

云环境下的 CRUAC 访问控制模型

常玲霞, 王凤英

(山东理工大学 计算机学院, 山东 淄博 255049)

摘 要: 提出了云计算环境下的 CRUAC 访问控制模型. 该模型以使用控制模型为基础, 引入了角色的概念, 并将约束信息加入到决策判定因素中. 该模型能够解决使用控制模型中将权限直接分配给用户所带来的系统开发、重用和系统安全管理等复杂性问题, 并且为云用户访问不同云服务器上的资源提供了一种解决方案, 能够较好地满足云计算环境对访问控制的需求.

关键词: 云计算; 访问控制; CRUAC; 约束; 安全

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2015)01-0131-05

An Access Control Model Named CRUAC in Cloud Computing

CHANG Ling-xia, WANG Feng-ying

(College of Computer Science and Technology, Shandong University of Technology, Zibo 255049, China)

Abstract: CRUAC is based on usage control model, the concept of role is introduced into the model, and the constraint information is added to the decision-making factors in the model. The model can solve the complexity problems such as system development, reuse, system security management caused by assigning permissions to users directly in usage control model, and provides a solution to solve the problem of cloud users access resources which were stored in different cloud servers. The model can better meet the needs of Cloud computing environment in access control.

Key words: Cloud computing; access control; CRUAC; constraint; security

1 引言

云计算是一种新的计算资源和存储空间共享的模式^[1]. 由于云计算的动态性、开放性等特征, 使云计算环境下的访问主体不仅包括已知用户, 也包括一些潜在的未知用户. 云计算环境中的资源在各个相互独立、身份未知的实体之间共享, 对资源分发后的访问控制、隐私保护等新需求更加迫切. 与传统环境下的访问控制相比, 云计算环境下的访问控制决策依据和决策元素更加复杂, 不仅产生了连续性和易变性等新需求, 访问控制的实施范围也从服务端扩展到了客户端. 因此, 云计算下的访问控制面临更加复杂的安全需求. 虽然, 访问控制技术是解决安全问题的一个重要技术手段^[2-9], 但传统的访问控制技术并不能很好地适用于云计算环境.

2 相关研究

2.1 传统的访问控制技术

传统的访问控制技术主要包括传统的访问控制模型、信任管理(TM)技术和数字版权管理(DRM)技术^[10].

传统的访问控制模型都是对封闭系统环境中的数据保护研究, 是基于主体、客体的属性和被请求的权限来授权的, 并且主体、客体的属性是由管理员分配和维护的; 在访问过程中, 如果用户的属性发生一些变化或者对资源提出了新的访问需求, 系统并不会做出相应的处理; 传统环境下的访问主体都是可认知的; 此外, 授权都是在访问之前进行的, 用户一经授权便一直拥有该权限, 访问过程中和访问之后该权限并不会被回收或者撤销.

收稿日期: 2014-04-19; 修回日期: 2014-06-10

基金项目: 国家自然科学基金(61473179); 山东省科技发展计划项目基金(2013GGX10116); 山东省自然科学基金(ZR2013FM013)

DRM 技术主要是对客户端的数据内容进行权限管理,为多媒体内容提供者保护他们的私有数据资源免受非法复制和使用提供了一种手段.但是,DRM 需要持续的监控,在大规模环境中难以实现.

TM 技术是近年来解决开放网络中未知用户的访问控制授权问题的一种技术.但它自身仍存在一些委托控制、证书收集等问题,此外,TM 主要是对服务器端用户和资源的管理,不能对已分发的数字资源进行控制.

传统的访问控制模型、DRM 和 TM 者三种技术针对各自的问题域分别提出了相应的解决方案,但是对资源的使用缺乏灵活性、动态性和细粒度的有效控制,不利于对资源的安全保护.因此,并不完全适用于云计算环境.

2.2 UCON 使用控制模型

使用控制模型 UCON(usage control)的概念是 Park 等人于 2002 年首次提出的^[11].被称为下一代访问控制模型.2005 年, Park 等人又提出了使用控制的核心模型 UCON_{ABC}^[12].

UCON_{ABC} 定义了授权(authorization)、义务(obligation)和条件(condition)三个与授权相关的决策因素,并且提出了访问控制的连续性(continuity)和可变性(mutability)两个重要属性,这是 UCON 和传统访问控制模型相比最大的特点.这两大特性能够提供灵活的、动态的和细粒度的有效控制,能够对用户进行使用前授权和使用过程中的授权,不仅能够保护封闭环境下的数字资源,也能够保护开放环境下的数字资源.

