第41卷 第6A期 2014年6月
计 算 机 科 学 Computer Science
Vol. 41 No. 6A June 2014

云环境下基于UCON的访问控制模型研究

蔡 婷[1] 陈昌志[1,2]
(重庆邮电大学移通学院计算机系 重庆 401520)[1] (重庆邮电大学计算机学院 重庆 400065)[2]

摘 要 UCON(Usage Control)访问控制模型,通过引入"义务"和"条件"两个概念,实现了传统访问控制模型、信任管理和数字版权管理3个技术领域的融合,扩展了模型的控制覆盖范围,能更好地应用于云计算环境。针对UCON模型的隐私保护问题,提出了一种基于加密方式的授权管理控制模型——AM-UCON。该模型在认证和监控的基础上,以多方验证的方法来提高属性更新的可信性和授权的正确性,能在一定程度上抵制恶意篡改隐私策略信息的问题。最后给出该模型的实现过程,并在基于云计算的数字对象发布系统中予以实现。

关键词 云环境,UCON,访问控制,授权管理,隐私策略
中图法分类号 TP393 **文献标识码** A

Research for Access Control Model Based on UCON in Cloud Computing

CAI Ting[1] CHEN Chang-zhi[1,2]
(Department of Computer, College of Mobile Telecom, Chongqing University of Posts and Telecommunications, Chongqing 401520, China)[1]
(College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)[2]

Abstract UCON(Usage Control) access control model, by introducing two concepts of "obligation" and "conditon", integrates the three technical fields of traditional access control model—confidence mana-gement and digital copyrigh management, and extends the cover scope in control mechanism of the model, which make it more adapt to cloud computing. In consideration of the privacy protection in UCON model, an authorized management control(AM-UCON) model based on encryption pattern was proposed. Based on identification and monitoring, the model uses multiple validation to improve the creditability in the renew of attributes and the correctness in authorization, to some extend, which can deal with the problem of malicious tampering for privacy strategies. Finally, the model's realization process was given, and was achieved in the digital object release system based on cloud computing environment.

Keywords Cloud environment, UCON, Access control, Authorize manage, Privacy strategy

1 引言

云计算的出现推动了互联网的进步,但其在安全性、可靠性等方面的表现仍不够理想,这就为访问控制模型的研究提出了新的要求。目前,云计算所面临的安全问题主要集中在访问控制和授权、虚拟化安全以及Web安全防护3方面[1]。由于受到虚拟化、弹性化等特性的影响,传统的访问控制模型并不完全适用于云计算环境,因此有必要针对云计算这一特殊的计算模式,设计一种符合云计算特点的访问控制模型。

传统的访问控制分为3类:自主访问控制(Discretionary Access Control, DAC)、强制访问控制(Mandatory Access Control, MAC)和基于角色的访问控制(Role-Based Access Control, RBAC)[2]。DAC模型在20世纪70年代初已形成,它定义了一套规则:系统中的主体可以自主地将其拥有的对客体的访问权限授予它的主体。这种模型简单直观,为用户提供了一种灵活易行的数据访问方式,但授权安全性相对较低、系统效率低下,难以满足大型系统的网络需求。MAC模型来源于军事和国家安全领域,通过控制主体和客体之间的信息流来控制对数据的访问,虽然强制访问控制很有效,但是缺乏灵活性,不能很好地适用于对数据完整性要求较高的商业应用领域。20世纪90年代,Ferraiolo等提出基于角色的访问控制模型(RBAC)[3],该模型引入角色的概念,将主体和客体分离,使访问控制变得更加灵活,简化了权限的管理。但由于传统访问控制模型的局限性,缺少一种综合的、系统的方法来控制特定环境中数字对象的使用;并且其授权均是在实施访问之前进行的,对访问过程中发生的新的授权需求并不能处理,这些缺陷导致上述模型不能很好地应用于云环境。2002年,R. Sandhu和J. Park首次提出了UCON(Usage Control,使用控制)模型[4],该模型相比传统访问控制模型来说,灵活性更高,更能适应云计算的发展需要。

2 UCON模型分析

对云计算来说,确定访问控制模型是制定云计算访问控制方案的首要任务。相对传统的访问控制模型,UCON模型引入了义务和条件两个核心元素,综合了信任管理和数字版权管理两项访问控制领域诞生的新技术[5,6],能够很好地满足云环境中的新需求。

蔡 婷(1984—),女,硕士,讲师,主要研究方向为网络安全结构与控制技术,E-mail: ct-dolphin@163.com;陈昌志 男,副教授,主要研究方向为计算机系统结构、图像处理等。

2.1 UCON 模型的新范围

UCON 模型中多了两个关键组件——义务和条件。其中，义务的加入使得模型将行为（主体引发的，或客体变化带来的）纳入了控制范围中，条件又将环境因素纳入到了控制范围中，加上引用监控机制的多样性和灵活性以及访问控制模型本身的存在元素，很好地实现了传统访问控制模型、信任管理和数字版权管理 3 种技术的融合[5,6]；并且，UCON 模型是由义务、条件和授权三者共同构建和作用，不仅能够实现原有的控制，还因为共同作用使得控制范围有所扩展，极大地提高了模型的灵活性和描述能力，从而更好地应用于云计算环境。

图 1 显示了 UCON 的覆盖区域和它与其他研究区域的关系。从图中可以看出，UCON 模型能够通过不同的配置覆盖诸如敏感信息保护等所有的访问控制目标。

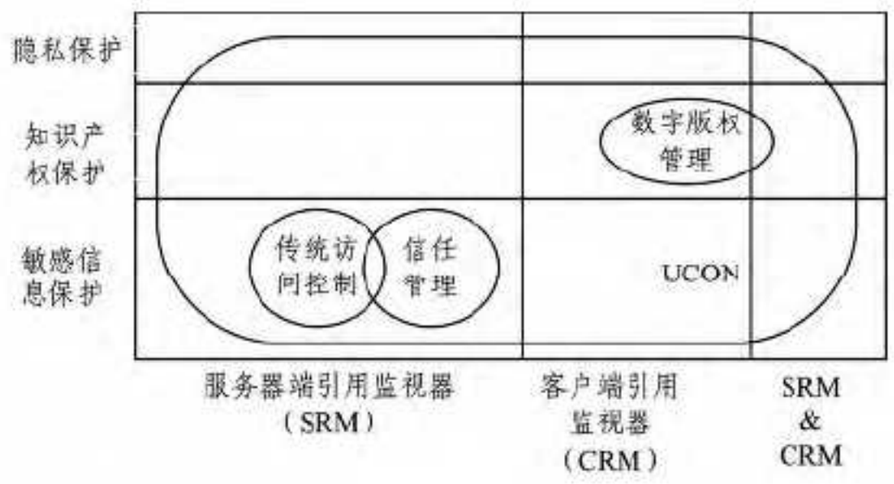

图 1 UCON 模型的覆盖范围

2.2 UCON 模型的新特征

义务和条件组件的加入同时也给 UCON 模型带来了两种重要的特性：连续性和可变性。传统的访问控制，授权决策都是在访问操作之前进行的，而 UCON 却可以实现在使用过程中（ongoing）和使用后（post）对数据资源的使用进行监控，这种“持续性”使得 UCON 具有持续控制的特性；所谓“可变性”，是指属性的可变性，系统能够在使用前、使用中和使用后实时地更新属性[5-7]。传统的访问控制，属性只能通过管理行为才能被修改，这种局限性无法满足实际应用中属性因主体行为而被修改的情况。图 2 描述了 UCON 模型的控制连续性和属性可变性，这两种特性使得 UCON 访问控制模型在应对云环境下基于历史的授权决策更容易实施。

