

一种适用于云计算环境的跨域访问控制模型

江泽涛, 谢 朕, 王 琦, 张文辉

(桂林电子科技大学 计算机与信息安全学院, 广西 桂林 541004)

摘 要: 使用控制模型(Usage Control, UCON)涵盖了传统的访问控制、可信管理及数字版权等复杂需求, 被称为下一代访问控制模型. 但是由于其授权实现较为复杂, 其实际应用还处于探索阶段. 将 UCON 模型中的义务元素删除、条件元素进拆分后使其实现大为简化. 同时提出了三种在云计算环境下将传统访问控制模型转换为支持 UCON 模型的方法.

关键词: 使用控制模型; 云计算; 跨域访问; 授权

中图分类号: TP391

文献标识码: A

文章编号: 1000—7180(2017)03—0065—05

A Cross-Domain Access Control Model for Cloud Computing Environments

JIANG Ze-tao, XIE Zhen, WANG Qi, ZHANG Wen-hui

(School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: UCON (Usage Control) is able to cover access control, trust management and DRM (Digital Rights Management) and called the next generation access control model. However, its practical application is still in the exploratory stage because of its mandate is complex. The author removes the obligation element and splits condition element to simplify the implementation. At the same time, author puts forward three basic control modes which can meet the needs of cross-domain access control in the cloud computing environment.

Key words: UCON; cloud computing; cross-domain access; authorization

1 引言

随着云计算的发展, 跨域访问成为一种越来越流行, 也越来越重要的数据交换方式, 同时由于对放置在云服务器中的数据失去控制, 如何在保证数据安全的情况下, 高效地管理数据的访问权限是云安全中非常重要的一环^[1]. 为此本文提出了云环境下, 一种基于 UCON 模型的跨域访问控制模型. 该访问控制模型不影响现有域内访问控制, 并实现了高效跨域访问控制.

访问控制通过对用户访问资源的活动进行监控, 使合法的用户在合法的时间内获得有效的访问

权限, 防止非授权用户访问资源^[2].

由于互联网环境下数据量的日益增多, 分散的资源已经无法应对大数据的存储及分析的需求. 云计算通过对网络中分散的资源及任务进行统一的调度和管理, 成为解决上述矛盾的一个重要途径, 但是, ABAC 简单的访问前单次授权模式无法满足复杂的云计算环境中的资源动态分配需求. 使用控制模型(Usage Control, UCON^[3])通过对可变属性的支持使得授权时间由访问前授权扩展为访问前(Pre)、访问中(OnGoing)及访问后(Post)三个阶段动态的授权决策, 可以及时地进行权限授予和回收. Park 等人在研究了传统领域的访问控制、可信管

收稿日期: 2016—06—09; **修回日期:** 2016—07—23

基金项目: 国家自然科学基金(61572147); 广西可信软件重点实验室项目(kx201502); 桂林电子科技大学图像图形智能处理重点实验室项目(GIIP201501, GIIP201401)

理、数字版权等问题后,明确了以授权(Authorization)、义务(oBligation)和条件(Condition)为核心的 UCON 模型(如图 1 所示),即 $UCON_{ABC}$ ^[4]模型,并给出了其在可信管理、数字版权等问题的应用模式^[5]. 尽管 $UCON_{ABC}$ 模型非常的强大,但是由于其授权实现较为复杂,其实际应用还处于探索阶段.

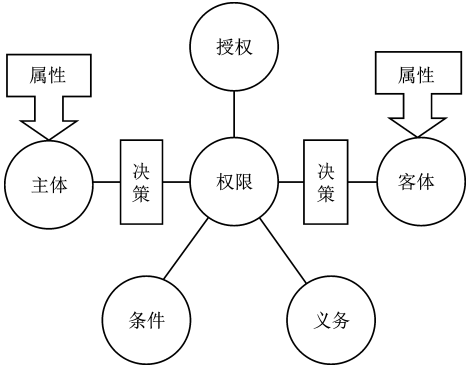


图 1 UCON 模型元素示例图

2 基于 $UCON_{ABC}$ 模型改进的 $UCON_{AC}$ 模型

$UCON_{ABC}$ 模型拥有强大的访问控制能力,能将传统的访问控制、可信管理及数字版权问题统一管理,非常适合作为云计算环境下的访问控制模型,但是授权实现较为复杂. 本文将从 3 个方面对传统的 $UCON_{ABC}$ 模型进行改进,从而使得在跨域访问控制中授权实现过程大为简化.

