软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(5):1129−1150 [doi: 10.13328/j.cnki.jos.004820]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

云计算访问控制技术研究综述*

王于丁, 杨家海, 徐 聪, 凌 晓, 杨 洋

(清华大学 网络科学与网络空间研究院,北京 100084)

通讯作者: 杨家海, E-mail: yang@cernet.edu.cn

摘 要: 随着云计算规模化和集约化的发展,云安全问题成为云计算领域亟待突破的重要问题.访问控制技术是安全问题的重中之重,其任务是通过限制用户对数据信息的访问能力及范围,保证信息资源不被非法使用和访问.主要对目前云计算环境下的访问控制问题进行研究,首先介绍访问控制理论;然后分析了云计算环境下的访问控制技术体系框架,重点从云计算访问控制模型、基于 ABE(attribute-based encryption)密码体制的云计算访问控制、云中多租户及虚拟化访问控制这 3 个方面对云计算环境下的访问控制问题进行综述,并且调研了工业界云服务提供商和开源云平台的访问控制机制;最后对未来的研究趋势进行了展望.

关键词: 云计算;云安全;访问控制;访问控制策略;访问控制模型;ABE(attribute-based encryption)

中图法分类号: TP309

中文引用格式: 王于丁,杨家海,徐聪,凌晓,杨洋.云计算访问控制技术研究综述.软件学报,2015,26(5):1129−1150. http://www.jos.org.cn/1000-9825/4820.htm

英文引用格式: Wang YD, Yang JH, Xu C, Ling X, Yang Y. Survey on access control technologies for cloud computing. Ruan Jian Xue Bao/Journal of Software, 2015,26(5):1129−1150 (in Chinese). http://www.jos.org.cn/1000-9825/4820.htm

Survey on Access Control Technologies for Cloud Computing

WANG Yu-Ding, YANG Jia-Hai, XU Cong, LING Xiao, YANG Yang

(Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China)

Abstract: With the intensive and large scale development of cloud computing, security becomes one of the most important problems. As an important part of security domain, access control technique is used to limit users' capability and scope to access data and ensure the information resources not to be used and accessed illegally. This paper focuses on the state-of-the-art research of access control technology in cloud computing environment. First, it briefly introduces access control theory, and discusses the access control framework in cloud computing environment. Then, it thoroughly surveys the access control problems in cloud computing environment from three aspects including cloud access control model, cloud access control based on ABE (attribute-based encryption) cryptosystem, and multi-tenant and virtualization access control in cloud. In addition, it probes the best current practices of access control technologies within the major cloud service providers and open source cloud platforms. Finally, it summarizes the problems in the current research and prospects the development of future research.

Key words: cloud computing; cloud security; access control; access control policy; access control model; ABE (attribute-based encryption)

随着云计算的发展,云安全成为越来越关键的问题.在云计算环境中,用户对放置在云服务器中的数据和计算失去控制,对于数据是否受到保护、计算任务是否被正确执行都不能确定,因此需要设计相应的安全机制和体系结构来保护用户数据的机密性、完整性、可用性[1,2].

* 基金项目: 国家重点基础研究发展计划(973)(2012CB315806); 国家自然科学基金(61170211); 教育部高等学校博士学科点专项科研基金(20110002110056, 20130002110058); 教育部-中移动科研基金(MCM20123041)

收稿时间: 2014-10-03; 修改时间: 2014-12-08; 定稿时间: 2015-01-21

2011年11月14日,对云安全研究最为活跃的组织云安全联盟(cloud security alliance,简称CSA)[3]发布了最新版的云计算服务安全实践手册《云计算安全指南(v3.0)》,该指南总结了云计算的技术架构模型、安全控制模型以及相关合规模型之间的映射关系,确定了云计算安全的 14 个焦点领域,对每个领域给出了具体建议,分别是云计算体系结构、政府和企业风险管理、法律问题、合规和审计、信息管理与数据安全、互操作性与可移植性、传统安全影响(业务连续性、灾难恢复)、数据中心运行、事故响应、应用安全、加密和密钥管理、身份授权与访问控制、虚拟化、安全即服务(SecaaS)等.

当前,云安全问题的重要性呈现逐步上升趋势,已成为制约其发展的重要因素,各大云服务提供商的安全问题屡见不鲜:2009 年 3 月,Google 发生大批用户文件外泄事件;2010 年底,微软的 Hotmail 出现了数据丢失现象,导致数万个邮箱账户被清空;2011 年 3 月,谷歌邮箱再次爆发大规模的用户数据泄漏事件,大约有 15 万 Gmail 用户发现自己的所有邮件和聊天记录被删除;2012 年,亚马逊北弗吉尼亚数据中心服务多次(4 月、6 月、10 月、12 月)宕机,导致托管的大量网站无法访问,相关企业营业收入受到很大的影响;2013 年 2 月,微软云服务两次大规模中断,包括 Windows Azure 云存储在内的很多服务都发生了故障,时间长达 10 多个小时;2014 年 9 月,詹妮弗·劳伦斯等好莱坞明星裸照泄露于网上,经证实,是黑客攻击了多个 iCloud 账号所致;再加上上半年曝光的 ios 后门事件,让苹果云安全再次受到质疑.因此,要让企业和组织大规模应用云计算技术与平台,放心地将自己的数据交付于云服务提供商管理,就必须全面地分析并着手解决云计算所面临的各种安全问题.从重大安全事件可以看出:数据安全是云安全的核心,对数据资源的访问控制成为云安全问题的重中之重.

访问控制的目的是通过限制用户对数据信息的访问能力及范围,保证信息资源不被非法使用和访问.传统计算模式下的访问控制技术基本上能够有效地对信息资源进行保护,防止非法访问.但是到了云计算时代,计算模式和存储模式都发生了很多变化,主要体现在以下 5 个方面:(1) 云计算环境中用户无法控制资源;(2) 用户和云平台之间缺乏信任;(3) 迁移技术可能导致数据要变更安全域;(4) 多租户技术使得访问主体要重新界定;(5) 虚拟化技术会让数据在同一物理设备上遭到窃取.所以,云计算给访问控制研究提出了新的挑战:如何发展传统的访问控制技术来解决新型的云计算安全问题.面对这个挑战,学术界许多学者已经展开了云计算环境下的访问控制技术的研究,主要研究点集中在云计算环境下访问控制模型、基于加密机制的访问控制、虚拟机访问控制等方面;各大云服务提供商在构建云平台和提供云服务的过程中也对现有的访问控制技术进行了尝试和实践.本文希望从学术界和工业界两个方面对目前云计算环境下的访问控制技术的研究和实践进行系统的综述和梳理,希望能给该领域的研究者一些启示,并对今后的研究方向做一个展望和探讨.

本文首先回顾访问控制理论的发展历史、经典模型和语言描述;然后分析云计算环境下的访问控制技术体系框架;接着对云计算环境下的访问控制问题从云计算访问控制模型、基于 ABE(attribute-based encryption)密码体制的云计算访问控制、云中多租户及虚拟化访问控制这 3 个方面进行综述,并对云服务提供商的访问控制机制进行调研;最后,对未来研究趋势进行展望.

1 访问控制原理概述

1.1 传统的访问控制技术

访问控制技术起源于 20 世纪 70 年代,当时是为了满足管理大型主机系统上共享数据授权访问的需要.所谓访问控制,就是在鉴别用户的合法身份后,通过某种途径显式地准许或限制用户对数据信息的访问能力及范围,从而控制对关键资源的访问,防止非法用户的侵入或者合法用户的不慎操作造成破坏[4].访问控制有很重要的作用:(1) 防止非法的用户访问受保护的系统信息资源;(2) 允许合法用户访问受保护的系统信息资源;(3) 防止合法的用户对受保护的系统信息资源进行非授权的访问.但随着计算机技术和应用的发展,特别是网络应用的发展,这一技术的思想和方法迅速应用于信息系统的各个领域.

Lampson[5]首先提出了访问控制的形式化和机制描述,引入了主体、客体和访问矩阵的概念,在随后 40 多年的发展过程中,先后出现了多种重要的访问控制技术,见表 1.访问控制技术作为实现安全操作系统的核心技术,是系统安全的一个解决方案,是保证信息机密性和完整性的关键技术,对访问控制的研究已成为计算机科学

的研究热点之一.随着网络和计算技术的不断发展,访问控制模型出现了许多以 RBAC 为基础的扩展模型,访问控制的应用也扩展到更多的领域,比较典型的有操作系统、数据库、无线移动网络、网格计算以及云计算等等.

Table 1 Development of access control

表 1 访问控制技术发展

名称	代表模型	作用
自主访问控制	HRU模型	主体对客体进行管理,由主体自己决定是否将客体访问权或部分访问权授予其他主体,这种控制方式是自主的.
强制访问控制	Bell-LaPadula (BLP)模型[6]	着重保护系统的机密性,遵循两个基本规则:“不上读”和“不下写”,以此实现强制存取控制,防止具有高安全级别的信息流入低安全级别的客体,主要应用于军事系统中.
基于角色的访问控制(role-based access control,简称RBAC)[7,8]	RBAC96模型[9],RBAC2000模型[10]	权限与角色相关联,用户通过成为适当角色的成员而得到这些角色的权限.

1.2 RBAC96访问控制模型

基于角色的访问控制模型表述了用户、角色和权限之间的复杂关系,解决了在传统的访问控制中主体始终是和特定的实体捆绑的不灵活问题,实现了主体的灵活授权,是最经典的访问控制模型.RBAC96 是 RBAC 模型家族的基础,之后的所有模型都是在 RBAC96 基础上发展的.RBAC96 包括了 4 种基于角色的访问控制模型,图 1 所示是它们之间的相互关系.

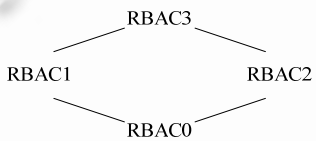

Fig.1 Relationship of RBAC96 model

图 1 RBAC96 模型之间的关系

RBAC0 是基本模型,由 4 个基本要素构成,即,用户(U)、角色(R)、会话(S)和授权(P).图 2 表示在一个信息系统中,定义并存在着多个用户和多个角色,同时对每个角色设置了多个权限关系,称为权限的赋予(PA).

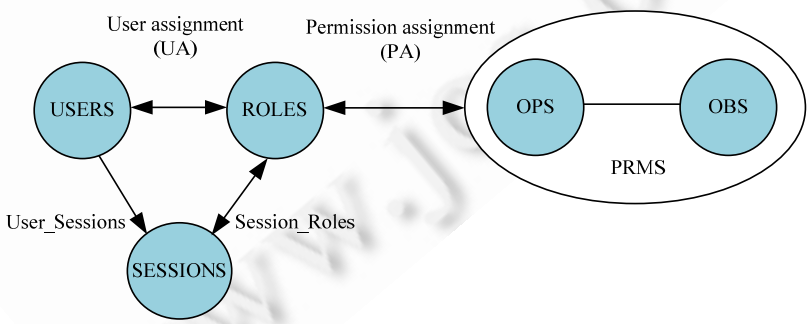

Fig.2 RBAC0 model

图 2 RBAC0 模型

在 RBAC 模型中,授权就是将这些客体的存取访问的权限在可靠的控制下连带角色所需要的操作一起提供给那些角色所代表的用户.通过授权的管理机制,可以给予一个角色以多个权限,而一个权限也可以赋予多个角色.RBAC1 为角色分级模型,在角色域中加入了角色的继承;RBAC2 为角色限制模型,加入了约束条件;RBAC3 为统一模型,是 RBAC1 模型和 RBAC2 模型的整合.RBAC 经过了多年的发展,形成了一套理论体系,其优点和缺点也很明显地显现出来.在近几年访问控制技术的发展中,研究人员在 RBAC 基础上提出了许多扩

展模型,比较常见的有基于任务的访问控制模型、基于时态模型的云计算访问控制、基于属性模型的云计算访问控制等.这些模型能够从不同层面解决系统中访问控制的问题,保证了信息访问的合法性、安全性以及可控性.而且随着云计算的发展,学者们将这些扩展的访问控制模型引用到了云计算的环境里.关于这些扩展模型的介绍和在云计算环境下的应用详见第 3.1 节.