3 云计算环境下的 CRUAC 访问控制模型

UCON 的连续性、可变性以及对象分发后的使用控制等特点提供了一种安全性和动态性较高的授权方式,对云计算环境下访问控制的多样化需求具有较好的适用性.但 UCON 的定义过于抽象,缺乏具体的授权策略,很难实现和管理.

虽然, RBAC 模型缺少一些支持现代访问控制领域的概念,并不能满足云计算环境中的访问控制需求,但是 RBAC 模型的定义清晰,管理灵活,容易扩展,在理论上和应用上都已经比较成熟,并有了大量的应用.在 UCON 中,管理员管理的对象包括客体、主体、权限和授权规则,这与 RBAC 要管理的对象相同,UCON 中主客体的可变性和授权的连续性并不需要管理员的管理,而是由监视程序自动完成的,条件和义务是系统的外部要求,也不需要管理

员来管理.在 RBAC 中,用户到角色的分配和权限到角色的分配都是由管理员完成的,这种情况在封闭系统中是可行的.对于云计算环境,用户可能是未知的,使用权限也可能是未知的,这里可以根据用户的属性来判断用户能否拥有某个角色来避免由管理员进行管理的局限性,从而解决云计算环境下用户角色分配的问题.虽然 UCON 也能够解决 RBAC 所面对的问题域,但 UCON 中并没有实现对用户、客体和权限的管理以及对约束条件的实现等问题.为了满足云计算环境下用户对访问控制的需求,这里将角色引入到 UCON 中,提出了云计算环境下的 CRUAC 访问控制模型.

3.1 CRUAC 访问控制模型的结构

CRUAC 是以 UCON 模型的核心模型 UCON_{ABC}为基础,同时引入了 RBAC 中角色的概念,把角色充当云用户行使权限的中介,将权限和云用户分开,并且将约束作为使用决策的一部分. CRUAC 模型的架构如图 1 所示.

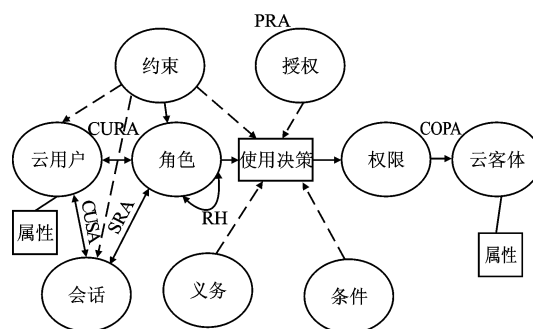


图 1 云计算环境下的 CRUAC 访问控制模型

3.2 CRUAC 访问控制模型的组成元素

CRUAC 的组成元素主要包括云用户,云客体,角色,权限,以及约束、授权、义务、条件 4 个决策因素.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,如服务、图片、音乐、视频等.

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.给云用户分配角色时,通过约束信息给角色引入时间限制来限制角色的有效期限.

属性集: $A = \{a_i \mid i = 1, 2, \dots, n\}$, 属性是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、身份等信息;云客体的名称,大小,所属的客体拥有者等信息.

会话集: $S = \{s_i \mid i = 1, 2, \dots, n\}$, 会话是特定环

境下一个云用户与一组角色的映射,云用户需要通过会话才能激活角色.云用户在每次会话中可以通过激活不同的角色来获取不同的访问权限.

约束集: $Cs = \{Cs_i \mid i = 1, 2, \dots, m\}$,约束是云计算环境中的访问控制需要充分考虑的一些用来表示实体状态的重要信息.本文中的约束信息包括时间 (Time)、位置 (Location) 和环境 (Environment).时间信息包括时间点集 T_1 (time point) 和时间段集 T_2 (time period). T_1 是云用户请求访问的时间, T_2 是云用户请求访问的一个时间区间.位置信息是云用户所处的物理位置,包括 IP 地址和空间位置信息.环境信息包括软件平台和系统状态(空闲、忙碌).

授权集: $Au = \{Au_i \mid i = 1, 2, \dots, n\}$,授权是云用户访问云客体之前必须满足的请求的集合.

