态(IP 地址、软件平台、物理位置等), 时间状态(任务开始执行的时间、持续的时间、结束的时间等), 监控信息(云用户属性的更改、访问过程行为的可疑、黑名单用户等). 任务情景的变化对任务所能享有的权限具有直接影响, 任务的状态也会动态的变化. 例如, 云计算提供的某服务只允许部分云用户在特定的时间段和网络内访问某些数据, 而在其他情况下的访问请求就被拒绝.

③任务优先级: 为了避免任务调用过程中相互之间发生冲突, 给任务划分不同的优先级别 P. 如果发生冲突, 由优先级高的任务优先执行. 另外, 为了防止优先级高的任务一直占用资源, 使优先级低的任务始终得不到执行, 设置每个任务的执行时限为 t , 超过时间段 t 之后由优先级队列中的下一任务执行.

(3) 约束管理

同一时间段内, 为了防止 CT-RBAC 模型中云用户与云用户之间、角色与角色之间以及会话与会话之间发生冲突, 需要分别对云用户、角色以及会话

设置约束条件.

①对云用户的约束:某一时间段内,云用户所拥有的角色数目是有限的.

②对角色的约束:要限制同一角色只能分配给有限个云用户.同一时间段内,相互冲突的角色,是不能同时分配给同一云用户的,相互冲突的云用户也不能属于相互冲突的角色.特定的角色可以被激活,但只能在规定的时段内(t_a, t_b)内被激活,并且该角色被激活的总次数是有限的.某段时间内,活动角色的总数目也是有限的.

③对会话的约束:在特定的时间段(t_m, t_n)内,某个云用户所能激活的会话数只能是有限个,并且在一次会话中的活动角色之间是不能相互冲突的.

(4)数据管理

存储在本地的数据可以受到局域网的保护,而云计算环境的开放性、共享性等特点以及云服务器的存在,使存储在云服务器上的云客体面临很多安全威胁.因此应对数据设置不同的安全等级设来细化对数据的访问控制管理.

当云用户创建时,云服务器根据云用户的具体属性(如职位、部门等)来设置它的安全级别,本文中取高、中、低三个级别.默认情况下,当云用户的安全级别高于云客体的安全级别时,对其具有读写权限;当云用户的安全级别与云客体的安全级别相同时,对其具有只读权限;当云用户的安全级别低于云客体的安全级别时,对其具有最小权限(即只对部分共享的数据有只读权限).如图2所示,这样分级地管理云用户和云客体,使同一云用户在分配特定角色的基础上对不同安全级别的云客体具有不同的访问权限,简化了对云用户的管理并且在一定程度上保护了云客体的安性.

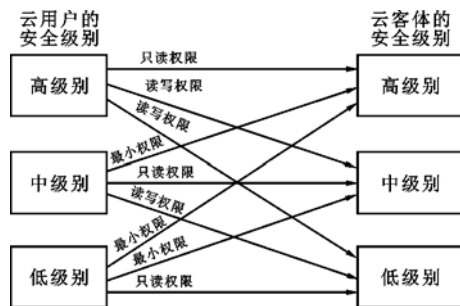


图2 云用户和云客体的安全级别

(5)权限管理

访问控制的主要目的之一就是防止非法用户获得权限,因此,对权限的管理尤为重要.

CT-RBAC模型中的关系主要包括云用户与云服务器之间的关系和云服务器与客体拥有者之间的关系,对权限的管理也从这两方面进行.

①云用户—云服务器

在访问过程中云用户对权限的需求往往是动态变化的,需要根据实际的访问情况来调整它的安全级别.这样,由云服务器监控云用户的访问行为,如果发现它的行为异常,则向下修改它的安全级别,严重情况下,强制其退出访问;如果云用户所具有的权限太小,以至于不能满足访问需求时,则向云服务器提出向上修改安全级别的请求,云服务器对该云用户进行安全验证后,发送修改云用户安全级别(云服务器为云用户所要修改的安全级别是能够满足其访问需求的最低安全级别)的申请和云用户的信息给客体拥有者.

②云服务器—客体拥有者

客体拥有者授予云服务器对其上传客体的管理权并且监控云服务器对其数据的管理行为.例如,当云服务器发送修改云用户安全级别的申请和云用户的信息给客体拥有者时,客体拥有者检查云服务器提交的信息后,发送允许或者拒绝修改云用户安全级别的消息给云服务器.这样,当云用户访问该云客体时由客体拥有者和云服务器共同管理,通过授权管理转换了云服务器在访问控制中的角色,使云服务器充当传递访问请求的中介.在一定程度上降低了云用户对云服务器的依赖,避免了由于云服务器的权限过大而带来的安全威胁,提高了客体拥有者对所属客体的监控能力并且减少了管理负担.