2.1 删除义务元素

义务元素为授权前或授权中对主体的强制要求. 例如在数字版权问题中,一部电影的数字拷贝每次播放需要缴费 1 元,义务元素的存在可以对每次的播放操作进行监控,确保用户的每一次观看行为都是已付费的. 但是,现实情况中,对于已经获取到客体资源的主体来说,监控或限制其后续行为的成本是非常高昂的. 相对于仅需要进行有限次决策的授权元素及条件元素,义务元素其实现的复杂度要显著高于前者. 同时在决策过程中义务的使用频率也较低,仅在涉及数字版权问题的情况下需要使用. 为了降低在决策及实现过程的复杂度,将义务元素删除.

2.2 捆绑主客体及其属性

在传统的客户端/服务端(Client/Server, C/S)模式中,主客体属性均存储在服务端中. 主体发起访问请求后,服务端根据本地存储的数据进行身份确认,根据主体身份读取主体属性(如图 2 所示).

这种模式下,大量的主体属性需要存储在服务

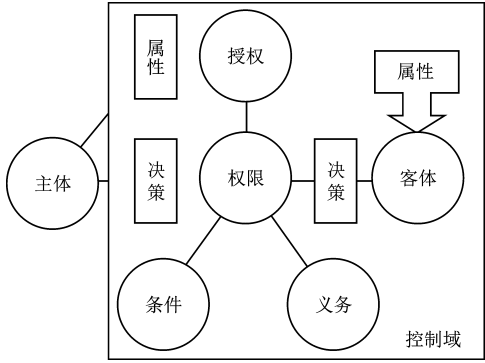


图 2 传统 C/S 模式元素分布示例图

端中,造成了服务端数据存储压力过大. 同时由于不同的服务端均需要存储主体属性,导致了数据大量的重复存储,而且客户端在更改数据时需要通知所有的服务端进行修改. 为了解决以上问题,将主体属性与主体捆绑存储于主体所在域内,客体属性与客体存储于客体所在域内. 例如,在网购的过程中,消费者分别在某东和某猫两家商城的服务端存储了自己的地址信息,当需要更换地址时,消费者必须同时在两家商城中修改信息. 而将消费者的地址信息存储于某个本域内的终端(例如手机)中,消费者在自己的手机上修改了地址信息后,下单时由服务端访问消费者的手机获取相关信息,就可以避免数据的重复修改及重复存储的问题.

2.3 分离条件元素

条件元素主要是针对当前域环境及系统状态的限制,根据申请发出时系统环境情况(如主体访问的地理位置和申请的时间等)以及系统状态(如 CPU 使用率、内存使用率、网络使用率和硬盘使用率等)进行决策. 条件元素的决策过程比较靠前,一般优先进行条件元素的决策再进行授权规则的决策,同时条件元素的设定更为全局化,条件的数据量较授权规则数量较少. 在 UCON 中,由于有条件元素的存在,可以实现对整体访问行为的精确管控. 在跨域访问过程中,由于主体与客体不在相同的域内,为了实现访问行为灵活的管控,将条件拆分为主体条件和客体条件. 主体条件针对域内主体发出访问申请时的系统状态或环境情况限定是否允许发出申请,例如针对学生的主体限制访问域外资源的时间为 7:00 至 23:00. 客体条件针对域内客体接收访问申请时的系统状态或环境情况限定是否可以接受申请,例如针对普通用户限制 8:00 至 22:00 时间内且平均 IO 使用率低于 50%时可访问域内资源.

在将义务元素删除、条件元素分离后,形成了一

种以授权 (Authorization) 和条件 (Condition) 为核心元素的 UCON 模型的扩展, $UCON_{AC}$ 模型. 尽管简化了针对数字版权保护相关的元素, $UCON_{AC}$ 模型依然具备强大的控制能力. 特别是对访问控制技术的支持没有改变, 但是实现难度却比原 $UCON_{ABC}$ 模型要大大降低. 同时由于其他类元素并未修改, 支持 $UCON_{ABC}$ 模型的访问控制系统几乎可以不做改动的支持新的 $UCON_{AC}$ 模型.

3 辅助模块

当前网络环境中, 各控制域现有的访问控制系统采用不同的访问控制模型, 大规模的将非 UCON 模型的访问控制系统转换为 UCON 模型, 必然需要消耗大量的资源. 同时, 控制规则的转换不仅需要大量的测试工作而且不可避免地会影响当前域内的访问控制行为. 为了更加方便地进行模型改造, 尽可能不影响控制域内正常访问, 需要新增辅助模块协助 (Assistant Module, AM) 完成 $UCON_{AC}$ 模型的改造.

针对未使用 UCON 模型的控制域, 需要增加一个独立的辅助模块 AM, 从而完成跨域访问控制. AM 模块的实现可以由不同的域内自助开发完成, 只需要支持统一的网间通讯协议并提供必备的功能. AM 需要提供以下几个主要功能.

AM 需要提供对于主体或客体的属性的提取及创建. 对于决策过程中需要用到的属性, 若属性能够直接从访问控制系统中进行提取, 则需要 AM 直接提取对应属性, 称为原始属性, 例如学生的学号信息; 若属性能够从原始属性中增强得来, 则需要 AM 记录相关属性的增强规则, 称为增强属性, 例如根据学生的学号信息增强出学生所属专业及入学时间; 若属性无法自动从域内获取, 则需要 AM 记录下对应的属性, 称为扩展属性, 例如学生的手机号.

AM 需要对外提供属性的读取功能. AM 需要对外提供统一的属性查询接口, 支持在授权过程中对属性的查询操作.

AM 需要对外提供属性的初始化及修改功能. 由于 UCON 模型支持可变属性, AM 需要对外提供统一的属性修改接口, 支持在授权过程中对某些属性进行修改, 或将某些不存在的属性进行初始化.

AM 需要对外提供条件的读取功能. AM 需要对外提供统一的条件查询借口, 支持在授权过程中对属性的查询操作.

AM 需要对条件中与属性无关部分进行简单决

策功能. AM 需要对仅涉及本域内环境或系统状态的简单条件予以决策, 例如当前系统时间及当前系统资源利用率等条件, 并选择允许决策的继续进行或拒绝.

在云计算环境下, 各个控制域采取的模型及策略均不相同, 模型的转换必然需要消耗大量的资源. 在添加辅助模块后, 可以在不影响控制域内正常访问的情况下实现模型的转换.

4 $UCON_{AC}$ 模型在跨域访问中的应用

在跨域访问中, 主体与客体分别处在不同的域内, 将主体所在域称为主域, 客体所在域称为客域, 若涉及到第三方域则称为异域. 根据负责授权决策的域不同, 我们将跨域访问行为分为客域控制、主域控制及异域控制.

4.1 客域控制

客域控制中, 主域内存储主体及其属性和条件, 客域内存储客体及其属性和条件以及授权规则, 由客域负责访问控制决策过程, 主域内新增辅助模块 (如图 3 所示).

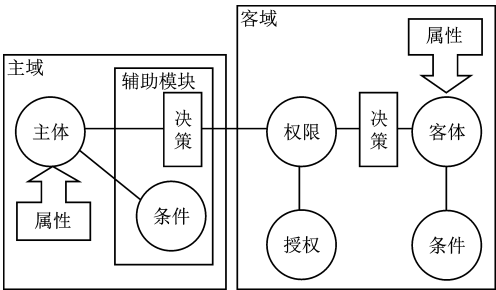


图 3 客域控制模式

这是与传统 C/S 比较类似的情况, 主域类似于客户端, 客域类似于服务端. 在传统的网络 C/S 模式中, 所有的资源均存储在服务端, 而客户端提出申请后, 由服务端进行身份校验, 根据获取的身份信息后查询用户的相关属性进行授权决策. 但是在云计算环境中, 服务端存储主体属性的方式, 不仅导致服务端数据存储量的暴增, 也导致各服务端的数据重复存储. 在客域控制模式下, 主体属性被从客域剥离出来, 存储于主域中, 既解决了客域数据存储的压力, 又避免了重复存储的问题.

整个访问过程, 由主域发起访问申请, 客域接到申请后提取授权规则、义务及条件, 并根据所需的主体属性向主域辅助模块进行属性查询, 并根据主域辅助模块的相关返回结果进行授权决策. 主要步骤如下.

Step 1:主体向客体申请权限(读/写).

Step 2:主域辅助模块根据主体的条件决策是否发送申请.

Step 3:客域根据客体条件决策是否接受申请.

Step 4:客域根据授权规则决定是否需要读取或修改属性.

Step 5:客域决策允许或拒绝访问.

4.2 主域控制

主域控制中,主域内存储主体及其属性和条件,客域内存储客体及其属性和条件以及授权规则,由主域负责访问控制决策过程,客域内新增辅助模块(如图 4 所示).

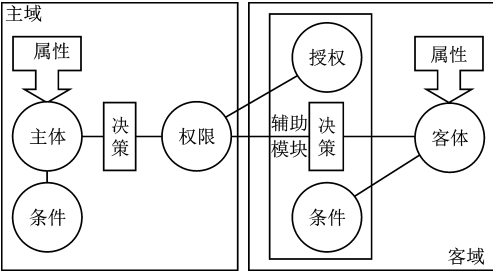


图 4 主域控制模式

这是一种比较少见的模式. 由于整个授权过程中的授权规则与客体及所需的权限相关,因此一般将授权决策的过程与客体放在同一域内. 但是在某些主体较多的域内也有对外提供资源访问的需求,或是两个域内同时拥有大量的主体与客体,主体需要在两个域间进行跨域访问,客体需要在两个域间进行跨域分享. 这种模式下主域和客域的位置是相互转换的,可以选择由支持 UCON_{AC}模型的域进行统一的授权决策操作.

整个访问过程,由主域发起访问申请,客体辅助模块接收到申请之后,根据客体及权限的相关设置返回对应授权规则及条件,主域根据客域辅助模块返回的信息及主体的相关属性进行授权决策. 主要步骤如下.

Step 1:主体向客体申请权限(读/写).

Step 2:主域根据主体的条件决策是否发送申请.

Step 3:主域向客域辅助模块读取授权规则.

Step4:客域辅助模块根据客体条件决策是否接受申请并发送授权规则.

Step5:主域根据授权规则决定是否需要读取或修改主体或客体的属性.

Step6:主域决策允许或拒绝访问.

4.3 异域控制

异域控制中,主域内存储主体及其属性和条件,客域内存储客体及其属性和条件以及授权规则,由于主域和客域均不支持 UCON_{AC}访问控制模型,需要新的第三方域来负责访问控制决策过程,称为异域. 主域和客域内新增辅助模块(如图 5 所示).

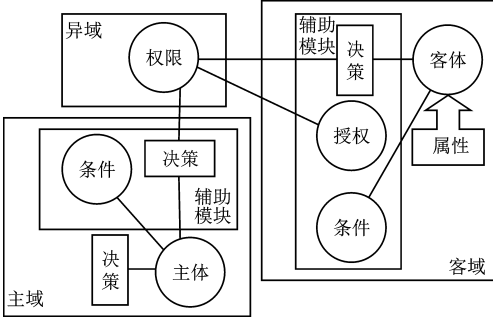


图 5 异域控制模式

这是一种对现有网络环境改造后将会出现的较为常见的模式. 对于主域和客域都使用较为简单的访问控制模型的情况,在传统的处理方式中想要使用跨域访问,需要对模型进行复杂的改造,或由双方管理员协商相关的转换原则,在云环境中这种事前协商或改造的方式显然不能满足实时性和复杂的域间关系的需求. 在异域控制中,需要协商一个可信的第三方域,用来对跨域访问控制进行决策,这种协商可以由两个域自助完成,不需要管理员的干预. 异域本身支持使用 UCON_{AC}模型进行访问控制. 主域和客域分别增加一个辅助模块,异域通过与主域和客域辅助模块通讯查询主体和客体属性并完成访问控制授权决策.