义务集: $OB = \{ob_i \mid i = 1, 2, \dots, n\}$,义务是云用户在获取权限或者对云客体进行操作后必须执行的某些要求.义务包括在访问之前执行的义务 (preOB) 和访问过程中执行的义务 (onOB).preOB 是在访问请求执行前云用户体必须满足的某些条件,如云用户必须提供个人信息才能下载网站上的某些资源.onOB 是在行使权限的过程中必须持续性满足或是周期性满足的条件,如,要求云用户必须处于登录状态才能执行事务性操作.云用户履行何种义务不是预先静态设置的,而是根据云用户、云客体的属性动态确定的,履行义务时也许会更新云用户或者云客体的属性,同时这些更新能够影响现在或将来的使用决策.

条件集: $Cd = \{Cd_i \mid i = 1, 2, \dots, m\}$,条件是对云用户授权前的相关决策因素的判定,是面向环境或面向系统的决策因素.条件根据对当前硬件环境或与系统有关的限制的评估来决定是否允许云用户请求.如云用户必须使用固定的 IP 地址在规定的时段访问资源;条件也可以是对网络流量进行的限制等.

权限集: $P = \{p_i \mid i = 1, 2, \dots, m\}$,权限是云用户以特定的方式(如读、写、执行)来访问某个云客体.当云用户访问云客体时,权限是随着云用户、云客体的属性和约束、授权、义务、条件这些决策因素而动态变化的.

使用决策 (UD) 定义为 $UD(Cs, Au, OB, Cd)$ 一个四元组,当云用户 cu_i 请求对云客体 co_j 的访问权限 p_i 时, Cs 为授权决策要判断的约束信息集, Au 为授权决策应判断的授权规则集, OB 是授权决策应判断的义务集, Cd 为授权决策要判断的条件集.

如果满足对 $UD(Cs, Au, OB, Cd)$ 的判断,则将 p_i 授予 cu_i ,否则不能将 p_i 授予 cu_i .

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

CUSA: $CUSA \subseteq CU \times S$,云用户和会话之间的分配关系.

SRA: $SRA \subseteq S \times R$,会话和角色之间的分配关系.

RH: 角色之间的继承关系.

PRA: $PRA \subseteq R \times P$,权限到角色的分配关系.

COPA: $COPA \subseteq CO \times P$,权限到云客体的授权分配关系.

此外,指向使用决策的带箭头的虚线表示使用决策由与虚线相连的这四个元素组成.由约束向外的带箭头的虚线表示约束信息是针对云用户、角色、会话和使用决策的.

4 CRUAC 模型的实现

4.1 CRUAC 模型的访问控制策略的组件

CRUAC 的访问控制策略主要包括两个组件:虚拟资源管理者 (VRM) 和访问控制模块 (ACM),其中,ACM 包括策略决策点 (PDP),策略执行点 (PEP) 和策略库 (PR).VRM 是负责提供和分发虚拟资源的虚拟资源管理服务器,它维持一个虚拟资源及配置列表.为了便于管理,本文称首次处理云用户访问申请的云服务器为内部云服务器 CS1,相对而言,其他的云服务器称为外部云服务器 CS2.虚拟资源列表包括内部虚拟资源列表和外部虚拟资源列表,其中,内部资源列表用来记录、管理内部云服务器上的虚拟资源,而外部虚拟资源列表只是对外部云服务器上资源的一种映射.VRM 能够根据虚拟资源列表来判断云用户访问的资源是存储在哪个云服务器上.每个云服务器只能对内部虚拟资源列表中的资源进行授权、管理,当云用户申请访问的资源在外部云服务器上时,需要跨云的访问控制.此外,VRM 能够监控使用中的资源、释放或者回收这些资源.

ACM 是用来执行云计算环境下访问控制的策略.PEP 是介于云用户和访问资源之间的一种服务或应用.当云用户申请访问时,PEP 向 PDP 发送授权请求,并根据 PDP 做出的决策结果实施访问操作.此外,PEP 还可以作为审计控制点,对进出边界的所有行为实施安全审计.PDP 主要包括策略评估者,策略评估者接收和评价授权请求,根据云用户、

资源、请求权限的类型、使用决策以及预定义的安全策略做出不同的策略决定,并将决策结果返回给 PEP. 在云用户访问资源的过程中 PDP 监控云用户的访问行为,动态的调整云用户的角色和权限. PR 是用来确定云用户能否访问云客体的一套授权规则.

4.2 CRUAC 的资源访问控制过程

由于云计算环境的异构性,不同云服务器可能使用不同的访问控制模型和策略.此外,由于一个云用户请求的资源也许并不存储在它所申请的云服务器上,而是存储在另一个云服务器上.因此一个完整的访问控制策略必须支持云用户在不同云服务器之间资源的访问.