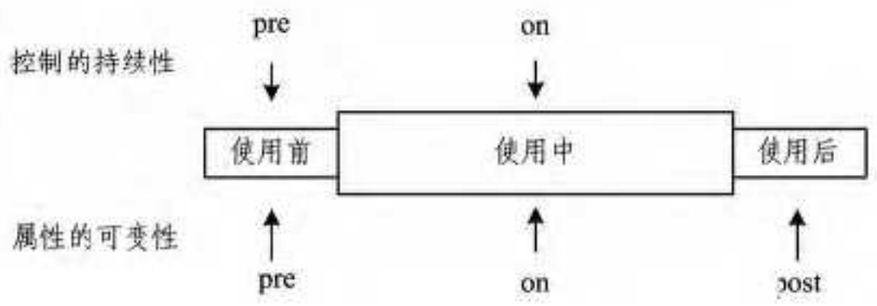

图 2 UCON 模型的控制连续性和属性可变性描述

3 UCON 模型的授权管理

使用中控制是 UCON 模型具有的新特性。UCON 模型提供在使用中进行属性更新和授权的能力，即主体（客体）的属性更新行为可能导致其他系统行为的产生，而其他行为的产生可能带来新的更新，因而每次更新行为不仅影响本次使用过程，还会影响其他的使用过程，甚至导致产生新的行为，这一特征提高了访问控制的灵活度，却也大大增加了 UCON 模型授权管理的复杂性。因而确保更新信息的正确性和真实性就显得极为重要。

UCON 模型的研究是基于“网络中传输的更新信息是可信的”这一假设的基础上。事实上，一方面随着网络日益动态化和分布化，正确操作的确定性降低，属性的新值可能不能及时捕获；另一方面，由于人为或非人为的篡改信息和攻击系统漏洞，都可能造成网络中违反策略的行为的执行。目前，使用中控制方面的研究成果较少，如何规避对于一个违反策略的访问的错误授权，有研究文献提出了使用中更新风险分析法[8]和使用中更新并发控制法[9]。本文尝试从隐私策略可信度的角度，探索一种确保隐私策略可信性的授权管理方法。

4 基于加密方式的授权管理控制模型（AM-UCON）

在云计算这种大规模的开放网络中，UCON 模型在具备明显的访问控制优势的同时，对于其属性的可更新性和控制的可持续性特点来说，使用中的安全授权管理成为一个难点。基于此，本文提出一种基于加密方式的授权管理控制模型——AM-UCON。这个模型的原理是，在认证和监控的基础上，以多方验证的方法来提高属性更新的可信性以及授权的正确性。通过实验表明，该模型方案对应用系统的响应时间和实时表现影响合理。

4.1 模型描述

AM-UCON 模型中包含 5 个主要模块：客户端应用模块、客户端监控模块、服务器端认证模块、服务器端监控模块和服务器端数据模块。图 3 描述了模型 AM-UCON 的组成结构和工作流程。其中，服务器端和客户端均有监视机制，对于服务器端的隐私策略文件的存储，本文采用 GFS（Google File System）[10] 模式，用空间换取安全性的方式提升隐私策略文件的安全性。具体做法是：①将授权和验证功能进行分离，以提高效率；②采用不同节点多个备份的方法，提高服务器端隐私文件的安全性。同时，为提高效率，规定仅在服务器端用于验证的端点隐私策略完整性被破坏，或者客户端传递回来的验证策略与服务器端不一致时，才启动备份数据进行验证和纠错。而对于 UCON 在使用中属性更新所带来的响应的隐私策略改变，则在每次隐私策略更改之时，需要对验证端点和备份端点的数据同时进行更新。最后，为进一步提升系统安全性，降低隐私策略被恶意篡改的风险，本方案中引入加密机制，对客户端和服务器端的隐私策略数据均进行了加解密操作，给系统添加一道屏障，如图 3 所示。

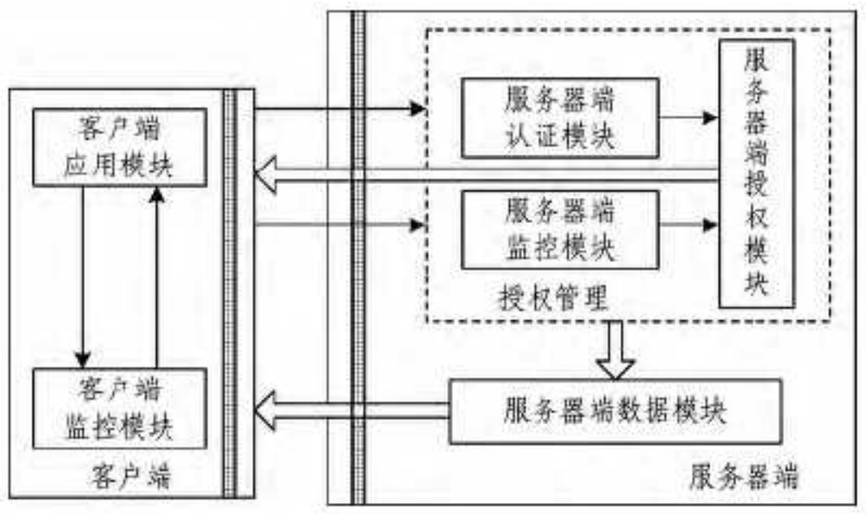

图 3 AM-UCON 模型的结构流程

4.2 模型实现

实验以一个基于云计算的数字对象发布系统为背景。该系统旨在通过服务器端的隐私策略来判定客户端的访问请求，从而确定是否允许该用户的访问以及应给予的访问权限。实验的硬件平台采用若干台主机和虚拟机（其中，一台主机用作服务器，其他主机和虚拟机均作为客户端接入系统）模拟云

环境，进行模型的可行性实验。实验中所涉及的大量用户形成的数据，是通过一台主机或虚拟机上同时模拟多个任务获取的模拟数据。图4和图5描述了服务器端的授权管理实现流程。

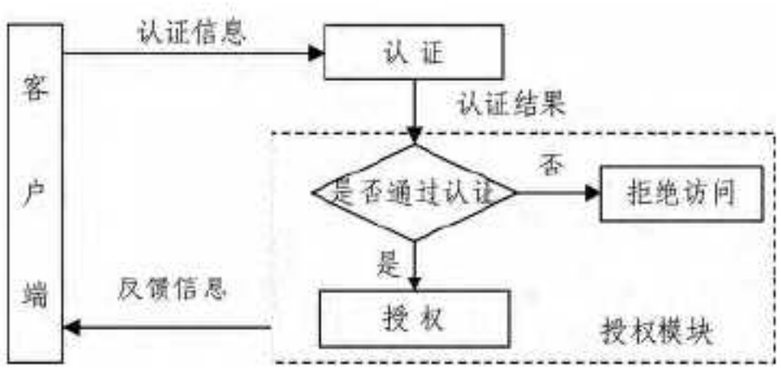

图4 服务器认证模块工作流程

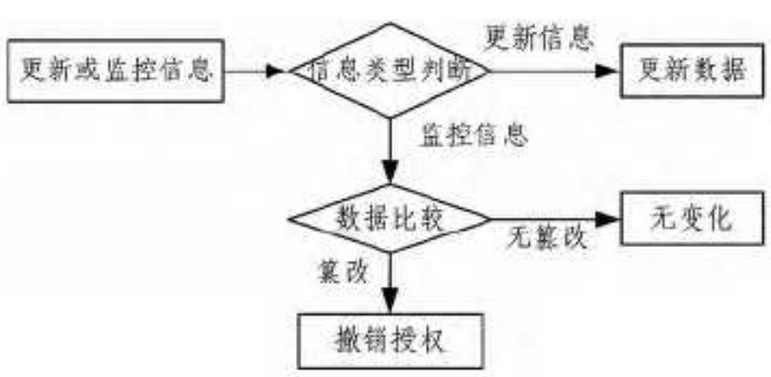

图5 服务器监控模块工作流程

AM-UCON模型方案中，服务器端向客户端发布隐私策略时，对隐私策略进行数字签名。在实验中，我们采取信息摘要的方式[11]，对发布的信息用SHA-1或MD5计算数字摘要信息。通过这样的加密和信息摘要的方式，在一定程度上保证了信息的机密性和完整性。图6是进行信息摘要的部分代码。

```
public String Encrypt(String strSrc,String encName){
  MessageDigest md=null;
  String strDes=null;
  byte[] bt=strSrc.getBytes();
  try{
    if(encName==null||encName.equals("")){
      encName="SHA-1";
    }
    md=MessageDigest.getInstance(encName);
    md.update(bt);
    strDes=bytes2Hex(md.digest()); //to HexString
  }
  catch (NoSuchAlgorithmException e){
    System.out.println("Invalid algorithm.");
    return null;
  }
  return strDes;
}
public String bytes2Hex(byte[]bts){
  String des="";
  String tmp=null;
  for(int i=0;i<bts.length;i++){
    tmp=(Integer.toHexString(bts[i] & 0xFF));
    if(tmp.length()==1){
      des+="0";
    }
    des+=tmp;
  }
  return des;
```

图6 信息摘要的部分代码

表1列出了计算信息摘要所消耗的时长。可以看出，该方法耗时较少，能够适用于对实时性要求较高的云计算应用，进而论证了本文提出的模型方案是可行的。

表1 AM-UCON计算信息摘要消耗时长

加密数据文件大小（字节）	消耗平均时长（毫秒）（300次实验平均）
4k	7.92
3.62M	148.23
13.6M	492.15
22.3M	826.78

结束语 结合云环境的特点，本文分析了UCON访问控制模型的优势，从理论上阐述了UCON模型更适用于云计算环境的观点。研究了UCON模型的授权管理问题，从提高授权的可信度、保护隐私策略信息的角度，提出了一种基于加密方式的授权管理模型（AM-UCON），并最后在模拟云环境的数据发布管理系统中得以实现。下一步，针对UCON模型在使用中的属性更新和授权问题，以及如何在安全的前提下提高系统的扩展性，还有待更深入的研究。

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] 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(S2)：267-270

[3] Ferraiolo D，Cugini J，Kuhn D R. Role Based Access Control (RBAC)：Features and Motivations[C]// Proc. 1995 Computer Security Applications Conference. December 1995：241-248

[4] Sandhu R，Park J. Towards Usage Control Models：Beyond traditional access control[C]// Proceedings of the 7th ACM Symposium on Access Control Models and Technologies. 2002：57-64

[5] 聂丽平. 基于UCON访问控制模型的分析与研究[D]：合肥：合肥工业大学，2006

[6] 崔永泉，洪帆，龙涛，等. 基于使用控制和上下文的动态网络访问控制模型研究[J]. 计算机科学，2008，35(2)：37-41

[7] Yao Dong-mei，Pan Jing-gui. A Method of Solving Geographical Constraints in Cloud Computing with UCON Access Control Model[C]// The 3rd International Conference on Information Science and Engineering. Yangzhou：ICISE，2012：5111-5114

[8] Krautsevich L，Lazouski A，Martineli F，et al. Risk-Aware Usage Decision Making in Highly Dynamic Systems[C]// The Fifth International Conference on Internet Monitoring and Protection. Barcelona：Spain，2010

[9] 李钢，李沛武，胡海霞. 使用控制系统中属性更新的并发控制研究[J]. 南京工程学院学报，2008，27(4)：19-23

[10] Ghemawat S，Gobioff H，Leung S T. The Google File System [C]// Proc. of the 19th ACM Symposium on Operating Systems Principles. New York：ACM Press，2003：29-43

[11] 陈坤定. 消息摘要算法在Java Web系统中的应用[J]. 长春大学学报，2012，22(4)：409-412

[12] Zhu Yan，Hu Hong-xin，Ahn G-J. Towards temporal access control in cloud computing[C]// INFOCOM，Proceedings IEEE. 2012：2576-2580