整个访问过程,由主域向客域发送客体及所需权限的申请,而后两者协商寻找支持授权决策的异域,由主域向异域发送客域、客体及权限的申请,异域向客域辅助模块查询客体及权限对应的授权规则及条件,向主域辅助模块查询决策中需要用到的主体属性,根据属性进行决策. 主要步骤如下.

Step 1:主体向客体申请权限(读/写).

Step 2:主域辅助模块根据主体的条件决策是否发送申请.

Step 3:客域辅助模块根据客体条件决策是否接受申请.

Step 4:主客域的辅助模块协商寻找负责决策的异域.

Step 5:异域向主域和客域的辅助模块申请属性,条件及授权规则以及更新主客体的属性.

Step 6:异域决策允许或拒绝访问。

以上三种模式涵盖了所有的基础跨域访问情景,在添加了辅助模块之后,不需要对原控制域的访问控制系统进行重建就可以实现 $UCON_{AC}$ 模型下的跨域访问控制,大大降低了模型改造的风险。

5 结束语

通过对义务元素的删除以及对条件元素的分离,使得 $UCON_{AC}$ 模型在跨域访问控制中更加的灵活易用,实现起来也更为简单。同时辅助模块使得各控制域在不影响域内正常访问的前提下,以较小的代价,改造为支持 $UCON_{AC}$ 跨域访问的控制域,与三种不同模式的跨域访问行为结合,涵盖了所有的基础跨域访问情况。但是对于异域存储属性的加密、域间可信判断、统一通信模型及属性存储模型的建立需要进一步的研究。

参考文献:

[1] 王于丁,杨家海,徐聪,等. 云计算访问控制技术研究综述[J]. 软件学报, 2015, 26(5):1129-1150.

[2] 李风华,苏铨,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, 40(4): 805-813.

[3] Park J, Sandhu R. Towards usage control models: beyond traditional access control[C]//Proceedings of the seventh ACM symposium on Access control models and technologies. ACM, 2002: 57-64.

[4] Park J, Sandhu R. The $UCON_{ABC}$ usage control model[J]. ACM Transactions on Information and System Security (TISSEC), 2004, 7(1): 128-174.

[5] Sandhu R, Park J. Usage control: A vision for next generation access control[M]//Computer network security. Springer Berlin Heidelberg, 2003: 17-31.

作者简介:

江泽涛 男,(1961-),博士,教授.研究方向为图像处理与计算机视觉、网络信息安全.

谢 朕(通讯作者) 男,(1989-),硕士研究生.研究方向为网络信息安全. E-mail:XenonZinc@qq.com.

王 琦 男,(1992-),硕士研究生.研究方向为网络信息安全.

张文辉 女,(1970-),硕士,副教授.研究方向为图像处理与计算机游戏设计.

(上接第 64 页)

[6] 徐进,孟晓风,钟波. 基于 MTM 总线的测试系统设计方法[J]. 计量与测试技术,2009,36(2):27-33.

[7] 王帅. 基于 MTM 总线的边界扫描控制器设计与实现[J]. 计算机测量与控制,2012,20(4):929-932.

[8] 卢上丁,雷加,黄新,等. MTM 总线模块间通信体系的研究和应用[J]. 计算机工程,2010,36(3):254-259.

[9] 张维旭,贺占庄. 基于 Nios II FPGA 和 ARINC429 通信板的设计[J]. 微电子学与计算机, 2006, 23(6): 210-212.

[10] 薛乐平,付宇卓,谢凯年,等. Core 与总线系统的异步通信接口设计[J]. 微电子学与计算机,2006,23(7): 111-114.

作者简介:

王宇飞 女,(1992-),硕士研究生.研究方向为数字通信及其 FPGA 实现. E-mail:575750947@qq.com.

邹小东 男,(1988-),硕士研究生.研究方向为数字通信及其 FPGA 实现.