4.2 实现过程

在CT-RBAC的模型中,云用户在CURA关系下得到角色,通过TRA把相应的任务和角色关联起来,并通过TPA分配客体的访问权限给任务来完成分级访问控制.图3为一次访问授权过程的流程图.

具体过程如下:

步骤1:当云用户 CU_i 申请访问云服务器CS上某一特定云客体 CO_j (其拥有者是 OW_j)时, CU_i 发送访问请求 Acc 给CS.

步骤2:CS将 CU_i 的信息和 Acc 提交给 OW_j ,如

图 3 中过程 ① 所示, OW_j 检查 CS 提供的信息, 若 OW_j 允许 CU_i 访问 CO_j 则发送 App 给 CS, 否则发送 Rej , 如过程 ② 所示. CS 对客体权限列表做出相应的修改同时根据 OW_j 返回的信息允许或者拒绝 CU_i 的 Acc , 如过程 ③ 所示. 如果允许转步骤 3, 否则强制 CU_i 退出, 访问结束.

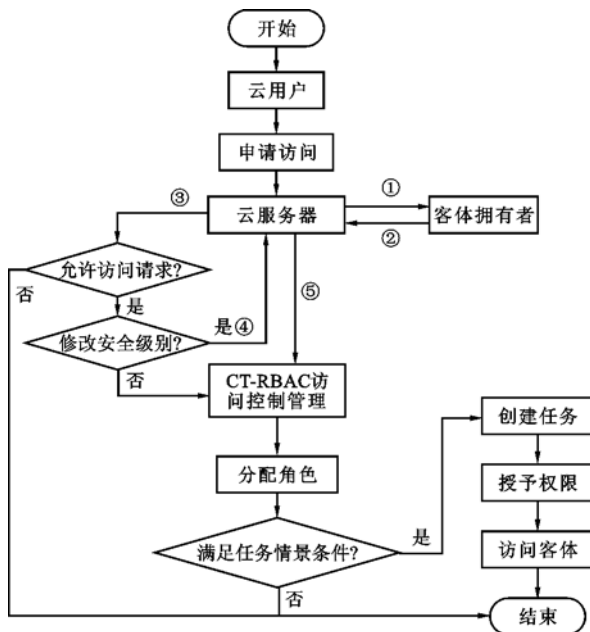


图 3 CT-RBAC 模型的访问控制实现流程

步骤 3: 默认情况下, 若 CU_i 是首次访问 CO_j , 则 CU_i 具有创建时 CS 为其划分的安全级别; 否则, CU_i 拥有最近一次访问 CO_j 的安全级别.

步骤 3.1 如果 CU_i 现有的权限能够满足对 CO_j 的访问需求, 那么 CU_i 不需要再申请修改安全级别.

步骤 3.2 如果 CU_i 现有的权限太小以至于不

能够满足对 CO_j 的访问需求, 则向 CS 提出向上修改安全级别的申请 CP, 如过程 ④ 所示. CS 根据 CU_i 现有的安全级别、访问需求、约束条件等, 把修改 CU_i 安全级别的请求以及 CU_i 的信息发送给 OW_j , 如过程 ① 所示. OW_j 检查 CS 提供的信息, 若 OW_j 同意修改请求, 返回 App , 否则返回 Rej , 如过程 ② 所示. CS 对客体权限列表做出相应的修改后, 转步骤 4, 如过程 ⑤ 所示.

步骤 3.3 访问过程中, CS 监控 CU_i 的访问行为. 如果发现 CU_i 的行为可疑, 则向低级的方向修改 CU_i 的安全级别; 严重情况下, 强制 CU_i 退出访问, 并将 CU_i 添加到拒绝访问列表中. 如果 CU_i 需要更多的访问权限, 则向 CS 提出向上修改安全级别的申请 CP, 这里与 CU_i 开始请求访问 CO_j 时具有的权限太小的情况类似, 不再详述.

步骤 3.4 访问过程中, OW_j 监控 CS 对其数据的管理行为, 并定时向 CS 发出提醒, 一旦发现 CS 的管理行为异常, 向 CS 发出警告.

步骤 4: CS 按照 CT-RBAC 访问控制策略给 CU_i 分配角色 R.

步骤 5: CS 判断该任务是否满足任务情景集的约束条件, 满足的话创建任务 T, 授予 T 对 CO_j 的操作权限, 并将 T 和 R 关起来联.

步骤 6: CU_i 所需的数据经安全验证后返回, 访问过程结束.

4.3 模型特点分析

CT-RBAC 继承了 RBAC 和 TBAC 的优点, 支持主动访问和被动访问. 具体如表 1 所示.

表 1 C-RBAC 模型特点以及优点分析

比较文献中的模型	CT-RBAC	CT-RBAC 的特点	CT-RBAC 的优点
文献[9]		考虑了任务执行时的情景条件.	提高了任务执行时的安全性和灵活性.
文献[10]		将用户划分为三类.	角色层次更加清晰, 易于管理.
文献[11]		考虑了 CS 的可信性, 由 OW 监控 CS 对 CO 的管理行为.	减少了由于 CS 不可信而带来的安全威胁
文献[12]		CU 对 CO 的访问权限可以根据实际访问需求来修改.	提高了 CS 对 CU 动态授权的灵活性.
文献[13]		由 OW 来授予 CS 对 CO 的管理权限, 同时在访问过程中由 OW 和 CS 共同管理 CO .	避免了 CS 的权限过大; 提高了 OW 对 CO 的监管能力、减轻了单独授权管理负担.
文献[14-15]		由 OW 监控 CS 的管理行为.	减少了成本, 易于扩展, 并简化了管理.

5 结束语

本文提出了 CT-RBAC 访问控制模型. 该方案考虑了云用户的动态变化性以及云计算的弹性特点,保证了云客体的安全可靠,具有很好的易扩展性和灵活性. 下一步的工作是对该模型的改进以及实施.

参考文献:

- [1] 陈全,邓倩妮. 云计算及其关键技术[J]. 计算机应用, 2009,29(9):2562-2566.
- [2] 冯登国,张敏,张妍,等. 云计算安全研究[J]. 软件学报,2011,22(1):71-83.
- [3] Balachandra R K, Ramakrishna P V, Drrakshit A. Cloud security issues[C]//IEEE International Conference on Services Computing. Bangalore: IEEE, 2009: 512-520.
- [4] 林闯,封富君,李俊山. 新型网络环境下的访问控制技术[J]. 软件学报,2007,18(4):955-966.
- [5] 邓集波,洪帆. 基于任务的访问控制模型[J]. 软件学报, 2003, 14(1):76-81.
- [6] Sandhu R, Coynee J, Feinstein HL et al. Role-Based access control models[J]. IEEE Computer, 1996, 29(2):38-47.
- [7] 熊智,王平,徐江燕,等. 一种基于属性的企业云存储访问控制方案[J]. 计算机应用研究, 2013, 30(02): 513-517.

- [8] 王小威,赵一鸣. 一种基于任务角色的云计算访问控制模型[J]. 计算机工程,2012,38(24):9-13.
- [9] LI Danchen, LIU Cheng, WEI Qiang. RBAC based access control for SaaS system[C]//2nd International Conference on Information Engineering and Computer Science. Wuhan:[s. n.],2010:1-4.
- [10] 朱养鹏,张璟. SaaS平台访问控制研究[J]. 计算机工程与应用,2011,47(24):12-16.
- [11] 赵明斌,姚志强. 基于 RBAC 的云计算访问控制模型[J]. 计算机应用,2012,32(z2):267-270.
- [12] 林果园,贺珊,黄皓,等. 基于行为的云计算访问控制安全模型[J]. 通信学报,2012,33(03):59-66.
- [13] Tang Z, Wei J, Sallam A. A new RBAC based access control model for cloud computing [J]. International Journal of Modern Education and Computer Science, 2012,5(3):279-288.
- [14] 洪澄,张敏,冯登国. AB-ACC:一种云存储密文访问控制方法[J]. 计算机研究与发展,2010,47(Suppl): 259-265.
- [15] 洪澄,张敏,冯登国. 面向云存储的高效动态密文访问控制方法[J]. 通信学报, 2011, 32(7):125-132.

作者简介:

- 常玲霞 女,(1989-),硕士研究生. 研究方向为访问控制.
- 王凤英 女,(1962-),教授. 研究方向为网络与信息安全.
- 赵连军 男,(1976-),博士,副教授. 研究方向为软件研发.
- 贾永新 男,(1975-),副教授. 研究方向为网络与信息安全.
- 程震 男,(1973-),副教授. 研究方向为网络与信息安全.

(上接第 151 页)

- [4] 梁义涛,庞蕊,朱远坤. 灰度图像二维 Otsu 折线阈值分法[J]. 计算机工程与应用,2012,48(33):178-182.
- [5] 郝颖明,朱枫. 2 维 Otsu 自适应阈值的快速算法[J]. 中国图像图形学报,2005,10(4):484-488.
- [6] Hou Z, Hu Q, Nowinski W L. On minimum variance thresholding[J]. Pattern Recognition Letters,2006,27(4):1732-1743.

作者简介:

- 张建明 男,(1964-),博士,教授. 研究方向为虚拟现实、图像处理、模式识别等.
- 李雨朋 男,(1989-),硕士生. 研究方向为图像处理、模式识别.