1.3 访问控制语言描述

在访问控制技术的发展和工程实践中,出现了许多语言对高效的用户访问和授权管理和流程进行描述,这些语言作为访问控制理论和工程实践之间的桥梁起着至关重要的作用,也是后人研究访问控制技术的主要工具.目前主要有以下 3 种语言可以对访问控制进行描述,其作用各不相同:

(1) 安全断言标记语言(security assertion markup language,简称 SAML)[11]是一个基于 XML 的标准,用于在不同的安全域之间交换认证和授权数据.SAML 标准定义了身份提供者和服务提供者进行以下工作:1) 认证申明,表明用户是否已经认证,通常用于单点登录;2) 属性申明,表明某个 Subject 的属性;3) 授权申明,表明某个资源的权限.

(2) 服务供应标记语言(services provisioning markup language,简称 SPML)[12]是一个基于 XML 的标准,主要用于创建用户帐号的服务请求和处理与用户帐号服务管理相关的服务请求.其主要目的有两个:一是自动化 IT 配置任务,通过标准化配置工作,使其更容易封装配置系统的安全和审计需求;二是实现不同配置系统间的互操作性,可以通过公开标准的 SPM 接口来实现.

(3) 可扩展访问控制标记语言(extensible access control markup language,简称 XACML)[13]是一种基于 XML 的策略语言和访问控制决策请求/响应的语言,协议支持参数化的策略描述,可对 Web 服务进行有效的访问控制.协议主要定义了一种表示授权规则和策略的标准格式,还定义了一种评估规则和策略,以做出授权决策的标准方法.XACML 提供了处理复杂策略集合规则的功能,补充了 SAML 的不足,很适合应用于大型云计算平台的访问控制中,对于实现跨多个信任域联合访问控制起着重要作用.目前,XACML2013 年发布了 3.0 版.

2 云计算环境下访问控制突出问题与技术手段

纵观云计算的服务体系,IaaS,PaaS 和 SaaS 都需要通过访问控制技术来保护相关信息资源,可以说,访问控制是贯穿于各层之间的一种安全技术.由于云计算的特殊性,云环境下的访问控制技术较之传统的访问控制技术更为关键,用户要使用云存储和计算服务,必须要经过云服务商 CSP 的认证,而且要采用一定的访问控制策略来控制对数据和服务的访问.各级提供商之间需要相互的认证和访问控制,虚拟机之间为了避免侧通道攻击,也要通过访问控制机制加以安全保障.因此,云计算中的认证和访问控制是一个重要的安全研究领域.目前,各大云服务提供商也采用了不同的访问控制机制对自己的云平台提供安全支持(详细请参考第 4 节),学术界也从体系结构和技术的角度对该问题进行了研究,但仍存在许多问题:

- 架构方面:(1) 传统的访问控制在适用范围和控制手段上也不能满足云计算架构的要求,由于虚拟技术的出现,云计算环境下的访问控制技术已从用户授权扩展到虚拟资源的访问和云存储数据的安全访问等方面,适用范围和控制手段显著增加;(2) 传统的访问控制分散式管理和云计算环境集中管理的需求之间存在矛盾;(3) 开放动态的访问控制策略对云安全的管理提出挑战.
- 机制方面:(1) 云计算环境各类服务属于不同的安全管理域,当用户跨域访问资源时,需要考虑统一策略,相互授权,资源共享等问题;(2) 云计算中,虚拟资源与底层完全隔离的机制使得隐蔽通道更不易被发现,需要访问控制机制进行控制;(3) 云环境的信任问题也直接影响访问控制.
- 模型方面:(1) 传统的访问控制模型已经不能满足新型的云计算架构要求,以传统的 RBAC 为例,云中的主体和客体的定义发生了很多变化,云计算中出现了以多租户为核心、大数据为基础的服务模式,所以在云计算的访问控制要对主体和客体的有关概念重新界定,这就导致了传统的访问控制模型要进行优化和更新,使其更适用于云计算环境;(2) 角色权限关系复杂的问题,用户变动频繁,管理员角色

众多、层次复杂,权限的分配与传统计算模式有较大区别.

在很多应用场景中,用户对数据的访问通常是有选择性并被高度区分的,不同用户对数据享有不同的权限.因此,当数据外包给云服务运营商,安全、高效、可靠的数据访问控制非常关键.传统的访问控制是用户在可信的服务器存储数据,由服务器检查请求的用户是否有资格访问数据.在云计算环境中,这种模式失效,因为数据的用户和服务器一方面不在同一个可信域内;另一方面,用户以租户的形式对云平台进行访问,所以服务器不再是被完全信任的角色,如果服务器被恶意控制或者可能的内部人攻击,用户的隐私数据可能暴露.综上所述,面对架构、机制和模型层面的问题,必须利用云计算丰富的技术资源,实现细粒度的访问控制设计,保证云中的数据不被非法访问,这样,用户才可以安全地将最繁重的任务委托给云平台,发挥云计算更高的效用.

围绕上述问题,工业界和学术界展开了一系列的研究,工业界的主要解决方案是采取多种访问控制技术相结合或多级访问控制的方式;学术界的主要研究集中在如何保护数据的安全上.访问控制的手段总结起来有 3 种,见表 2.

Table 2 Methods of access control

表 2 实现访问控制的手段

名称	举例	作用
访问控制规则	访问控制列表ACL、访问控制矩阵	网络端口和准入控制
访问控制模型	MAC,DAC,RBAC等	静态分配权限
加密机制	ABE (attribute-based encryption)	保护云中存储数据和主客体交互

需要注意的是,第 3 种是通过密钥机制对数据进行访问控制,其基本思想是主体对数据进行加密,只有能够解密的客体才能对数据进行访问.另外在虚拟环境下,由于虚拟机可以共享物理资源,所以租户之间就可以通过侧通道攻击来从底层的物理资源中获得有用的信息,这也是云计算安全面临的一个新研究课题.综上所述,根据目前学术界的研究现状,我们总结出一个基本的云计算环境下的访问控制体系框架,如图 3 所示.把云计算环境分为用户(租户)、云平台、网络基础环境这 3 部分,用户(租户)和云平台之间要通过访问控制规则和访问控制模型进行访问控制,云平台和网络基础环境大部分采用访问控制规则,云平台中,虚拟机之间要进行虚拟设备的访问控制,对于存储在云平台内部的数据可以基于某种访问控制模型和基于密码学的访问控制手段进行安全保护.可信云平台计算和安全监控审计则是辅助云环境下访问控制技术的必要手段.

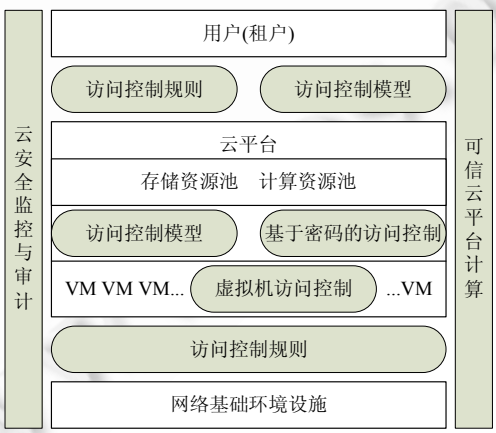

Fig.3 Access control framework in cloud computing environment

图 3 云计算环境下访问控制体系框架

基于上述云计算访问控制技术框架,学术界也多从上述 3 种访问控制手段来进行研究:(1) 访问控制规则研究更多的是对规则的整合优化,使访问控制规则开销更低,效率更高,容量更小,但在云计算环境下研究较少,本文将不去讨论该问题;(2) 访问控制模型在云计算环境下研究较多,主要思路是模型在云计算新环境下的改进

和扩展,使模型更好地为云计算服务;(3) 基于加密机制的访问控制研究更多的是基于 ABE 密码体制的云计算访问控制,主要运用在对云存储的数据访问.另外,虚拟机访问控制研究大多和多租户联系在一起,通过隔离等手段达到虚拟机的访问控制.第 3 节将详细论述云计算环境下访问控制模型、加密机制和虚拟机访问控制等方面的研究情况.

3 云计算环境下访问控制研究

云计算环境下访问控制的研究是伴随着云计算的发展而发展的,在云计算之前,有许多学者研究网格中的访问控制问题,由于网格技术被云计算技术所取代,研究方向也就转移到云计算的访问控制上来.云计算的安全问题很多,可以说,访问控制是云计算安全中的核心内容.根据前述的云计算环境下的访问控制框架和目前学术界研究的内容,云计算访问控制的研究主要集中在以下 3 个方面:云计算访问控制模型、基于 ABE 密码体制的云计算访问控制、云中多租户及虚拟化访问控制研究.

3.1 云计算访问控制模型研究

访问控制模型就是按照特定的访问策略来描述安全系统,建立安全模型的一种方法.用户(租户)可以通过访问控制模型得到一定的权限,进而对云中的数据进行访问,所以访问控制模型多用于静态分配用户的权限.云计算中的访问控制模型都是以传统的访问控制模型为基础,在传统的访问控制模型上进行改进,使其更适用于云计算的环境.目前,对云计算中访问控制模型的研究刚刚起步,根据访问控制模型功能的不同,研究的内容和方法也不同,研究比较多的有基于任务的访问控制模型、基于属性模型的云计算访问控制、基于 UCON 模型的云计算访问控制、基于 BLP 模型的云计算访问控制等.

3.1.1 基于任务模型的云计算访问控制

1997 年,Thomas 等人采用面向任务的观点,提出了基于任务的访问控制模型(task-based access control,简称 TBAC)[14],从任务的角度来建立安全模型和实现安全机制,在任务处理的过程中提供了动态实时的安全管理.该模型能够对不同工作流实行不同的访问控制策略,并且能够对同一工作流的不同任务实例实行不同的访问控制策略[15],非常适合云计算和多点访问控制的信息处理控制以及在工作流、分布式处理和事务管理系统中的决策制定[16].

TBAC 在云计算中的研究多从工作流中的任务角度建模,依据任务和任务状态的不同对权限进行动态管理,使得对于用户级的每一次访问都可以根据任务约束进行建模分析,极大地增强了云中的访问控制的动态性.文献[17]采用任务与 RBAC 结合的模型提出了 T-RBAC,将工作流分解为一些相互依赖的任务,然后将任务分配给角色,角色通过执行任务节点来取得.云服务器通过客体拥有者授权获得权限,并在授权过程管理中充当传递访问请求的可信中间人,使得访问控制安全不需要完全依赖于云服务器的可信度,同时,利用云服务器分担部分授权工作,减轻用户负担.图 4 是 T-RBAC 访问控制模型.

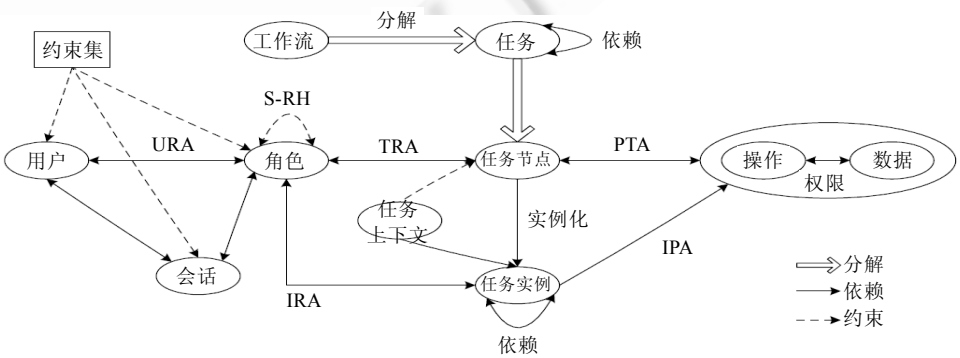

Fig.4 T-RBAC model[17]

图 4 T-RBAC 模型[17]

Huang 等学者首先在云计算环境的服务端进行角色分类,根据访问客体的不同,分配不同的访问角色;然后,在任务分配权限的阶段对权限进行不同的分类,从而可以进一步解决主体对于客体访问过程中产生的效率低和频繁访问的问题[18].文献[19]将 RBAC 应用于可扩展的分布式工作流系统中,在确保分布式工作流系统可扩展的前提下,该模型能够有效地增强对授权访问工作流系统用户的安全控制,但缺乏对工作流在虚拟环境下访问控制问题的讨论.

3.1.2 基于属性模型的云计算访问控制

基于属性的访问控制针对目前复杂信息系统中的细粒度访问控制和大规模用户动态扩展问题,将实体属性(组)的概念贯穿于访问控制策略、模型和实现机制这 3 个层次,通过对主体、客体、权限和环境属性的统一建模,描述授权和访问控制约束,使其具有足够的灵活性和可扩展性.简单来说,RBAC 是 ABAC 的一个子集,ABAC 可以提供基于各类对象属性的授权策略,同样支持基于用户角色的授权和访问控制,角色在 ABAC 中仅仅是用户的一个单一属性[20].

目前,基于属性的访问控制在云安全领域主要集中在将 RBAC 和 ABAC 结合起来,既保证提高用户的隐私,同时也支持访问控制.Ei 等学者将云环境归纳为 3 种属性[21],分别是 U(云资源的使用者)、R(云资源)、E(环境,具体的时间和位置),将云中的属性通过 RBAC 模型进行访问控制.他们还基于此模型开发了一个访问控制系统,这个系统的核心模块就是嵌入 ABAC 的 RBAC.文献[22]采用一种分层的方法来整合 ABAC 和 RBAC.上层是一个标准的 RBAC,支持模型的验证和审查;下层是基于属性的策略生成的安全信息,通过基于属性的策略来对系统进行 RBAC 控制,兼顾了两者的优点.

另外,时间的约束是云计算环境下比较重要的属性约束,时间因素无处不在,用户仅在特定的时间段具有特定的角色,而且云计算的工作模式就是按时计费,所以必须要通过时间来约束对云中数据的访问控制,因此迫切需要 RBAC 模型能够支持复杂的时间约束建模.目前,对单独时间约束的云计算访问控制模型也做了一些研究,Bertino[23]很早就提出了一种基于时态特性的访问控制模型(temporal role-based access control,简称 TRBAC),将时态约束加入到 RBAC 中.该模型带有时态约束,但是没有考虑对用户-角色分配和角色-权限分配的时态因素.文献[24]提出的时态模型把模型要素及其关系上的时态约束嵌入到模型中,通过定义新的时态继承机制实现动态的基于角色的存取控制.该模型能够有效地减少约束规则库中的规则数量,提高存取控制效率,但不太适合大规模的分布式计算.

3.1.3 基于 UCON 模型的云计算访问控制

使用控制模型(usage control,简称 UCON)[25]不仅包含了 DAC,MAC 和 RBAC,而且还包含了数字版权管理、信任管理等,涵盖了现代信息系统需求中的安全和隐私这两个重要的问题.因此,UCON 模型为研究下一代访问控制提供了一种新方法,被称作下一代访问控制模型.UCON 除了授权过程的基本元素以外,还包括义务和条件两个元素.当主体提出访问请求时,授权(authorization)组件将根据主体请求的权限,检查主体和客体的安全属性,比如身份、角色、安全类别等,从而决定该请求是否被允许.义务(obligation)就是在访问请求执行以前或执行过程中必须由义务主体履行的行为;条件(condition)是访问请求的执行必须满足某些系统和环境的约束,比如系统负载、访问时间限制等(如图 5 所示).

云计算环境下的 UCON 模型主要研究以下两个方面:一是设计更适用于云计算的 UCON 访问控制机制和系统;二是研究由于义务和条件的加入,当用户在访问数据时,如何进行位置、时间等方面的约束才能使模型具有更高效的访问控制能力.但是,如何在实际应用中有效地更新属性并确保属性更新的正确性,而更新过的属性能影响进一步的控制,这也给使用中的授权问题带来了更多的风险.文献[26]将风险评估的方法引入 UCON 的授权机制中,提高了使用访问控制模型的灵活性和安全性,使用控制模型的提出主要是面向分布式环境的访问控制需求.文献[27]提出了一种分布式计算环境下使用控制的实施方案,虽然 UCON 模型在分布式、跨域环境下具有明显的优势,但是该模型的授权管理较为复杂.Tavizi 等人构造了一个新的 UCON 模型,主要解决了云计算环境下主体的属性易变性和义务的处理,但没有更深入的理论研究[28].Aliaksandr 等学者提出了一种基于 UCON 和 XACML 标准规范的授权框架,框架整合 OpenNebula 工具箱来实施访问控制,在授权进行的过程中能

够保持访问控制不中断[29].Msahli 等人在云计算环境中引入一个新的实体证据管理者(proof manager,简称 PM),以管理数据提供者和用户之间的证据,并使用 UCON 模型来对云计算中的访问控制管理建模.通过模型来管理两者之间的证据交换、授权等问题,保证云平台安全策略的正常下发[30].

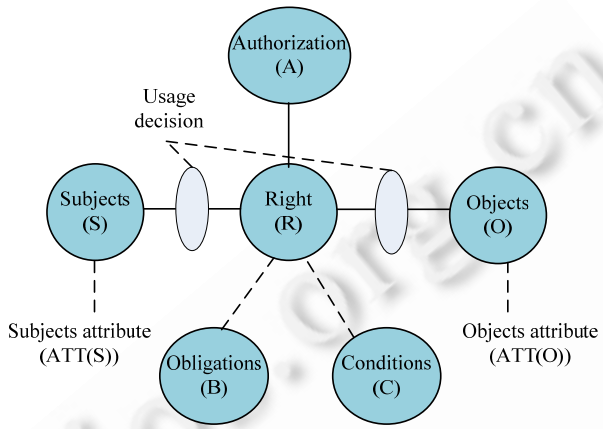

Fig.5 UCON model[25]

图 5 UCON 模型[25]

3.1.4 基于 BLP 模型的云计算访问控制

BLP 模型是强制访问控制模型,主要用于比较强调机密等级的系统或者云环境,比如军事、金融等行业.目前,对 BLP 模型在云计算中的研究主要集中在修改传统的 BLP 模型使其更适用于云计算环境上,并证明模型满足简单安全属性公理和*属性公理**.文献[31]以 BLP 模型和 Biba 模型为基础,借鉴有关行为定义的思想,结合云计算环境的特点,用行为综合角色、时态和环境状态的相关安全信息,将 BLP 和 Biba 模型相结合,提出了 CCACSM,并证明其满足简单安全属性和*属性公理.图 6 是 CCACSM 访问控制模型.

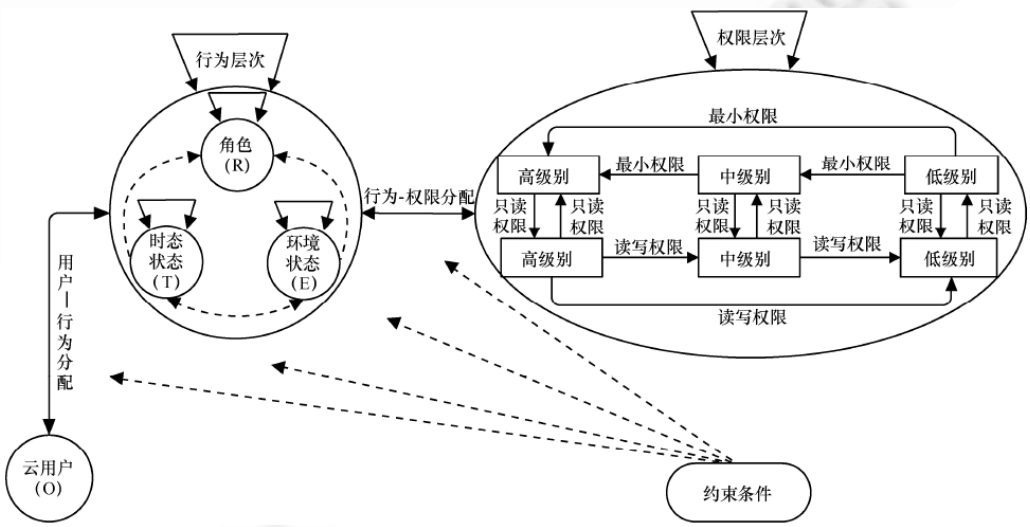

Fig.6 CCACSM model[31]

图 6 CCACSM 模型[31]

** 属性公理表明:若主体对客体有“只写”权限,则客体的安全级至少和主体的当前安全级一样高;若主体对客体有“读”权限,则客体的安全级不会比主体当前安全级高;若主体对客体有“读写”权限,则客体的安全级等于主体的当前安全级.

文献[32]提出了一种基于 BLP 模型的访问控制机制的虚拟机系统,不仅实现了简单的虚拟机间的隔离,而且还能实现高效的共享,该文献从理论上证明了该系统的安全性,也实现了一个基于 Xen 的虚拟机系统的访问控制机制原型系统.

3.1.5 小 结

为了更为直观、简洁地分析和对比各访问控制模型的能力、性能及安全性,我们定义了 14 个方面的指标,并进行了定性的比较.这些指标包括安全性(主体对客体授权是否是强制安全的)、机密性(模型能否保证客体的机密性)、授权灵活性(给客体授权是否灵活高效)、最小特权(模型是否具有最小特权原则)、职责分离(模型是否具有职责分离原则)、描述能力(模型形式化描述是否逻辑清晰)、细粒度控制(能否对云计算环境中的数据进行细粒度访问控制)、云环境属性(是否允许将云环境的相关属性,如时间、区域等加入到模型中)、约束描述(是否引入约束机制对授权的各个环节进行相应限制)、云环境动态变化(模型能否动态地适应云计算环境的变化,并做出相应的调整)、兼容性(模型能否兼容各种程序)、扩展性(模型是否具有良好的扩展性)、易管理程度(云平台管理员是否容易对模型进行管理)和建模容易度(模型建立是否容易简捷),见表 3.表 3 中的符号"√"表示该项指标性能较好,空白则表示不好或尚未具有该项指标特征.

Table 3 Performance comparison among access control models

表 3 访问控制模型性能对比

	RBAC	TBAC	ABAC	UCON	BLP
安全性					√
机密性					√
授权灵活性	√			√	
最小特权	√	√			
职责分离	√	√			
描述能力	√		√	√	
细粒度控制			√	√	√
云环境属性		√	√	√	
约束描述	√				
云环境动态变化		√	√	√	
兼容性			√	√	
扩展性			√	√	
易管理程度	√				
建模容易度	√				√

综上所述,访问控制模型在云计算环境下的研究取得了一些发展,但总体来说还有些缺陷,主要体现在:

1) 云计算中的访问控制模型的主体发生了变化.云计算中用户与租户的关系很复杂,两者同时都是访问控制模型的主体,所以要进一步形式化描述云计算中用户和租户的关系以及在模型中的作用.
2) 没有综合考虑云计算的特性因素,如时间、位置的影响,云资源服务化、云资源迁移的影响等.云计算是一个动态的分布式系统,所以将云计算中动态的因素作为访问控制模型的约束条件进行研究,才可能更加适合云计算环境.
3) 云计算将资源作为服务提供给用户,从模型角度来讲,访问的客体发生了变化:服务将成为直接客体,数据成为间接客体,将服务作为客体加入到模型中将更适合于云计算环境.所以,服务化模型也是未来研究的重点.

3.2 基于ABE密码机制的云计算访问控制研究

密码机制是通过加密数据,使只有具备相应密钥的授权人员才能解密密文.密码机制访问控制技术可在服务器端不可信的环境中保证数据的机密性.数据所有者在数据进行存储之前预先对其进行加密,通过控制用户对密钥的获取来实现访问控制,这要求加密密钥必须由数据所有者自己生成并管理.目前已提出了大量层次访问控制的密码解决方案.之所以采用密码体制进行访问控制,是因为云平台大多不可信,用户将数据存放在不可信的平台上是不安全的,对于数据的隐私保护、机密性、完整性都不能达到很高的安全等级;并且一旦数据上

传至云,数据提供者就不能对数据有更多的控制权,所以采用密码方式对数据进行保护非常有必要.这种方法主要针对主客体之间交互比较多的数据和比较敏感的数据.目前,ABE(属性基加密)就是一种最常见的密码机制.

ABE 密码机制自 2005 年开始研究,其发展了传统的基于身份密码体制关于身份的概念,将身份看作是一系列属性的集合.Sahai 与 Waters 第一次提出基于模糊身份加密的方案[33],将生物学特性直接作为身份信息应用于基于身份的加密方案中,Sahai 在论文中引入了属性的概念.2006 年,Goyal 等人在基于模糊身份加密方案的基础上提出了基于属性的加密方案 ABE[34],随后衍生出了两种与策略树有关的 ABE 算法,即,密钥策略 ABE(key-policy attribute-based encryption,简称 KP-ABE)和密文策略 ABE(cipher-policy attribute-based encryption,简称 CP-ABE).2006 年,Sahai 等人[35]首次提出了 KP-ABE 的概念,在 KP-ABE 中,可描述的一组属性与密文相联系,解密密钥用策略树来约束,当访问控制策略树能够匹配属性后,解密者才能获取解密密钥.因此,加密方对明文没有任何的控制权,KP-ABE 适合于大规模网络环境下的密钥管理[36].2007 年,Sahai 和 Waters 又提出了 CP-ABE[37]的概念,在 CP-ABE 中,访问控制策略树与密文相联系,解密密钥用一组可描述的属性来约束,当解密方拥有的属性匹配策略树成功时才能获得解密密钥,获得对资源的访问权.与 KP-ABE 相比,CP-ABE 更适合于大规模环境下的访问控制,目前学术界对 ABE 在云计算环境下的应用大部分都采用 CP-ABE 算法.

图 7 是 ABE 密码体制在云计算环境下的模型,包括 4 个参与方:数据提供者、可信第三方授权中心、云存储服务器和用户.方案描述如下:首先,可信授权中心生成主密钥和公开参数,将系统公钥传给数据提供者;数据提供者收到系统公钥之后,用策略树和系统公钥对文件加密,将密文和策略树上传到云服务器;然后,当一个新用户加入系统后,将自己的属性集上传给可信授权中心,并提交私钥申请请求,可信授权中心针对用户提交的属性集和主密钥计算生成私钥,传给用户;最后,用户下载感兴趣的数据.如果其属性集合满足密文数据的策略树结构,则可以解密密文;否则,访问数据失败.

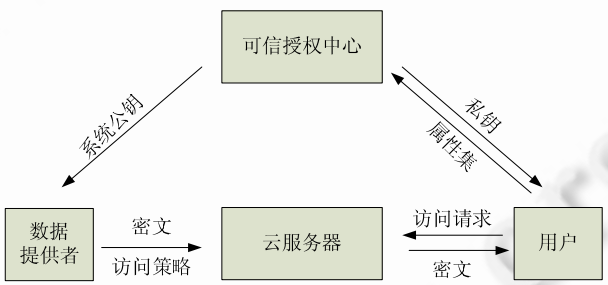

Fig.7 Model of ABE for cloud computing environment[38]

图 7 ABE 在云计算环境下的模型[38]

ABE 包括 4 个步骤,见表 4.

Table 4 ABE algorithm steps

表 4 ABE 算法步骤

Setup	授权中心执行,生成主密钥*MK*和系统公钥*PK*
Encrypt	*CT*=*Encrypt*(*PK*,*M*,*T*),发送方执行,属性集*T*加密消息*M*,生成密文*CT*
KeyGen	*SK*=*KeyGen*(*MK*,*A*),授权中心执行,生成用户的私钥*SK*
Decrypt	*M*=*Decrypt*(*CT*,*SK*),接收方执行,利用自己的私钥解密得到*M*

ABE 最突出的优点是很适合于分布式环境下解密方不固定的情况,加密方加密信息时无需知道具体是谁解密,而解密方只需符合相应属性条件即可解密;并且 ABE 将加密规则蕴含在加密算法之中,可以免去密文访问控制中频繁出现的密钥分发代价.ABE 具有很强的安全性:(1) ABE 的算法基于椭圆曲线上的双线性对,从密码学理论上来讲,破译密码是不可能的;(2) ABE 的密文被附上了一个存取结构,这个存取结构的复杂性使得在安全性证明的模拟过程中,模拟者难以将其“嵌入”一个普通简单的困难性假设(如 Diffie-Hellman 假设等),这导

致了挑战密文的困难;(3) ABE 私钥具有一定的属性,不同的私钥属性集合可能具有相交的属性,这样的私钥相关性也给模拟私钥提取问询造成了困难.

目前,ABE 在云计算环境中实现对数据的访问控制主要从 3 个方面进行研究:第一是细粒度访问控制,第二是用户属性撤销问题,第三是多授权中心(multi-authority)方案.ABE 在提供数据安全性的同时进行细粒度的访问控制,直接将 ABE 技术应用于云存储系统并不能很好地解决一些诸如效率和可扩展性的问题.例如,云存储系统涉及大量的用户和数据,加密、用户组和密钥的管理等机制都需要较高的可扩展性,直接应用 ABE 会导致效率不高的问题;用户属性的撤销设计难度较大,实现起来效率不高;特权用户仍可获取用户敏感数据,数据属主仍未达到对共享数据访问的完全控制;将 ABE 与可信计算研究相结合等问题.

3.2.1 ABE 细粒度访问控制研究

ZHU 等人建立了一个有效的 RBAC 和 ABE 兼容的云数据加密体制[37],这种加密体制设计为将用户通过 RBAC 访问云中数据和数据在云中的 ABE 加密同时进行,通过算法将二者在理论上结合起来,达到控制数据泄露的效果.Anuchart 等人提出了一个基于 OAuth 标准和 CP-ABE 的授权方案(AAuth)[39],它提供了端到端加密和基于 ABE 的令牌策略,这些策略使得无论是授权中心还是数据拥有者都可以认证云中的数据.与以用户为云中心的方法不同,当处于不信任的云环境中的时候,数据拥有者控制自己的数据,使自己的数据不受云中非法用户的访问.Sun 等人在基于密文属性的加密算法 CP-ABE 的基础上提出了云存储数据安全访问控制方案,将公钥和私钥形式化为读写权限、通过设计密钥来进行访问控制并直接进行分布式分发密钥的方法更容易管理密钥,同时也对用户更透明,即,少让用户涉及密钥生成、密钥发布等事务[40].Ruj 等人提出了一种可对云中的数据实现隐私保护和认证的访问控制框架,在这个框架中,云平台可以在数据拥有者往云平台存放数据之前对其进行认证,而对于认证过的用户可以在云平台中对数据进行 ABE 加密存储[41].

3.2.2 用户属性撤销研究

用户属性撤销是指当用户的属性发生变化时,它就失去了对该加密数据的访问权限.那么,ABE 该如何对用户的权限进行撤销或者更改,这个问题在云计算环境下非常关键.目前对这个问题有些研究,但是还需要设计更高效的算法.文献[42]提出代理重加密方案(attribute-based proxy re-encryption,简称 ABPRE),通过代理将密文从一种访问结构树加密变为另一种访问结构树加密,以达到权限撤销的目的.但该方案的撤销单位只能是属性集,即,具有相同身份特征的一类用户.文献[43]利用 CP-ABE 算法和公钥密码系统来实现密文访问控制.该方案不足的是,数据拥有者仍然要承受巨大的重加密代价.文献[44]提出在应用 CP-ABE 算法时扩展一个用户属性,即,为该属性贴上一个终止时间,保证了密钥的安全性.但该方案的缺陷是:用户需要周期性地向认证中心申请私钥,效率低;而且在终止时间之前,用户的权限是无法撤销的.Yu 等人在文献[45]中提出了 CP-ABE 算法中的一种属性撤销方案,方案假定 CSP 是存在一定可信度的,数据拥有者将部分工作交付 CSP 执行.但该方案中访问结构树只支持“and”门限,并不能提供精细灵活的访问控制策略.同年,Yu 等人又在文献[46]中描述了基于 KP-ABE 技术在云计算环境实现细粒度的访问控制;同时,运用基于重加密技术实现了有效的用户撤销机制.在他们的方案中,首先选择一个对称密钥将文件加密;其次,针对每一个属性集合中的属性,在密文添加一个特别密文元素,在解密操作中,这些密文元素将会被用来恢复这个对称密钥.

3.2.3 ABE 在多授权中心(multi-authority)方案的研究

ABE 在授权的时候,用户的每个属性需向一个可信的授权中心获得签名私钥,这就需要单个授权中心管理大量属性,这会极大地增加其工作负担,降低效率,这就出现了多授权中心的概念.多授权中心要求由不同的认证中心来认证每个用户保存属性或访问树,并且额外需要一个可信的中心授权方来管理和约束各个授权中心.多授权中心是云计算环境的特点,最早是由 Chase[47]提出的多授权中心概念,并给出了一个多授权中心的基于属性的加密方案,用户的多个属性由不同的授权中心监管,并分别对其中的每个属性产生加密私钥.基于此方案,Chase 第一次提出了一种多授权中心的基于属性的签名方案,为了防止授权中心盗用私钥,方案中每个授权中心控制一部分属性,能够抵抗伪造性攻击和合谋攻击,拥有保护签名者的私密信息和较高的签名效率的优势.

另一个主要的挑战是来自不同部门的多个用户(包括属性已被撤销的用户和非法用户等)获得非法访问数

据的权限,所以近些年也有学者继续研究多授权中心的 ABE 方案.文献[48]提出了一个分布式 KDC (密钥分发中心)的方法,给数据所有者和用户分配一个特定的属性集,数据所有者进行加密,用户如果匹配上了数据集就可以解密,进而从云中获取数据.ABE 的加密模型的应用是安全的,前面已有概述,这就导致破译密码是完全不可能的.Yang 等人在文献[49]中提出了一个适合云计算环境的多授权中心访问控制模型.根据这一模型,每个用户被分配一个独有的用户标识符(UID)和一个独有的授权标识符(AID).UID 和 AID 都是由被信任的证书颁发机构(CA)签发的,防止多个用户勾结非法访问数据,被 CA 认证过的 UID 要和密钥一起来使用才能对数据进行解密,很好地保证了数据的安全性.Yang 等人又在第 2 年做了进一步的研究,提出了 DAC-MACS(数据访问控制的多授权中心云存储).这个方案使用基于 token 加密的方法来管理各个授权中心,使其不易被非法用户进行攻击;同时,方案设计和实现了用户属性撤销时的正向安全和后向安全,达到了高效属性撤销的效果[50].文献[51]提出了一种层次化的属性基访问控制方案,该方案在 CP-ABE 的基础上加入属性基签名(ABS),并将 multi-authority 进行分层处理,每层 authority 担任 CP-ABE 不同的算法,实现权限授予和粗粒度资源访问的功能.

综上所述,将 ABE 用在云计算的访问控制技术领域,能够将其优点完全发挥出来,一方面是 ABE 算法体系适用于云计算架构,另一方面是 ABE 能够完整地实现对云平台中的数据进行访问控制.目前,研究更多的主要是将 ABE 应用到云计算中之后算法自身的一些问题,比如更细粒度的访问控制、用户属性撤销、多授权中心方案等方面.展望未来的研究,可以更注重云计算环境下 ABE 与其他技术的结合,如,ABE 与身份认证技术相结合,研究访问控制中通过用户属性进行身份认证的问题;ABE 与可信计算技术相结合,研究利用数据提供者和用户对云服务器的信任关系进行访问控制的问题等.

3.3 云中虚拟化及多租户访问控制

由于租户间共享物理资源,并且其可信度不容易得到,所以租户之间就可以通过侧通道攻击来从底层的物理资源中获得有用的信息[52].此外,由于在虚拟机上要部署访问控制策略可能会带来多个租户访问资源的冲突,导致物理主机上出现没有认证的或者权限分配错误的信息流.云环境下,租户之间的通信应该由访问控制来保证,并且每个租户都有自己的访问控制策略,使得整个云平台的访问控制变得复杂.所以,最重要的是要隔离租户间出现的异常的流量,部署适当的访问控制策略来屏蔽非法的流量,来避免各种各样的攻击.例如,攻击者可以通过发送大量的授权请求和恢复来尝试进行拒绝服务攻击与之位于同一物理机的其他虚拟机,这就需要在受害虚拟机上部署访问控制策略来隔离从底层的物理主机向受害虚拟机发送类似的信息流,从源头上避免虚拟机之间存在的不安全性.

目前,对多租户访问控制的研究主要集中在对多租户的隔离和通过 hypervisor 实现虚拟机的访问控制,但是在虚拟环境下,如何将隔离、访问控制模型和网络结构等多种手段相结合来实现访问控制的研究还比较少.管理虚拟机间的访问控制策略一般有以下两种方案:

- 第 1 个解决方案是在每个虚拟机上部署各自的访问控制策略,以便直接管理目标.然而这种方法可扩展性差,而且对于多租户的云平台来说部署繁琐,不能够很好地管理.
- 另一个解决方案是使用集中式存储访问控制策略和组成员,将访问控制策略部署在 hypervisor 上,通过集中部署访问控制策略来管理 hypervisor 层之上的所有虚拟机.然而这样一个集中的服务必须保持非常高的可用性和低响应时间,并且还要抵御拒绝服务攻击.

所以,怎样对访问控制策略进行管理也是云计算环境下要深入研究的问题.

3.3.1 通过对多租户的隔离实现访问控制

Hao 等人[53]提出了将网络访问控制策略存储在一个中心服务器处,在转发元件(即,增强型的二层交换机)中强制施行这些策略.客户网络的隔离通过使用虚拟局域网来实现,当分组发往同一个 VLAN 时,不需要经过策略检测就直接发送到目的地虚拟机;而当分组是发往不同的 VLAN 时,则根据安全策略进行转发判定.Factor 等人为了提高系统物理隔离的安全性,提出了安全逻辑隔离的多租户(SLIM).SLIM 采用了完整的安全模型和安全的租户资源、云存储系统以及租户之间逻辑隔离的原则,并在 OpenStack 做了实验[54].

文献[55]提出了将云服务提供商和租户(客户)的安全职责分离.该文献提出了一个基于多租户访问控制模

型,在该模型中,CSP 可以操作对云中租户的添加、删除和管理以及相关的安全问题.由租户来管理自身的访问控制,通过访问控制确保租户自身的安全性.例如,在 PaaS 服务交付模式,CSP 应提供一个安全的计算平台和开发环境,而客户应确保他们的应用程序安全可靠;在 IaaS 服务交付模式,CSP 应为客户提供可信的基础设施,而客户应确保相关的实例和镜像安全.Almutairi 等人[56]提出了一种分布式安全架构,并对其进行了安全性证明.这种架构由 3 部分组成:虚拟资源管理器(VRM)、访问控制机制(依据基于角色的模型实施)和云提供商在多租户环境中实施的 SLA.云间的通信、租户在同一层或不同层的通信以及内部云通信都采用这种分布式安全架构.

3.3.2 将多租户技术与 RBAC 模型相结合进行访问控制

各个租户可以访问在同一个云服务器的不同的应用和计算资源,为了避免产生访问控制失败的问题,可以将访问控制技术回归至模型的研究.许多学者将多租户技术加入 RBAC 模型中,生成新的访问控制模型,加强租户对数据的访问控制.Tang 等人[57]在多租户认证系统(MTAS)的基础上与 RBAC 模型相结合,提出了管理多租户认证系统(AMTAS)模型.在 MTAS 基础上增加了信任的条件,对多租户之间的信任进行了形式化分析.Yang 等人[58]提出并设计了基于角色的多租户访问控制(RB-MTAC).RB-MTAC 不仅适用身份管理来确定用户的身份和适用的角色,而且可以高效地管理租户的访问权限来实现应用程序的独立和数据的隔离,以提高云计算多租户服务的安全性和私密性.

3.3.3 通过 hypervisor 实现虚拟机的访问控制

文献[59]中比较了两种可以实现多租户安全的有效结构:一种是基于虚拟化的多租户架构,一种是基于操作系统多租户的结构.他们都能在虚拟机的 hypervisor 上隔离用户,并通过一个共享的操作系统实现强制访问控制.最后结果表明,基于操作系统多租户的结构开销更小.文献[60]中提出了一种基于 hypervisor 的多租户访问控制机制,称为 CloudPolice.这种方法对于云环境的访问控制有更好的伸缩性和健壮性.文中给出了一种处理可伸缩性的方法,让 hypervisor 来动态地协调它所承载的虚拟机的访问控制策略,根据源虚拟机到目的虚拟机之间的具体通信状况来确定访问控制策略的分布,其访问控制策略包括租客隔离、租客间通信、租客间公平共享服务和费率限制等.图 8 是 CloudPolice 的具体实施方案,其主要思想是:当数据流到来的时候,源 hypervisor 抢在数据流到目的 hypervisor 之前发送一个控制策略数据包,目的 hypervisor 检查这个数据包:如果策略符合,则将数据流接受;如果不符合,则反馈给源 hypervisor,停止或减少数据流.

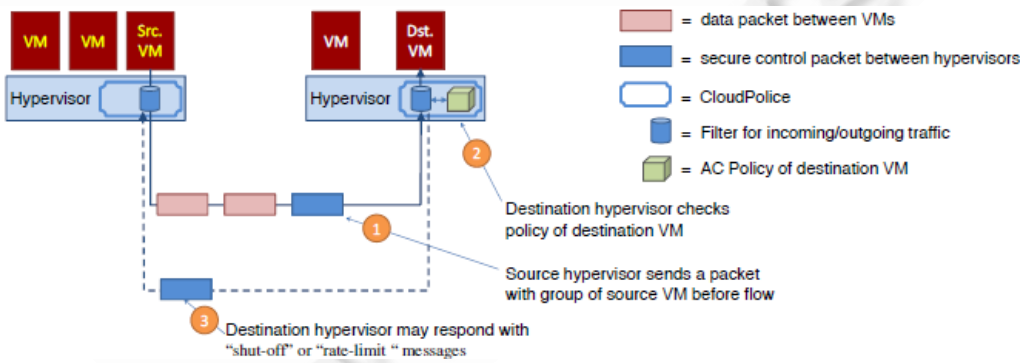

Fig.8 Workflow of CloudPolice[60]

图 8 CloudPolice 工作流程[60]

总之,当前阶段,虚拟化技术已经比较成熟,多租户之间的访问控制策略一般和虚拟机内部结构和工作状态联系得比较紧密,要全面了解 CPU 虚拟化、内存虚拟化、I/O 虚拟化的技术,才能在此基础上拓展其安全性.

4 工业界的云计算访问控制

工业界在发展各自云计算服务规模、性能的同时,也不断提升云计算平台的安全能力.对于云安全中的访

问控制技术,各大云服务提供商和开源云平台在体系结构、控制手段、具体技术等方面都有所研究,并运用到实际运营当中.EMC 信息安全事业部 RSA 首席技术官 Hartma 表示[61],专业的安全厂商可以满足云计算服务提供商 3 个方面的安全需求:

- 第一,保护云服务提供商免受外来攻击.
- 第二,满足云计算环境中不同租户之间的数据独立性.在一个云环境中,通常会有两个以上的租户,他们之间的数据不能互相干扰;而且在未经授权的情况下,一个用户不能访问另一个用户的数据.
- 第三,确保云服务提供商自身平台安全,比如访问控制、身份认证等基础性的要求.

只有满足这 3 个方面的需求,企业才能放心地将他们的应用转移到云平台上.

4.1 各个云服务提供商访问控制的应用

Amazon[62]云平台的数据管理是通过 Amazon Simple Storage Service(S3)提供的可靠网络存储服务,通过 S3,个人用户可以将自己的数据放到云平台上去,并进行访问和管理.S3 将每个数据对象(object)存储在称为桶(bucket)的容器中进行管理,Amazon 不仅控制用户对 object 的操作(读、写、删),也会控制用户对 bucket 的操作(罗列对象、增加、移除对象等).Amazon 访问控制方式有 4 种:

1) IAM.通过在 Amazon 账户之下创建多个用户,分配相应的安全凭证给用户以及管理他们的权限.
2) ACL.账户层次的访问控制策略,即,访问权限是基于资源的权限.以对象和桶为中心,定义了哪些 Amazon 账户能够访问对象和桶.
3) Bucket Policy.兼具用户层次和账户层次的控制策略,桶策略不仅可以控制访问桶的用户,还可以控制特定源 IP 地址的访问.另外,Bucket Policy 可以实现让其他账户上载对象到桶中,以实现跨账户的权限控制.图 9 显示出 IAM Policy 和 Bucket Policy 的不同.
4) 查询字符串身份认证.该机制利用 URL 与其他用户共享数据对象,通过在 URL 中附加签名和有效期来访问共享数据.

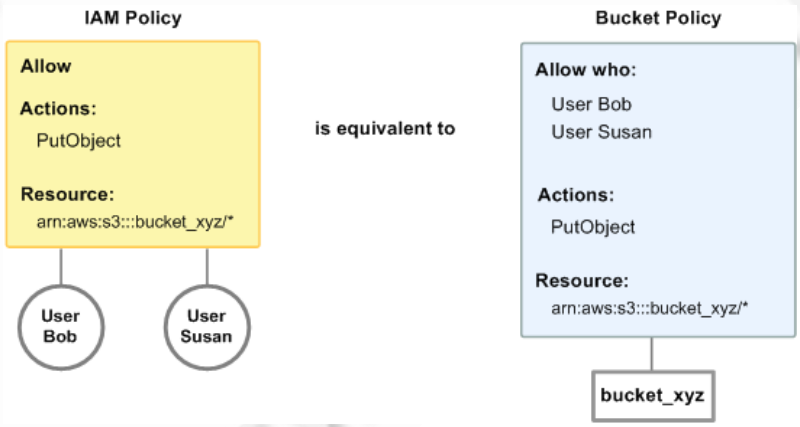

Fig.9 Comparison between IAM Policy and Bucket Policy in Amazon[62]

图 9 Amazon 中,IAM Policy 和 Bucket Policy 对比[62]

微软云,即 Windows Azure[63],它定义了 3 种数据存储方式:Blob,Table 和 Queue.其中,Blob 用来存储大数据(如图片、视频等),Table 提供维护服务状态的结构化存储,Queue 提供异步任务数据的分发.Windows Azure 的访问控制管理主要有两个方面:

1) 共享访问签名.在特定时间间隔内,对 3 种数据存储方式进行受限访问权限,通过 URL 与其附加签名和有效期来访问共享数据.
2) Blob policy.使用 Blob 容器级别的访问策略可从服务器方面提供对共享访问签名的额外控制级别.

容器级别的访问策略可将共享访问签名分组,并进一步限制策略所约束的签名.用户可使用容器级别的访问策略改变签名的启动时间、到期时间或许可证,或者在发布签名后予以撤回.

另一方面,微软还致力于访问控制产品的开发,它和以 VMware 为首的阵营各自提出了 NVGRE(network virtual GRE)和 VXLAN(virtual extensible LAN),用于解决跨数据中心的大规模 VLAN 通信、虚拟机迁移等问题:前者使用了 L2oUDP 的封装方式,支持 16M 的 tenant ID;后者使用了 L2oGRE 封装方式,也支持 16M 的 tenant ID.这两种技术的主要特点是,隧道的起点和终点在 vswitch 上,而不是物理交换机上,以期达到快速部署、灵活创建虚拟化网络的目的.两个提案都解决了相同的问题:VLAN 的上限只有 4 094 个,无法支持多个云租户和应用程序.不同之处在于存储目标地址的位置.

Google 云[64]的访问控制技术为每个用户提供一个唯一的用户 ID,此 ID 用来识别每个用户在 Google 云的活动记录.通过用户 ID,Google 云平台给分配相应的权限.数据容器桶是 Google 云存储中存放数据的最基本容器,所有数据都必须存放在桶中,Google 利用桶来组织数据.Google 存储提供了两种访问控制机制:

1) ACL.在 Google 云的访问控制列表机制中,主要有读、写、完全控制 3 种级别的权限,在桶和对象的拥有者未指定桶和对象的 ACL 时,系统会使用默认的 ACL 来控制用户访问.所有桶默认其拥有者具有完全控制权限,拥有者可以通过修改和更新 ACL 来控制其他用户的不同权限.
2) 签名的 URL(查询字符串认证).不需要 Google 账号就能访问数据,该机制类似于 Amazon 查询字符串认证,也是通过在 URL 中附加签名和有效期来访问共享数据.

百度云[65]云存储(BCS)服务目前支持两种方式对存储资源进行访问控制:

1) URL 签名:通过对 URL 进行签名来识别访问者的身份,从而实现用户身份验证.百度云存储的开发者可根据 Access Key 和 Secure Key 对本次请求进行签名,BCS 根据签名来判断当前发起请求的用户的身份.
2) 通过 ACL 来管理 bucket 和 object 的访问控制权限,管理方式即设置 bucket policy 和 object policy.通过设置 policy,可允许云存储用户将资源(bucket 和 object)的访问和控制权限开放给其他用户.

云服务提供商访问控制技术对比情况见表 5.

Table 5 Comparison among access control technology of cloud service providers

表 5 云服务提供商访问控制技术对比

	Amazon	Windows Azure	Google	百度云
存储对象	Bucket 和 Object	Blob,Table 和 Queue	Bucket 和 Object	Bucket 和 Object
访问控制策略	IAM policy,Bucket policy,ACL,结合使用 Bucket policy 和 ACL,URL 签名	共享访问签名,Blob policy	URL 签名,ACL(Bucket policy 和 Object policy)	URL 签名,ACL(Bucket policy 和 Object policy)

4.2 各项开源云平台访问控制技术

目前,主流的开源云平台主要集中在 OpenStack[66],CloudStack[67]和 Eucalyptus[68]这 3 个产品中,其中以 Openstack 最为流行.这样的开源云平台构建云服务,对于市场上很多寻求灵活性和定制化的云环境的客户来说是极具吸引力的选择.在访问控制性能方面,三者都具有很高的安全性,保证用户级别和权限的有效区分,保证虚拟机严格按照策略进行访问.三者的相同点是均设置了安全组(security group),安全组是一些规则(ACL 或 IPtable)的集合,管理员或者授权用户通过设置这些规则来对虚拟机的访问流量加以限制,达到访问控制的效果.不同点有很多,表 6 从以下 3 个方面对开源云平台访问控制技术进行对比,分别是访问控制组件、用户级别区分、虚拟机和网络访问.

这里着重介绍 Openstack 的 Keystone 组件,它采用统一 token 的认证方式,用户从认证到申请虚拟机、镜像、网络服务都要通过各个模块对用户 token 的确认,核实通过后才能继续操作.通过对 token 的确认,Openstack 对用户进行相应的身份授权.图 10 是 Keystone 在 Openstack 中的访问控制流程图.

Table 6 Comparison among access control technology of open source cloud platforms

表 6 开源云平台访问控制技术对比

	OpenStack	CloudStack	Eucalyptus
访问控制组件	1. 认证授权组件 Keystone:提供了认证和管理用户、帐号和角色信息、授权服务,如图 10 所示; 2. 网络组件 Neutron:管理安全组、虚拟机和网络访问.	1. 没有专用访问控制组件; 2. 资源域(zone)管理用户、安全组、虚拟机和网络访问,资源域之间可以实现完全物理隔离的,硬件资源、网络配置、虚拟机都是独立的.	1. 没有专用访问控制组件; 2. 云控制器(CLC)处理身份认证、用户管理; 3. 集中控制器(CC)管理安全组、虚拟机和网络访问.
用户级别区分	1. 分为 User 和 tenant (project),User 通过 tenant 对云平台进行操作,每个 tenant 都有 admin 级别和普通级别,两者权限不同,不同的 tenant 资源隔离.	1. 分为 Domain\Account\User,树状结构,Account 属于 Domain, User 是 Account 的别名,不同 Account 的资源相互隔离.	1. 分为 Account\User 两级结构,User 分为 admin 级别和普通级别,两者权限不同 admin 级别可以进行 Group 编辑.不同 Account 的资源相互隔离.
虚拟机和网络访问	1. 对网络组件 Neutron 中的 port 设置进入规则和流出规则来实施访问控制,每个 tenant 默认一个安全组,允许 tenant 的虚拟机之间内部通信; 2. 网络隔离主要通过 VLAN,Flat 或者 FlatDHCP 模式实现.	1. 对一组(个)IP 或同一安全组的所有 VM 设置进入规则和流出规则来实施访问控制,每个 User 初始默认一个安全组,一个 User 可以创建多个安全组,可同时应用多个安全组在一个虚拟机上; 2. 网络隔离主要通过 VLAN 实现.	1. 为虚拟机提供 3 层网络的防火墙服务,对同一安全组的所有 VM 设置进入规则和流出规则来实施访问控制,每个 User 默认一个安全组,允许 tenant 的虚拟机之间内部通信; 2. 网络隔离主要通过 VLAN 或者 ebtable 实现.

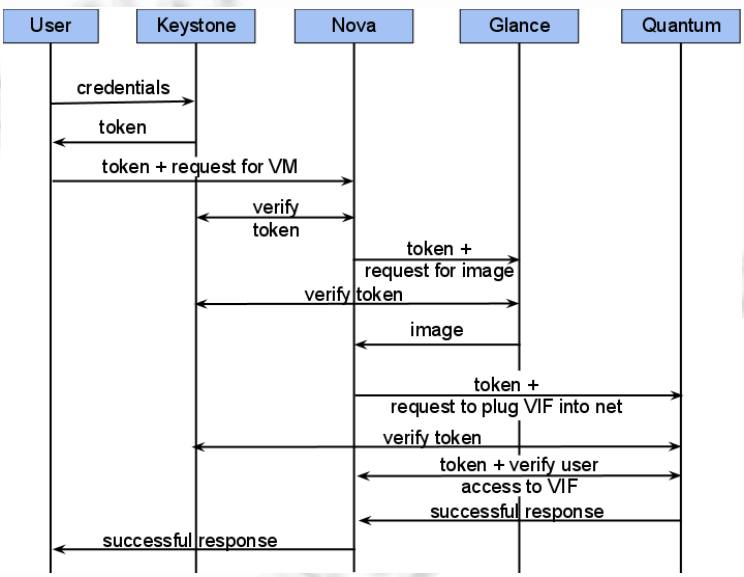

Fig.10 Access control flow of Keystone in Openstack[69]

图 10 Keystone 在 Openstack 中的访问控制流程[69]

综上所述,目前的工业界都在其云平台中实现了一些基本的访问控制技术,但是也存在许多共性的问题:第一,云平台服务提供商提供的云存储服务中虽然运用了云的理念和技术,但是对于保证存储数据访问的安全性来说,采用传统的访问控制技术基本上能够实现,如加密等;第二,目前大部分云平台服务提供商都以 RBAC 为基础来实现用户对云中数据的访问控制,虽然能够实现对数据的基本访问控制,但基本上没有考虑云计算的新特点给传统的访问控制技术带来的挑战,缺乏理论上对云环境下的访问控制模型的支持;第三,不少厂商能够提供部分面向 IaaS 的访问控制服务,但是将访问控制服务与 SaaS 结合很少,所以还需要工业界对访问控制技术继续探索和研究.

5 云计算访问控制展望

由于云计算自身的特点,导致了云计算安全问题更加突出,如资源共享、多租户、虚拟化和资源服务化等概念.所以对云计算环境下的访问控制研究必须立足于云计算自身的特点,结合传统的访问控制技术来进行研究.还有一个不能忽视的问题就是,网络基础设施安全性对云平台的影响也起到很关键的作用,例如,使用 VLAN 和防火墙等也可以从底层对云中的资源进行保护.所以,建设安全的网络基础设施环境是云计算环境下实现访问控制的基础.

研究云计算中的访问控制需要考虑的因素很多:

- 从位置上来说,一方面要考虑用户(租户)进入云平台时的访问控制策略,二要考虑云平台内部数据和资源对于需求者的访问控制,三要考虑虚拟机之间的访问控制.
- 从规模上说,一方面要考虑粗粒度的访问控制,要从云平台的大环境中考虑,对物理资源和虚拟资源进行访问控制,保护底层资源不被破坏,为云计算奠定安全基础;另一方面还要考虑细粒度的访问控制,保证云中的数据、信息流、记录等等不被恶意人员所窃取.
- 从访问控制的设计上来说,新的访问控制机制对于云计算环境必须灵活(支持多租户环境)、可伸缩(可处理成千上万的机器和用户)和网络独立(与底层网络拓扑结构、路由和寻址不耦合).

我们认为未来云计算中访问控制技术应该重点从以下几个方向进行研究.

5.1 基于虚拟化的访问控制技术研究

(1) 研究虚拟技术的访问控制

虽然虚拟技术有良好的隔离性,但在很多应用上必须进行虚拟机间的通信,而虚拟机间频繁的交互带来了新的安全挑战.例如,由于云计算环境是多租户模式的,用户(租户)更喜欢独立于其他用户(租户)来进行通信,虚拟机间有可能产生未经授权的非法访问、通过虚拟机间通信产生攻击行为;由于属于不同的组织或部门的虚拟机(通常有不同的安全级别)常常运行在同一台物理主机上,因此,研究多级安全和多层次的访问控制方案十分必要,例如,在 VM 和 hypervisor 上同时使用访问控制,这样可以保证不同的 VM 从底层资源分离开,防止侧通道攻击等.

(2) 研究虚拟机动态迁移对访问控制的影响

云计算最大的一个特性就是弹性计算,虚拟机可以根据性能进行动态的迁移,这给访问控制带来了许多挑战.一般数据的存储模式有两种:一种是共享存储,一种是虚拟机存储.如果是共享存储,虚拟机迁移对数据的访问控制影响不大,但对访问控制策略的部署和管理要做到随着虚拟机的迁移而迁移,不能出现策略的更改;如果是虚拟机存储,那么随着虚拟机的迁移,数据就很有可能被迁移到其他的网络(包括 VLAN)中去,并且由于虚拟机性能不同,访问数据的权限也有可能发生变化.所以,怎样保证迁移过程中网络和权限变化对数据访问控制的影响就非常关键.

5.2 基于信息资源属性变化的访问控制技术研究

(1) 研究云计算客体属性服务化的访问控制模型

在云计算中,无论是 IaaS,PaaS 还是 SaaS 都是将资源进行了服务化,因此可以将传统的访问控制模型客体各个要素加以服务化,形成服务池,并将实际资源和服务池分开进行管理,让主体通过服务池来访问实际的资源.这一方面是可以将访问控制模型作为服务来提供给用户,另一方面是可以将服务作为访问控制的最终目标.这样才能将传统的访问控制模型更好地与云计算相结合,极大地减少了云平台中各种资源在访问控制过程中可能出现的问题,也符合云计算真实的模型.

(2) 研究权限属性动态化的云计算访问控制技术

在数据正在访问的过程中,如果此数据的访问权限发生改变,该如何做到有效地进行访问控制,以防止由于对数据继续访问而违反访问控制策略,从而减少从云计算内部对数据和资源进行威胁?在数据进行访问过程中,用户的角色和角色权限分配分别进行设计,通过用户、角色、对象和环境的属性来作为影响整个访问控制的因

素,并且用户角色和角色权限分配规则将会实时地执行访问控制决策.

(3) 研究能够感知位置属性的角色控制模型

在云中能够对用户的位置进行感知,通过位置来确定用户的角色,从而防止向不完全信任的云服务器暴露用户的身份、角色或位置等.当用户处于一个特定的位置时,位置属性感知在前几年有学者研究过,如文献[70−73]等,这些文献很好地研究了如何通过感知位置属性来进行角色的划分,但是在云计算环境下研究该问题还不多见.当云计算环境扩大到一定规模时,用户所处的位置就非常重要,可以决定该用户能够获得什么样的资源;而且通过位置信息可以判断该用户是否处在相对可信的环境下,结合信任模型可以激活角色,从而有效地保护用户的身份.

(4) 研究 Inter-Cloud 访问控制

随着新型的云计算技术——Inter-Cloud Computing 的日渐成熟,访问控制技术也要逐步地适应 Inter-Cloud.要在实现 Inter-Cloud 的资源信息共享访问基础上提供 Inter-Cloud 之间的相互授权机制,使不同云内的用户可以相互跨云访问对方的资源,从全局实现对云中资源的访问控制管理.因此,云计算环境中的访问控制需要进行 Inter-Cloud 的授权机制.另外,在 Inter-Cloud 之间进行互操作时,Inter-Cloud 之间的访问控制策略可能不一样,可能会发生访问控制的冲突问题,因此需要研究 Inter-Cloud 环境中的一致性访问控制以及相关的冲突检测机制.

5.3 基于信任关系的访问控制技术研究

随着对信任模型研究的深入,云计算系统中的数据提供者、云平台、用户这三者两两之间的信任关系都不同,它们必须通过一个都信任的第三方机构来进行相关密钥、数据的交换和访问控制,如果将信任模型和云计算的访问控制技术相结合,安全性和可管理性都可以得到保障.文献[74,75]涉及到了相关研究,但没有将信任模型与访问控制模型很好地结合在一起,研究有待深入.这部分内容可从以下两点进行研究:

1) 将信任模型集成到传统的访问控制模型中.模型在用户获得角色之前,首先计算该用户的信任值,然后根据信任值决定用户能够获得该角色,即,用户的信任值决定其能否获得对应的权限,这样就能够保证主客体双方的安全性,防止攻击事件的产生.
2) 将信任模型集成到ABE中.在通过ABE机制进行访问控制的时候,可以通过信任值决定数据提供者、云平台、用户的信任关系,如果可信,就可以依托可信强大的云环境来进行复杂密钥管理和加解密计算,既保证了安全性,也充分利用了云计算的计算能力来减轻整个系统的计算负担.

6 结束语

云计算中的访问控制问题是当前安全领域最重要的问题,其研究受到了学术界和工业界的广泛关注,近年来也取得了一定的进展,同时也仍然面临着严峻的挑战.本文研究了云计算环境下访问控制体系框架,从云计算访问控制模型、基于 ABE 密码体制的云计算访问控制、云中多租户及虚拟化访问控制研究这 3 个方面对云计算环境中的访问控制问题进行了全面的综述,调研了目前工业界各类产品的访问控制机制,同时展望了未来重点研究的方向,希望对后面的研究者有所裨益.

最后不得不提的是,云计算中的访问控制问题不仅仅是技术问题,它还涉及标准化、法律法规以及行为准则等很多方面[76].如果没有一个良好的环境和严格的监管模式来保证,访问控制问题将无从谈起.因此,在保证技术发展的基础上,需要学术界、工业界以及相关管理部门共同工作,为创造一个安全的云环境而努力.

致谢 在此,我们向对本文提出宝贵修改意见的评审老师和同行表示衷心的感谢.

References:

[1] Curry S, Darbyshire J, Fisher DW, Hartman B, Herrod S, Kumar V, Martins F, Orrin S, Wolf DE. Infrastructure Security: Getting to the Bottom of Compliance in the Cloud. The Security Division of EMC, 2010.

[2] Kaur PJ, Kaushal S. Security Concerns in Cloud Computing. In: Proc. of the HPAGC 2011. CCIS 169, 2011. 103−112.

[3] Feng DG, Zhang M, Zhang Y, Xu Z. Study on cloud computing security. Ruan Jian Xue Bao/Journal of Software, 2011,22(1): 71−83 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[4] Lin C, Feng FJ, Li JS. Access control in new network environment. Ruan Jian Xue Bao/Journal of Software, 2007,18(4):955−966 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/955.htm [doi: 10.1360/jos180955]

[5] Lampson BW. Protection. In: Proc. of the 15th Princeton Symp. on Information Sciences and System. 1971. 431−443.

[6] Bell DE, Lapadula LJ. Secure Computer Systems: Mathematical Foundations. Vol.1. Bedford: The Mitre Corporation, 1973.

[7] Ferraiolo D, Kuhn DR. Role-Based access control. In: Proc. of the 15th National Computer Security Conf. 1992. 554−563.

[8] Sandhu R, Bhamidipati V, Munawer Q. The ARBAC97 model for role-based administration of roles. ACM Trans. on Information and System Security (TISSEC), 1999,2(1):105−135. [doi: 10.1145/300830.300839]

[9] Sandhu R, Coyne EJ, Feinstein HL, Youman CE. Role-Based access control models. IEEE Computer, 1996,29(2):38−47. [doi: 10.1109/2.485845]

[10] Ferraiolo DF, Sandhu R, Gavrila S. Proposed NIST standard for role-based access control. ACM Trans. on Information and System Security, 2001,4(3):224−274. [doi: 10.1145/501978.501980]

[11] Cantor S, Moreh J, Philpott R, Maler E. Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Open, 2005.

[12] Gary C, Sun M. OASIS Service Provisioning Markup Language (SPML) Versions 2.0. OASIS Open, 2006.

[13] Erik R, Axiomatics AB. OASIS eXtensible Access Control Markup Language (XACML) Versions 3.0. OASIS Open, 2013.

[14] Thomas R, Sandhu R. Task-Based authorization controls (TBAC): A family of models for active and enterprise oriented authorization management. In: Proc. of the 11th IFIP WG11.3 Conf. on Database Security. Lake Tahoe, 1997. 166−181.

[15] Deng JB, Hong F. Task-Based access control model. Ruan Jian Xue Bao/Journal of Software, 2003,14(1):76−82 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/76.htm

[16] Li FH, Su M, Shi GZ, Ma JF. Research status and development trends of access control model. Chinese Journal of Electronics, 2012,40(4):805−813 (in Chinese with English abstract).

[17] Wang XW, Zhao YM. A task-role-based access control model for cloud computing. Computer Engineering, 2012,38(24):9−13 (in Chinese with English abstract).

[18] Huang Y, Li KL. Model of cloud computing oriented T-RBAC. Application Research of Computers, 2013,30(12):3735−3737 (in Chinese with English abstract).

[19] Sun YQ, Meng XX, Liu SJ, Pan P. Flexible workflow incorporated with RBAC. In: Proc. of the 9th Int'l Conf. in Computer Supported Cooperative Work in Design (CSCWD 2005). 2005. 525−534.

[20] Li XF, Feng DG, Chen ZW, Fang ZH. Model for attribute based access control. Journal on Communications, 2008,29(4):90−98 (in Chinese with English abstract).

[21] Ei EM, Thinn TN. The privacy-aware access control system using attribute-and role-based access control in private cloud. In: Proc. of the 2011 4th IEEE IC-BNMT. 2011. 447−451. [doi: 10.1109/ICBNMT.2011.6155974]

[22] Huang JW, David MN, Rakesh B, Jun HH. A framework integrating attribute-based policies into role-based access control. In: Proc. of the SACMAT 2012. 2012. 187−196. [doi: 10.1145/2295136.2295170]

[23] Bertino E, Bonatti P, Ferrari E. TRBAC: A temporal role-based access control model. ACM Trans. on Information and System Security, 2001,4(3):191−223. [doi: 10.1145/501978.501979]

[24] Wang XM, Zhao ZT. Role-Based access control model of temporal object. Acta Electronica Sinica, 2005,33(9):1634−1638 (in Chinese with English abstract).

[25] Park J, Sandhu R. Towards usage control models: Beyond traditional access control. In: Proc. of the 7th ACM Symp. on Access Control Models and Technologies (SACMAT 2002). 2002. 57−64. [doi: 10.1145/507711.507722]

[26] Krautsevich L, Lazouski A, Martinelli F, Yautsiukhin A. Risk-Aware usage decision making in highly dynamic systems. In: Proc. of the 5th Int'l Conf. on Internet Monitoring and Protection. Barcelona: IEEE Computer Society, 2010. 29−34. [doi: 10.1109/ICIMP.2010.13]

[27] Chu XB, Qin Y. A distributed usage control system based on trusted computing. Chinese Journal of Computers, 2010,33(1):93−102 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2010.00093]

[28] Tina T, Mehdi S, Peyman D. A usage control based architecture for cloud environments. In: Proc. of the 2012 IEEE 26th Int'l Parallel and Distributed Processing Symp. on Workshops & PhD Forum. 2012. 1534−1539. [doi: 10.1109/IPDPSW.2012.193]

[29] Lazouski A, Mancini G, Martinelli F, Mori P. Usage control in cloud systems. In: Proc. of the 7th Int'l Conf. for Internet Technology and Secured Trans. 2012. 202−207.

[30] Mounira M, Rached A, Ahmed S. Access control in probative value cloud. In: Proc. of the 8th Int'l Conf. for Internet Technology and Secured Trans. (ICITST 2013). 2013. [doi: 10.1109/ICITST.2013.6750274]

[31] Lin GY, He S, Huang H, Wu JY, Chen W. Access control security model based on behavior in cloud computing environment. Journal on Communications, 2012,33(3):59−66 (in Chinese with English abstract).

[32] Weng CL, Luo Y, Li ML, Lu XD. A BLP-based access control mechanism for the virtual machine system. In: Proc. of the 9th Int'l Conf. for Young Computer Scientists (ICYCS 2008). 2008. [doi: 10.1109/ICYCS.2008.503]

[33] Sahai A, Waters B. Fuzzy identity based encryption. In: Proc. of the Advances in Cryptology, Eurocrypt. LNCS 3494, Springer-Verlag, 2005. 457−473. [doi: 10.1007/11426639_27]

[34] Vipul G, Amit S, Omkant P, Brent W. Attribute-Based encryption for fine-grained access control of encrypted data. In: Proc. of the ACM Conf. on Computer and Communications Security. 2006. 89−98. [doi: 10.1145/1180405.1180418]

[35] Ostrovsky R, Sahai A, Waters B. Attribute-Based encryption with non-monotonic access structures. In: Proc. of the 14th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2007. 1−17. [doi: 10.1145/1315245.1315270]

[36] Attrapadung N, Imai H. Conjunctive broadcast and attribute-based encryption. In: Shacham H, Waters B, eds. Proc. of the Pairing-Based Cryptography—Pairing 2009. Berlin: Springer-Verlag, 2009. 248−265. [doi: 10.1007/978-3-642-03298-1_16]

[37] Zhu Y, Ma D, Hu CJ, Huang D. How to use attribute-based encryption to implement role-based access control in the cloud. In: Proc. of the CloudComputing 2013. 2013. [doi: 10.1145/2484402.2484411]

[38] John B, Amit S, Brent W. Ciphertext-Policy attribute-based encryption, In: Proc. of the IEEE Symp. on Security and Privacy. 2007. 321−334. [doi: 10.1109/SP.2007.11]

[39] Anuchart T, Guang G. OAuth and ABE based authorization in semi-trusted cloud computing. In: Proc. of the DataCloud-SC 2011. 2011. 41−50. [doi: 10.1145/2087522.2087531]

[40] Sun GZ, Dong Y, Li Y. CP-ABE based data access control for cloud storage. Journal on Communications, 2011,32(7):146−152 (in Chinese with English abstract).

[41] Sushmita R, Milos S, Amiya N. Privacy preserving access control with authentication for securing data in clouds. In: Proc. of the 2012 12th IEEE/ACM Int'l Symp. on Cluster, Cloud and Grid Computing. 2012. 556−563. [doi: 10.1109/CCGrid.2012.92]

[42] Liang XH, Cao ZF, Lin H, Shao J. Attribute based proxy re-encryption with delegating capabilities. In: Proc. of the 4th Int'l Symp. on Information, Computer and Communications Security (ASIACCS 2009). New York: ACM Press, 2009. 276−286. [doi: 10.1145/1533057.1533094]

[43] Hong C, Zhang M, Feng DG. AB-ACCS: A cryptographic access control scheme for cloud storage. Journal of Computer Research and Development, 2010,47(Suppl.):259−265 (in Chinese with English abstract).

[44] Pirretti M, Traynor P, McDaniel P, Waters B. Secure attribute-based systems. In: Proc. of the 13th ACM Conf. on Computer and Communications Security (CCS 2006). New York: ACM Press, 2006. 99−112. [doi: 10.1145/1180405.1180419]

[45] Yu SC, Wang C, Ren K, Lou WJ. Attribute based data sharing with attribute revocation. In: Proc. of the 5th Int'l Symp. on Information, Computer and Communications Security (ASIACCS 2010). New York: ACM Press, 2010. 261−270. [doi: 10.1145/1755688.1755720]

[46] Yu SC, Wang C, Ren K, Lou YJ. Achieving secure, scalable, and fine-grained data access control in cloud computing. In: Proc. of the INFOCOM 2010. 2010. 1−9. [doi: 10.1109/INFCOM.2010.5462174]

[47] Chase M. Multi-Authority attribute based encryption. In: Proc. of the 4th Theory of Cryptography Conf. (TCC 2007). 2007. 515−534.

[48] Ruj S, Nayak A, Stojmenovic I. DACC: Distributed access control in clouds. In: Proc. of the 10th IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications. 2011. 91−98. [doi: 10.1109/TrustCom.2011.15]

[49] Yang K, Jia XH. Attribute-Based access control for multi-authority systems in cloud storage. In: Proc. of the 32nd IEEE Int'l Conf. on Distributed Computing Systems. 2012. 536−545. [doi: 10.1109/ICDCS.2012.42]

[50] Yang K, Jia XH, Ren K, Zhang B. DAC-MACS: Effective data access control for multi-authority cloud storage systems. In: Proc. of the 2013 IEEE INFOCOM. 2013. [doi: 10.1109/INFCOM.2013.6567100]

[51] Liu XJ, Xia YJ, Jiang S, Xia FB, Wang YB. Hierarchical attribute-based access control with authentication for outsourced data in cloud computing. In: Proc. of the 2013 12th IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications. 2013. [doi: 10.1109/TrustCom.2013.60]

[52] Meghanathan N. Review of access contorl models for cloud computing. CS & IT-CSCP, 2013. 77−85. [doi: 10.5121/csit.2013.3508]

[53] Hao F, Lakshman TV, Mukherjee S, Song HY. Secure cloud computing with a virtualized network infrastructure. In: Proc. of the 2nd USENIX Conf. on Hot Topics in Cloud Computing. 2010. 1−7.

[54] Factor M, Hadas D, Hamama A, Har'el N, Kolodner EK. Secure logical isolation for multi-tenancy in cloud storage. In: Proc. of the 29th Symp. on Mass Storage Systems and Technologies (MSST). IEEE, 2013. 1−5 [doi: 10.1109/MSST.2013.6558424]

[55] Li XY, Shi Y, Guo Y, Ma W. Multi-Tenancy based access control in cloud. In: Proc. of the 2010 Int'l Conf. on Computational Intelligence and Software Engineering (CiSE). 2010. 1−4 [doi: 10.1109/CISE.2010.5677061]

[56] Almutairi AA, Sarfraz MI, Basalamah S, Aref WG, Ghafoor A. A distributed access control architecture for cloud computing. IEEE Software, 2012,29(2):36−44. [doi: 10.1109/MS.2011.153]

[57] Bo T, Ravi S, Qi L. Multi-Tenancy authorization models for collaborative cloud services. In: Proc. of the Int'l Conf. on Collaboration Technologies and Systems (CTS). 2013. [doi: 10.1109/CTS.2013.6567218]

[58] Yang SJ, Lai PC, Lin J. Design role-based multi-tenancy access control scheme for cloud services. In: Proc. of the 2013 Int'l Symp. on Biometrics and Security Technologies. 2013. 273−279. [doi: 10.1109/ISBAST.2013.48]

[59] Anil K, Moitrayee G, Roman P, Christian C, Robert H. A comparison of secure multi-tenancy architectures for filesystem storage clouds. In: Proc. of the 12th Int'l Middleware Conf. 2011. 1−20. [doi: 10.1007/978-3-642-25821-3_24]

[60] Lucian P, Minlan Y, Steven YK, Sylvia R, Ion S. CloudPolice: Taking access control out of the network. In: Proc. of the Hotnets 2010. 2010. [doi: 10.1145/1868447.1868454]

[61] http://smb.chinabyte.com/443/12276443.shtml

[62] http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingIAMPolicies.html

[63] http://baike.baidu.com/view/1997158.htm

[64] Google. Security Whitepaper: Google Apps Messaging and Collaboration. http://www.chinacloud.cn/show.aspx?id=10858&cid=29

[65] http://developer.baidu.com/wiki/index.php?title=docs

[66] http://www.openstack.org/

[67] http://cloudstack.apache.org/

[68] https://www.eucalyptus.com/

[69] http://www.cnblogs.com/yuki-lau/archive/2013/01/04/2843918.html

[70] Covington MJ, Long W, Srinivasan S, Dey AK, Ahamad M, Abowd GD. Securing context-aware applications using environment roles. In: Proc. of the 6th ACM Symp. on Access Control Models and Technologies. 2001. [doi: 10.1145/373256.373258]

[71] Damiani ML, Bertino E, Catania B, Perlasca P. GEO-RBAC: A spatially aware RBAC. ACM Trans. on Information and System Security, 2007,10(1):1−42 [doi: 10.1145/1210263.1210265]

[72] