云计算环境下访问控制关键技术

冯朝胜[1,2,3],秦志光[3],袁 丁[1],卿 昱[2]
(1.四川师范大学计算机科学学院,四川成都 610101;2.中国电子科技集团公司第30研究所,四川成都 610041;
3.电子科技大学计算机科学与工程学院,四川成都 610054)

摘 要: 可控信任域的消失和多租户环境的出现,导致云计算环境下访问控制在诸多关键技术上都面临新的严峻挑战.该文从身份供应、身份认证、访问控制、身份联合和单点登录几个方面介绍了产业界在云访问控制上面临的问题和主要解决方法.从访问控制模型、基于属性的密文访问控制和外包数据的访问控制三个方面评述了学术界在云访问控制上的最新研究成果.基于对已有技术和研究成果的分析,预测了云访问控制研究的未来走向.

关键词: 云计算; 身份管理; 访问控制; 数据服务外包
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2015)02-0312-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.02.017

Key Techniques of Access Control for Cloud Computing

FENG Chao-sheng[1,2,3], QIN Zhi-guang[3], YUAN Ding[1], QING Yu[2]
(1. *School of Computer Science, Sichuan Normal University, Chengdu, Sichuan* 610101, *China*;
2. *The No.30 Institute of China Electronic Technology Corporation, Chengdu, Sichuan* 610041, *China*;
3. *School of Computer Science & Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan* 610054, *China*)

Abstract: The loss of on-board domain and appearance of multi-tenant context bring some new problems and challenges to access control. In this paper, these problems are listed and the reasons are analyzed first. And then, aiming at these problems, the corresponding solutions and techniques are introduced in terms of identity provision, authentication, authorization, identity federation and single sign-on. Next, latest works about access control of cloud computing are reviewed in terms of access control models, attribute based access control of cipher text, and access control of outsourcing data. At last, the trend of study on access control of cloud computing is analyzed and predicted.

Key words: cloud computing; identity management; access control; data service outsourcing

1 引言

访问控制是云计算亟待解决难题[1,2].当用户将数据处理和数据存储外包给云服务提供商时,就意味数据及其处理已脱离了数据所有者的掌控,换句话说,用户数据为外包云服务提供商所控制.这样,防止云服务提供商非法访问数据就成了难题.另外,虚拟化和多租户技术是云计算采用的两种关键技术,也是资源能动态伸缩和充分利用的关键原因.然而,虚拟化技术使不同用户(采用虚拟机进行隔离,针对IaaS模式[3,4])共享着相同的硬件资源,而多租户技术使不同用户(共享一个实例,用户数据一般存放在一张数据表上,采用标签进行隔离,针对SaaS[3,4]模式)共享着相同的软件资源,这种共享形成了多租户环境,它对访问控制提出更高要求,因为访问控制是将用户区分开来和防止用户非法访问的主要手段.访问控制必须确保即使数据都在同一物理主机上,用户也只能访问自己的数据而无法访问其他用户数据.事实上,Google Docs在2009年3月就发生过不同用户之间文档的非授权交互访问问题[5].

访问控制一直是学术界和产业界关注的热点问题,而云计算的访问控制同样引起了广泛关注.该文基于已有的技术和研究,对云环境下访问控制面临的问题进行了分析.

收稿日期:2013-01-31;修回日期:2014-06-22;责任编辑:蓝红杰
基金项目:国家自然科学基金(No.061373163);国家科技重大专项课题(No.2011ZX03002-002-03);国家科技支撑计划课题(No.2014BAH11F01,2014BA11F02);可视化计算与虚拟现实四川省重点实验室课题(No.PJ2012002)

2　云环境下访问控制面临的问题

传统计算模式下,企业信息系统的软硬件设施一般都部署在企业内部.企业内部的计算机、网络、路由器等 IT 设备和设施形成了一个可被企业信息系统管理员完全控制的网络,通常称作“可控信任域”.在这种模式下,由于所有的 IT 资源都置于企业的完全控制之下,所以对于企业而言实现身份管理和访问控制还不是那么困难.然而,一旦企业将部分甚至全部业务置于云端(以下如不特别说明,云都指公有云),“可控信任域”就不复存在.企业信息系统工作在一个更大的域中,这个域至少由企业域和云域组成,如图 1 所示.显然,企业原有的由防火墙、IDS 等组成的“可信边界”无法保护这样的域,原来支撑企业信息系统的“可控信任域”被“不可信域”所替代,企业只能控制部分“不可信域”,对其中存储着其数据的“云域”没有控制权[6].另外,由于云端会根据应用的实时需要动态进行资源供给,网络范围一直会处于动态变化之中,这种动态性使企业和云服务提供商进行访问控制变得困难.云环境下访问控制主要面临以下难题[3,6,7].

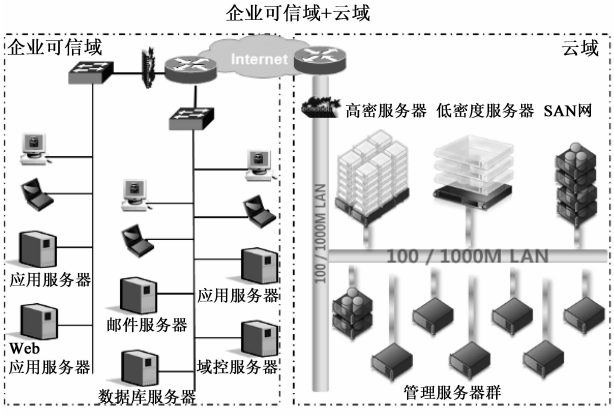

图1　企业可信域与云域

(1)身份供应

传统计算模式下,企业内部用户身份信息是由内部专门的身份供应机构根据人力资源部门提供的人力资源信息来供应和同步的.这个过程由于发生在企业信息系统可信边界之内,所以身份供应较易实现,身份同步较为快速.一旦引入云服务,不同域(至少包括企业可信域和云域)环境中的身份供应成为难题.如果企业域和云域都提供身份供应,身份信息同步是首要难题.如果由云来提供身份信息,隐私保护成为首要难题.如果身份供应依然由企业实现,又会出现跨域认证问题.

对于个人用户,云环境采用的主要身份供应方式是自主供应.在这种模式下,用户的隐私信息如身份标识符、凭证信息等,容易泄露.在云中,特别是是在公有云中——资源为众多用户所共享,隐私是否能得到有效保护是十分重要的问题.

(2)认证

传统信息系统中使用得最多的是“用户名 + 口令”认证方式,尽管该方式属于安全性较低的弱认证方式,但威胁主要来自可信域内部,由于系统工作在可信边界内,所以安全较有保证.然而,这种认证方式的安全性远远无法满足有着泛在接入(在任意时间任何地方以任意终端设备,如个人电脑、手机、*PDA* 等,访问服务)基本特征的云环境的需要,而应代之以更安全的多因子强认证方式,并且对于不同安全级别的服务应采用不同力度的强认证方式.

企业采用云服务后,企业信息系统就至少位于两个域中:一个为企业自身,另一个为云服务提供商.出于隐私保护考虑,企业可能不会将用户基本身份信息传送给云服务提供商.在这种情况下,云计算供应商自身无法认证用户身份,而需要将认证委托给购买相关云服务的企业.在企业使用云服务时,以可信和可管的方式认证用户身份是至关重要的需求.凭证管理、强认证、委托认证和服务间的信任关系管理,都是企业必须解决的认证难题.

(3)访问授权

要进行访问授权,首先要做的就是选择合适的访问控制模型.鉴于云计算自身的特点,可能并不是所有的模型都能应用于云计算环境之中.什么样的访问控制模型适用于云环境? SaaS、PaaS 和 IaaS 云服务提供商分别应选择什么样的访问控制模型? 这些都是亟待解决的问题.如果策略决定点和策略执行点都部署在云端(或云服务提供商处),云端的策略信息和用户基本信息保持与企业相关信息的同步就会成为难题.如果不能实现同步,访问授权就会出现错误.如果将策略决定点部署在企业内部,而将策略执行点部署在云端,就可以避开信息远程同步难题,但另外一个难题随即就会出现:授权与应用分离.实际上,还没有应用真正做到这一点.

(4)身份联合

云环境下,服务访问往往会跨越多个域,每个域都可能都有着自己的身份供应方式、认证方式和访问控制方法.在这种情况下,如果没有一种统一的方式来实现身份管理和访问控制,就会出现系统不兼容问题,同时也使用户访问变得异常复杂.解决这个问题的方式就是身份联合.然而,由于面向云的身份联合标准并没有制定出来,现有的云服务提供商和企业遵循的标准又不尽相同.因此,如何实现身份联合就成了不小的难题.

(5)单点登录

云环境是个多域环境,任何一个包含云应用的企业信息系统至少包括两个域:企业域和云域.在传统模式下,当用户访问企业信息系统时,由于只有一个可为企业完全控制的信任域,企业可以通过像建立统一门户这样的方式来实现域内信息系统的单点登录,即用户只需登录一次就能访问其信息系统中所有的应用和数据.但是在云这样的多域环境中,企业没有能力控制所有的域,因而也就很难通过建立统一的门户来实现单点登录.

3 云访问控制技术

针对云环境下访问控制面临的诸多难题,包括云安全联盟在内的一些组织和包括亚马逊、谷歌、微软等在内的云服务提供商都纷纷提出了自己的解决方案,其中的一些方案已应用于云产品中.下面对云访问控制解决方案和技术进行说明.

3.1 云身份供应

3.1.1 云身份供应方法

服务供应标记语言 SPML(Service Provisioning Markup Language)[8]是云身份供应标准尚未制定出来前云服务提供商普遍遵循的身份供应工业标准.SPML 是由结构化信息标准促进会开发的基于 XML 的身份供应语言和架构,它主要用于合作企业之间实现用户信息、资源信息和服务信息的交换.SaaS 或 PaaS 云服务提供商可以采用两种方式[2]来支持 SPML:一种是向用户提供 SPML 适配器或连接器;另一种是提供 SPML 网关[3,6].

3.1.2 基于 SPML 的身份供应

一旦 SPML 被支持,SaaS 云服务提供商可以实时地向新用户提供身份供应服务[6].新用户的身份信息通过 SAML 令牌传送给云服务提供商,云服务提供商从新用户的 SAML 令牌上提取属性信息,建立 SPML 消息,处理身份供应服务请求.身份供应服务依次将用户身份信息添加到云用户身份信息数据库中.身份供应采用 SPML 协议有利于身份供应的标准化和自动化,能有效克服定制方案的不足.

3.2 云认证

3.2.1 云身份认证方法

云计算的多租户特征决定了其应采用强认证方式[6,7].如果认证由云来提供,认证可以由云服务提供商实施,也可以将认证外包给专门云身份服务 IDaaS[9](ID as a Service)提供商.如果认证由企业提供,要求云服务提供商支持将认证委托.这样,企业就能利用像 SAML 这样的开放标准和现有基础设施实施强认证.SaaS 云和 PaaS 云的认证服务一般都内置在平台中,而 IaaS 云的特点决定了其认证服务主要由企业自己来构建.对于 IaaS 云的管理员,可以通过虚拟专用网 VPN 来认证身份;而对于 IaaS 云普通用户,可以采用虚拟专用网和身份联合两种方式.

3.2.2 S3 的身份认证

S3(Amazon Simple Storage Service)[10]是亚马逊推出的简单存储服务,用户通过亚马逊提供的服务接口可以将任意类型的文件临时或永久地存储在 S3 服务器上.S3 向用户提供了身份认证和访问控制安全机制[11],S3 的认证过程如图 2 所示.为进行身份认证,在新用户注册时,亚马逊分配给每个用户一个 Access Key ID 和一个 Secret Access Key.Access Key ID 是一个 20 位的字符串(由字母和数字组成),Secret Access Key 是一个 40 位的字符串.Access Key ID 用来标识服务的请求者,而 Secret Access Key 则参与身份认证过程,用来验证服务请求的合法性.在认证过程中,认证算法是关键.S3 采用的身份认证算法基于 HMAC-SHA1 数字签名方式.HMAC-SHA1 是一种安全的消息认证协议,该协议利用 hash 函数保证数据的完整性,利用共享密钥和消息认证码保证数据的真实性,它可以有效防止数据在传输过程中被截获和篡改.HMAC-SHA1 消息认证机制的成功在于一个加密的 hash 函数、一个加密的随机密钥和一个安全的密钥交换机制.

3.2.3 基于 OAuth 的跨域身份认证

OAuth[12]是一个支持跨域访问即工作在一个域中的应用访问另外一个域中应用的协议(它正成为工业标准),很适合云应用系统这样的多域环境.OAuth 支持企业将其存储在一个云中的私有资源共享给其他云用户,在共享过程中,不会暴露用户的认证信息.对于应用开发者而言,OAuth 是一种安全的数据发布和交换方法.对于云服务提供商而言,OAuth 提供一种在保证凭证信息安全的情况下访问其它云上数据的方式[9].最近,谷歌发布了包含 OPenID 和 OAuth 协议的混合协议,该协议将授权和认证过程结合来提高可用性,而需要的步骤却更少.谷歌的 GData API 宣布支持 OAuth.

3.3 云访问授权

自主访问控制 DAC(Discretionary Access Control)、强制访问控制 MAC(Mandatory Access Control)和基于角色的访问控制 RABC(Role Based Access Control)是当前信息系统主要采用的访问控制模型.非结构化数据适合采用自主访问控制模型;事务处理服务最好采用基于角色的访问控制模型;如果必须基于资产或信息的种类来实现访问控制,那么最好采用强制访问控制模型.对于云服务提供商提供的 Web 服务,最好采用自主访问控制模型;对于非 Web 服务,采用基于角色的访问控制模型更合适[3,6].

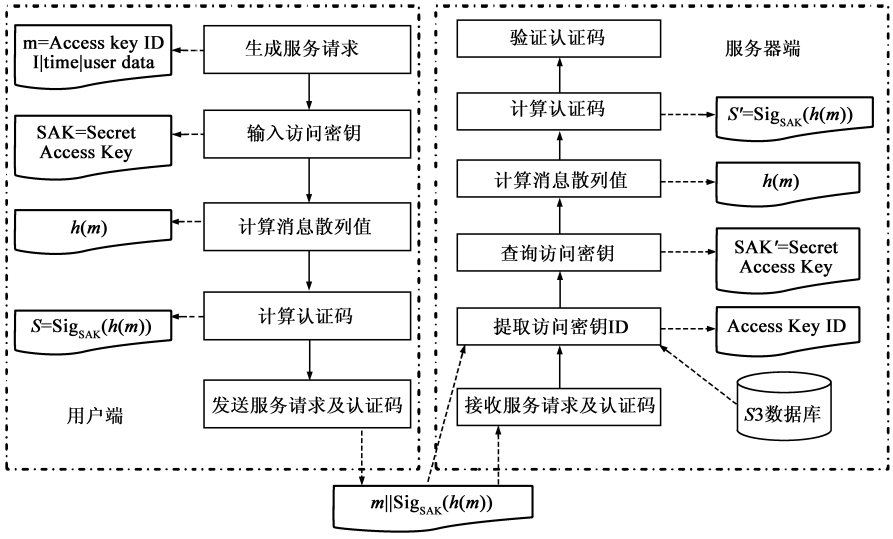

图2　S3认证过程

3.3.1　基于 XACML 的访问授权

已有的集中式授权和分散式授权都基于特定的应用授权模型进行授权,但特定的应用授权模型难以描述访问多个应用的用户权限.因此,需要为不同应用的访问提供标准化的语言、访问授权方法和执行策略来建立一个通用的授权标准.授权基于各种授权策略和规则,策略和规则围绕用户角色和职责制定.可扩展访问控制标记语言 XACML[13](eXtensible Access Control Markup Language)正是这样的标准,它是由 OASIS 批准的通用的基于 XML 的用于策略管理和访问决策的访问控制语言,该语言支持基于 XML 的通用策略语言,主要用于实现资源的访问控制.作为访问控制标准,XACML 不仅给出了策略语言模型,而且还给出了策略管理和访问的环境模型[3,6].XACML 很适合云计算这样的多域和多应用环境.

3.3.2　Windows Azure 访问控制服务

NET 访问控制服务[14]是微软公司云计算平台 Windows Azure 采用的访问控制服务.该服务通过令牌机制和身份标识机制使用声明转换引擎实现了身份联合,依靠现有的支持标准协议的账户存储机制,实现了单点登录、集中授权和访问控制逻辑.开发者不再需要为自己的应用程序创建账户和角色数据库,有效地解决了"身份爆炸"难题.

Windows Azure 采用 SAML[15](Security Assertion Markup Language)令牌传输身份信息.一个 SAML 令牌包括多个声明,每个声明中都可能包含着用户的部分身份信息,如用户名、身份角色、电子邮件地址,等等.令牌的创建是由安全令牌服务(Security Token Service,STS)负责,STS 在创建令牌时还会根据用户身份信息核定用户可以访问的信息资源即进行授权.在 Windows Azure 中,有两种 STS,一种是客户 STS,部署在企业内部,主要负责请求令牌的创建;另外一个为访问控制服务端的 STS.当用户提交的令牌声明和应用程序的要求不匹配时,使用事先定义好的规则,STS 能够创建一个新的应用程序需要的令牌..NET 访问控制服务的运行机制如图 3 所示.

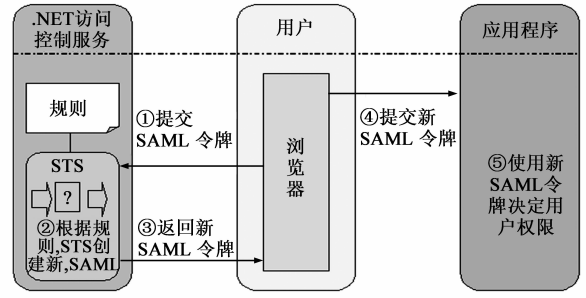

图3　NET访问控制服务

3.4　云身份联合

3.4.1　云身份联合方法

云计算环境下实现身份联合有两种方式:在企业内部建立身份供应机构 IdP[16](Identity Provider);在云端由专门的提供商统一提供身份管理服务即 IDaaS.构建云身份联合模型应遵循如下步骤[3,6]:① 建立一个身份管理权威机构;② 确定用户基本属性;③ 设立身份供应机构.该机构支持单点登录服务且能为云服务提供商所访问.SAML 是事实上的身份联合标准,它已为 Google Apps、Salesforce.com 等云所支持.

3.4.2　基于 IdP 的身份联合

基于 IdP 的身份联合方式带来的最大好处是保证了身份联盟与企业内部在策略、处理方法和访问管理框架上的一致性.企业通过改造提升现有身份管理系统就能实现对身份联合的支持,而无需推翻原有系统.

这种方式还使企业无需关注身份供应机构自身是否可信安全.该方式的不足是:在现有身份管理系统不支持身份联合的情况下,管理外部用户身份的效率会很低.

在基于 IdP 的身份联合方式中,云服务将认证委托给企业自己的身份提供机构.如果一些云服务提供商将认证委托给同一个身份供应机构,对于企业而言,这些云服务商就组成一个可信云环,企业在可信云环内实现身份联合[3,6].

3.4.3 基于 IDaaS 的身份联合

企业在几乎不改变原有信息系统结构的情况下就能支持这种模式.一旦企业身份目录和云端的身份目录建立起同步,用户就能使用账户、口令和认证策略访问云服务.该方式的不足是:企业不知道服务细节;如果身份属性没有被正确定义,无法与身份正确关联,那身份属性管理就可能变得复杂.

在基于 IDaaS 的身份联合模式中,云服务提供商将身份管理委托给专门的云身份管理服务提供商.当要通过身份联合访问云服务时,企业既需要使用自己的身份管理机构来管理身份信息,同时又需要将身份信息传送到云身份管理服务提供商处并时刻保持两者信息的同步[3,6].从根本上讲,IDaaS 属于软件即服务模型.

3.5 云单点登录

单点登录 SSO(Single Sign On)是指用户只需在网络中进行一次身份认证,便可以访问其授权的所有网络资源,而不再需要其它的身份认证过程,简单讲,就是一次登录,多处访问.实现单点登录的前提是相关应用系统或可信域已经利用身份联合技术构建了身份联盟.单点登录之所以得以实现,是因为安全凭证信息能在安全联盟中快速传递或共享.单点登录的现有标准是 SAML,现有的云服务提供商也多基于该标准来实现单点登录.基于 SAML 的单点登录方式访问谷歌 Web 应用过程如图 4 所示[6].

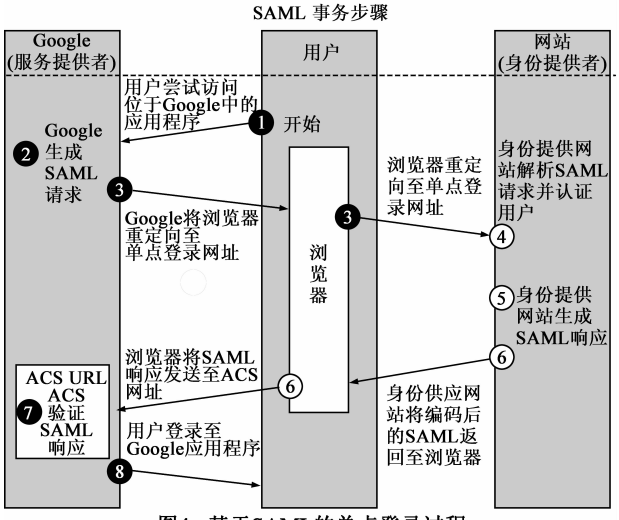

图4 基于SAML的单点登录过程

4 云访问控制研究

云访问控制涉及到网络访问控制和数据访问控制[16],学术界更关注数据访问控制.

4.1 云访问控制模型

文献[17]提出了基于 RBAC 的面向云环境的自适应访问控制模型.在该模型中,当服务请求成本比预算限制要低时角色保持不变,但如果高于或者等于预算,角色就会转换为更高的版本.这种基于角色的变换模型可以解决云计算环境变量的动态变化问题,但该模型是一种粗粒度的访问控制模型,针对的是明文数据.文献[18]提出了 GTRBAC 模型,该模型对 TRBAC 模型[19]进行了改进和扩展,旨在解决 RBAC 模型中用户有可能只在一个特定的时间段内才能指派给一个角色、一个角色可能只能临时依赖于另一个特定的角色的问题.文献[20]针对有关混杂角色层次中的权限查询等问题提出了唯一激活集(UAS,uniquely activable set)以及求解算法.UAS 能在既有角色继承,又含有角色激活关系的混杂角色层次中,针对一定的权限,给出相应的唯一角色集合.上述访问控制模型均不能区分普通用户和资源拥有者管理角色,而且缺乏处理云计算环境中海量用户及高并发访问的能力.针对这些问题,文献[21]基于传统的 RBAC 模型提出了一种面向云计算环境中的访问控制模型 CARBAC.在该模型中,角色分为用户角色和数据所有者角色,二者都具有相应的继承和激活的角色层次关系.该模型的最大问题是要求数据所有者具有很强的计算能力并时刻在线以维护角色的层次关系和进行角色指派,没有发挥云强大的计算优势.另外,该模型针对的是明文数据.文献[22]提出了基于行为的访问控制模型.该模型除利用 BLP 模型保证数据的保密性和利用 Biba 模型保证数据的完整性外,还分别在权限和行为两个层次上进行访问控制.该模型同 BLP 模型和 Biba 模型一样都属于强制访问控制模型,强制访问控制会大大降低云资源的可用性.

4.2 基于属性的云密文访问控制

2006 年,文献[23]首先提出了基于属性的加密方法 ABE(Attribute-based Encryption),其基本思想是:密文与私钥分别与一组属性关联,当用户的私钥属性与密文属性相互匹配到达一个门限值时,该用户才能解密密文.文献[24]在基于模糊身份加密方案的基础上提出了密钥策略的基于属性的加密方案 KP-ABE.该方案使用访问控制结构的加密密钥.2007 年,Bethencourt J 等[25]提出了一种密文策略的基于属性的访问控制方法 CP-ABE,该方法使用访问控制结构加密明文.在用户访

问权限被撤销时,KP-ABE 和 CP-ABE 算法要求数据所有者对数据重新加密.这两种方案的访问控制结构都基于秘密共享方法生成.由于 ABE 算法的效率较低,重加密代价很大.如何有效地支持动态策略,已成为 ABE 面临的主要难题.为解决以上问题,文献[26]提出了一种面向云存储环境的密钥策略的基于属性的访问控制方案.在该方案中,采用代理重加密方法使得密钥密文的重加密由云服务器来完成而数据又不会泄露,懒惰加密方法则提高了重加密的效率.文献[27]提出一种混合访问控制方案.将用户域分成私人域和公共域.私人域采用 CP-ABE 进行访问控制,而公共域则采用分级的 CP-ABE 进行访问控制.以上方案共同的优点是可以进行细粒度的访问控制,共同的不足是要求用户对文件或数据加密,加重客户端的负担,没有充分利用云端超强的计算能力.

4.3　外包数据的访问控制

由于云数据属于外包数据,因此已有的外包数据访问控制方案对云数据的访问控制具有借鉴意义.下面介绍一些典型的外包数据访问控制方案.

文献[28]提出面向公有云的访问控制框架.数据所有者在本地加密数据后将其上传到云端.用户要访问数据,须向数据所有者发出授权访问请求.如批准访问,数据所有者将访问令牌和访问凭据发给请求用户.用户凭借令牌从存储数据的云端提取密文数据,然后利用访问凭据解密数据.该框架最大的问题是加密/解密都由运算能力较弱的用户端机器完成,没有充分发挥云的优势.数据更新、权限撤销等问题如何解决也没提及.

文献[29]提出一种面向公有云的外包数据访问控制方案.该方案的访问控制思想与文献[28]基本相似:数据所有者将数据加密后存放于云端;用户要访问数据,须向数据所有者请求授权证书(相当于令牌)和解密密钥(相当于访问凭据).但不同的是文献[28]提出的框架是较为抽象的模型,而文献[29]的方案很具体.在该方案中,数据加密是以数据块为单位而并非是文件,且不同的数据块采用不同密钥进行加密;加密密钥连接成密钥树以减少用户管理的密钥数量.该方案支持数据的插入和更新以及用户权限的撤销操作.不足是效率不高,缺乏海量用户数据处理能力和高并发访问能力.

文献[30]提出一种面向云计算环境的基于 XML 的分布式访问控制架构.该架构采用 XML 以实现访问控制策略的分发,采用基于角色的访问控制模型 RBAC 以实现简化管理和支持系统规模的扩展.该架构的明显不足是很多访问控制的关键问题如身份认证、密钥管理、访问控制策略的冲突与解除等,并没有得到有效解决.

5　云访问控制未来研究趋势

云计算环境面临大量访问控制难题,部分问题已经被解决,但多数问题特别是细粒度的访问控制和密文的访问控制问题并没有得到有效解决.云计算环境下访问控制面临的主要需求、挑战及对策[3,6]如表 1 所示.

从已有云访问控制技术和研究看,云访问控制的未来研究将关注以下问题:

(1)标准化　作为众多技术的"集中云",云计算本身几乎还没有任何技术标准被制定 出来.在这种情况下,云服务提供商一般都采用传统信息系统的标准作为参考标准来实现相关技术.由于不同企业或云服务提供商遵循的标准往往不同,企业应用与云应用之间、不同云服务提供商的云应用之间,无法相互融合

(2)密文的访问控制　在已有的云中,所采用的访问控制技术几乎都针对的是明文.事实上,针对密文的访问控制同样重要,因为存储在云中的用户隐私数据和敏感数据通常是以密文形式存在的.现有的云密文访问控制研究还处于理论研究阶段,面临的一大问题是因用户权限撤销导致的密文数据重加密问题.

(3)细粒度的访问控制　已有的云访问控制方式是基于用户身份的粗粒度的访问控制,这种粗粒度给本来就是多租户环境的云环境带来安全隐患.因此,研究 *ABE* 这样的细粒度访问控制方式非常重要和必要.

(4)访问控制的服务化　在用户数量不太多的情况下,由云应用服务提供商和企业一起来实现访问控制是可行的.但随着用户规模的大幅度增加,云应用服务提供商和企业就会花大量时间来确保访问控制,影响应用服务效率.该问题的解决办法是实现访问控制的服务化,将访问控制交由专门而又专业的云访问控制服务提供商来实施.

(5)跨云授权　为实现一个云服务,系统可能需要访问多个云中的应用和数据.由于同一个用户在不同云中有着不同的权限,并且授权难以像认证模块那样从应用中分离出来,因而实现跨云授权十分困难.

(6)身份供应的自动化　当前,云服务提供商还主要采用人工方式实现身份供应.然而,当用户数量达到一定规模后,人工方式就必须为自动化方式所替代.

表 1 云访问控制面临的问题与对策

相关技术	主要需求	面临的挑战	解决方案
身份供应	①快速支持和同步 ②身份的自主供应和自动撤销 ③保护隐私	①缺乏标准支持 ②现有的解决方案为专有解决方案 ③缺乏身份供应 API	①基于 SPML 标准修改或扩充自己的身份信息数据库 ②SaaS 或 PaaS 云向用户提供 SPML 适配器(包括连接器)或 SPML 网关 ③IaaS 云提供 SPML 的 API
身份认证	①采用强认证方式 ②认证级别的动态调整 ③支持认证委托	①凭证管理 ②认证兼容	①基于 SAML 进行强认证 ②SaaS 云和 PaaS 云将认证服务内置于平台中 ③IaaS 云认证服务由企业自己来构建
访问授权	①支持多租户环境 ②远程策略支持 ③支持多种用户	①访问控制模型的选择 ②用户信息和策略的同步 ③授权与应用的分离	①面向 Web 方式的自主访问控制模型,面向非 Web 方式的基于角色的访问控制模型或基于属性的访问控制模型 ②策略决定点和执行点分离 ③策略格式采用 XACML 标准
身份联合	①建立标准 ②支持联合网关 ③支持单点登录	①建立标准 ②在云身份联合标准建立前,支持多种现有标准	①采用 SAML 标准 ②基于企业自己的身份供应机构实现身份联合 ③基于专门的云身份服务提供商实现身份联合

6 结束语

“可信控制域”的消失和多租户环境的出现,向云访问控制提出了新的挑战,其必须能将同一主机上的不同用户数据隔离开来,防止用户访问同一主机上(IaaS 模式)或同一进程(SaaS 模式)上其它用户的数据.该文首先列举了云计算在访问控制上面临的主要问题,分析了云计算存在访问控制问题的根本原因.从身份供应、身份认证、访问控制、身份联合和单点登录几个方面介绍了产业界在云访问控制方面采用的主要解决方法和技术.从访问控制模型、基于属性的密文访问控制和外包数据的访问控制三个方面评述了学术界在云访问控制上的最新研究成果.基于对已有技术和研究成果的分析,预测了云计算环境下访问控制研究的未来发展趋势.

参考文献

[1] Ren K, Wang C, Wang Q. Security challenges for the public cloud[J]. IEEE Internet Computing, 2012, 16 (1): 69 – 73.

[2] Takabi H, Joshi J B D, Ahn G. Security and privacy challenges in cloud computing environments [J]. Security & Privacy, IEEE, 2010, 8(6): 24 – 31.

[3] Ronald L, Russell D. Cloud Security: A Comprehensive Guide to Secure Cloud Computing[M]. Wiley Publishing, Inc., 2010.

[4] 罗军舟,金嘉晖,宋爱波,等.云计算:体系架构与关键技术[J].通信学报,2011,32(7):3 – 21.
Luo Junzhou, Jing Jiahui, Song Aibo, et al. Cloud computing: architecture and key technologies[J]. Journal on Communications, 2011, 32(7): 3 – 21. (in Chinese)

[5] IT 专家网.盘点 2011 年各月影响云计算发展的大事件[EB/OL]. http://www.ctocio.com.cn/cloud/261/12232761-10.shtml, 2012.

[6] Tim M, Subra K, Shahed L. Cloud Security and Privacy[M]. O'Reilly Media, Inc, 2009.

[7] Cloud security alliance. Guidance for identity & access management V2.1[EB/OL]. http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf, 2012.

[8] OASIS. Service provisioning markup language (SPML)[EB/OL]. http://www.oasis-open.org/committees/provision/, 2012.

[9] Slidershare. net. Identity-as-a-service-presentation[EB/OL]. http://www.slideshare.net/prabathsiriwardena/identity-as-a-service-presentation, 2012.

[10] Amazon. Amazon simple storage service[EB/OL]. http://awsdocs.s3.amazonaws.com/S3/latest/s3-dg.pdf, 2012.

[11] 刘鹏.云计算[M].北京:电子工业出版社,2011.

[12] IETF. The OAuth 1.0 Protocol[EB/OL]. http://tools.ietf.org/html/rfc5849, 2012.

[13] OASIS. OASIS eXtensible access control markup language (XACML) TC[EB/OL]. http://www.oasis-open.org/committees/tc-home.php? wg-abbrev = xacml, 2012.

[14] Microsoft. Windows azure[EB/OL]. http://social.technet.microsoft.com/, 2012.

[15] OASIS. Security assertion markup language (SAML)[EB/OL]. http:// www.oasis-open.org/committees/.../docs/cs-sstc-core – 00.doc, 2012.

[16] 俞能海,郝卓,徐甲甲,等.云安全研究进展综述[J].电子学报,2012,41(2):371-381.
Yu Nenghai, Hao Zhuo, Xu Jiajia, et al. Review of cloud computing security[J]. Acta Electronica Sinica, 2012, 41(2): 371 – 381. (in Chinese)

[17] Jung Y, Chung M. Adaptive security management model in the cloud computing environment[A]. Proceedings of the 12th International Conference on Advanced Communication Technology[C]. Washington DC: IEEE Press, 2010. 1664 – 1669.

[18] Chandran S M, Joshi J B D. Towards administration of a hybrid role hierarchy[A]. Proceedings of the 2005 International Conference on Information Reuse and Integration[C]. Las Vegas: IEEE Press, 2005. 500 – 505.

[19] Bertino E, Bonatti P A, Ferrari E. TRBAC: a temporal role-based access control model[J]. ACM Transactions on Information and Systems Security, 2001, 4(3): 191 – 223.

[20] Du S, Joshi J B D. Supporting authorization query and inter-domain role mapping in presence of hybrid role hierarchy [A]. Proceedings of the 2006 ACM Symposium on Access Control Models and Technologies [C]. Lake Tahoe: ACM Press, 2006. 228 – 236.

[21] 杨柳,唐卓,李仁发,等.云计算环境中基于用户访问需求的角色查找算法[J].通信学报,2011,32(7):169 – 175.
Yang Liu, Tang Zhuo, Li Renfa, et al. Roles query algorithm in cloud computing environment based on user require[J]. Journal on Communications, 2011, 32(7): 169 – 175. (in Chinese)

[22] 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,2013,33(3):59 – 66. (in Chinese)
Lin Guoyuan, He Shan, Huang Hao, et al. Access control security model based on behavior in cloud computing environment[J]. Journal on Communications, 2013, 33(3): 59 – 66. (in Chinese)

[23] Sahai A, Waters B. Fuzzy identity-based encryption[A]. Proceedings of Eurocrypt 2005[C]. Berlin, 2005. 457 – 473.

[24] Goyal V, Pandey, O, Sahai A, et al. Attribute based encryption for fine-grained access control of encryption security data [A]. Proceedings of the 2006 ACM conference on Computer and Communications Security[C]. Alexandria, Virginia, USA: ACM Press, 2006. 89 – 98.

[25] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[A]. Proceedings of the 2007 IEEE Symposium on Security and Privacy [C]. Berkeley: IEEE Press, 2007. 321 – 334.

[26] Yu S, Wang C, Ren K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[A]. Proceedings of IEEE INFORCOM 2010[C]. San Diego, CA: IEEE Press, 2010. 1 – 9.

[27] 陈丹伟,邵菊,樊晓唯,等.基于 MAH-ABE 的云计算隐私保护访问控制[J].电子学报,2014,42(4):821 – 827.
Chen Danwei, Shao Ju, Fan Xiaowei, et al. MAH-ABE based privacy access control in cloud computing[J]. Acta Electronica Sinica, 2014, 42(4): 821 – 827. (in Chinese)

[28] Kamara S, ? Lauter K. Cryptographic cloud storage[A]. Proceedings of the 14th international conference on Financial cryptography and data security[C]. Berlin, Germany, 2010. 136 – 149.

[29] Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data[A]. Proceedings of the ACM Workshop on Cloud Computing Security[C]. Chicago, USA, 2009. 55 – 66.

[30] Abdulrahman A A, Muhammad I S, Saleh B, et al. A distributed access control architecture for cloud computing[J]. IEEE Software, 2012, 29(2): 36 – 44.

作者简介

冯朝胜　男,1971 年生于四川广元,博士后,教授,硕士生导师,中国计算机协会高级会员.2010 年获得电子科技大学信息与通信工程博士学位.研究方向为云计算安全.
E-mail: csfenggy@126.com

秦志光　男,1956 年生于四川荣昌,博士,电子科技大学计算机科学与工程学院教授、博士生导师,IEEE 高级会员.研究方向为密码学、网络与信息安全.

袁　丁　男,1967 年生于四川宜宾,博士,四川师范大学计算机科学学院教授,硕士生导师.2003 年获得西南交通大学工学博士学位.研究方向为网络与信息安全.

卿　昱　女,1970 出生于四川,中国电子科技集团公司第三十研究所研究员,硕士生导师.研究方向为网络与信息安全.