云用户访问云服务器上资源的具体过程如图 2 所示,步骤如下:

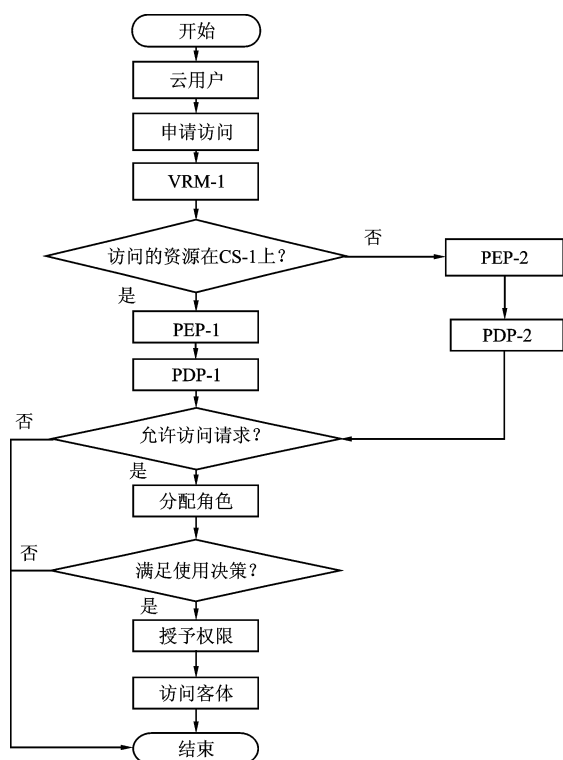


图 2 CRUAC 模型的访问控制实现流程

(1) 当一个云用户 cu_i 请求访问资源的时候,该请求包括的 cu_i 的身份信息、请求资源以及请求该资源的权限类型(如读或者写权限),这个请求也可能包括认证或者授权需要的证书.该请求消息被发送到 CS1 的虚拟资源管理者 VRM-1.

(2) VRM-1 判断 cu_i 所请求的资源是否在 CS1 的资源库中.如果 cu_i 所请求的资源在 CS1 的资源库中,VRM-1 将判断结果以及 cu_i 的请求信息发送给 CS1 的策略执行点 PEP-1,转步骤 3;否则,如果

cu_i 要访问的资源在 CS2 上,转步骤 6.

(3) PEP-1 从该请求中提取 cu_i 的身份凭证,生成包含 cu_i 身份信息的访问请求,并将此访问请求转发给 CS1 的策略决策点 PDP-1.

(4) PDP-1 首先检查 cu_i 的身份信息,并根据 CS1 的使用决策 UD-1 中的约束信息 $Cs-1$ 判断是否允许 cu_i 的访问请求.如果允许,转步骤 5;否则 PDP-1 向 PEP-1 发送拒绝消息,访问终止.

(5) PDP-1 从 PR-1 中的用户-角色指配关系给 cu_i 分配一个角色,并根据 UD-1 中的决策信息来判断是否对 cu_i 做出授权.如果 cu_i 满足 UD 中的决策因素,PDP-1 对 cu_i 做出授权,将授权决定结果发送给 PEP-1,并通知 CS1 的 VRM-1 来标识和配置本次需要的资源;否则强制 cu_i 退出,访问结束.

PEP-1 接受策略决策中心对授权请求做出的决定,授予或者拒绝 cu_i 的授权请求,执行访问请求,完成对目标资源的操作,访问结束.

(6) VRM-1 将 cu_i 的请求信息发送给 CS2 的策略执行点 PEP-2.

PEP-2 根据 cu_i 的信息生成访问请求,并将其发往 CS2 的策略决策点 PDP-2.

PDP-2 首先检查 cu_i 的身份信息,并根据 CS2 的使用决策 UD-2 中的约束信息 $Cs-2$ 判断是否允许 cu_i 的访问请求.如果允许,转步骤 7;否则 PDP-2 向 PEP-2 发送拒绝消息,访问终止.

(7) PDP-2 从 PR-2 中的用户-角色指配关系给 cu_i 分配一个角色,并根据 UD-2 中的决策信息来判断是否对 cu_i 做出授权.如果 cu_i 满足 UD-2 中的决策因素,PDP-2 对 cu_i 做出授权,将授权决定结果发送给 PEP-2,并通知 CS2 的虚拟资源管理者 VRM-2 来标识和配置本次需要的资源;否则强制 cu_i 退出,访问结束.

PEP-2 接受策略决策中心对授权请求做出的决定,授予或者拒绝 cu_i 的授权请求,执行访问请求,完成对目标资源的操作,访问结束.

此外,在 cu_i 访问资源的过程中 PDP 监控 cu_i 的访问行为,动态地调整 cu_i 的角色和权限.如,当 cu_i 由于属性的更改使其角色不再符合授权规则时,系统将结束 cu_i 本次的访问控制过程;当 cu_i 做出非法访问的时候,系统会撤销赋予 cu_i 的权限.

5 CRUAC 模型的特点分析

CRUAC 模型是一种特殊的使用控制模型,与 RBAC 和 UCON 相比,CRUAC 模型的主要特点如

表 1 所示.

表 1 CRUAC 模型的特点

	优点	缺点
RBAC	授权灵活;易于实现	不具有动态性,不能实现实时约束
UCON	具有连续性和可变性;能够实施实时控制;能够表示多种访问控制模型	模型抽象,实施困难
CRUAC	具有连续性和可变性;能够实施实时控制;能够表示多种访问控制模型;决策因素更具体;授权灵活;管理简单;能够实现跨云访问控制	模型的实现比较复杂

(1)CRUAC 模型中引入了角色的概念,采用基于角色的授权方式最大程度地减少了因权限赋予具体化造成的系统灵活性的降低,便于实施和管理. CRUAC 也能够表达 DAC、MAC、RBAC 等访问控制模型.

(2)CRUAC 模型将约束信息引入到决策因素中.约束不仅能够对模型中的各个元素进行冲突控制,也能够动态地支持使用决策的连续性和属性的可变性,能够对资源提供充足的保护.

(3)CRUAC 模型除了保留了 UCON_{ABC} 模型的主要概念和特性,还对部分概念的定义进行了具体化,提高了模型的可管理性和可应用性.

(4)在访问过程中,CRUAC 模型一直监控云用户的访问控制过程,并根据监控结果改变该云用户角色的属性和授予云用户的权限. CRUAC 模型中,当云用户被授予一定的初始权限后,在使用权限的过程中,CRUAC 模型根据授权、义务、条件和约束四个决策因素的限制来改变云用户的权限.云用户的权限是随着它对资源的访问状况而动态变化的.权限的动态变化过程反映了 CRUAC 授权的连续性和动态性.

(5)CRUAC 模型提供了一种跨云访问的访问控制策略,为资源更好的共享提供了一种解决方案.

6 结束语

CRUAC 模型继承了 UCON 和 RBAC 的优点,不但能够解决 UCON 模型具有的广泛的问题域和 UCON 模型中将权限直接分配给用户所带来的安全问题,也能够解决 RBAC 中的职责分离问题,为跨云访问问题提供了一种解决方案.与 UCON 相

比,CRUAC 易于实现和应用,能够较好地满足云计算环境对访问控制的需求.下一步工作是对该模型的优化和应用研究.

参考文献:

- [1] 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.
- [2] 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.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] A A Almutairi, M I Sarfraz, S Basalamah, et al. A distributed access control architecture for Cloud computing[J]. ,IEEE Software, 2012,29(2):36-44.
- [7] Berger S,Cáceres R,Goldman K, et al. , Security for the Cloud Infrastructure: Trusted Virtual Data Center Implementation[J]. IBM J Research and Development, 2009,53(4): 560 - 571.
- [8] Y Zhu, H X Hu, G J Ahn, et al. Towards temporal access control in cloud computing [C] // 2012Proceedings IEEE on INFOCOM. Beijing:IEEE, 2012:2576-2580.
- [9] 张德银,刘连忠. 多安全域下访问控制模型研究[J]. 计算机应用,2008,28(3):633-636.
- [10] R Sandhu, J Coynee, H L Feinstein, et al. Role-Based access control models[J]. IEEE Computer, 1996,29(2):38-47.
- [11] J PARK, R Sandhu. Towards usage control models: Beyond traditional access control [C]// Proceedings of the 7th ACM Symposium on Access Control Models and Technologies. Monterey Colifonia: ACM press, 2002:57-64.
- [12] J PARK, R Sandhu. The UCONABC: usage controlmodel[J]. ACM Trans on Information and System Security,2004,7(1): 1-47.

作者简介:

常玲霞 女,(1989-),硕士研究生.研究方向为访问控制、数据起源. E-mial:lingxia1224@126.com.

于风英 女,(1962-),教授.研究方向为网络与信息安全.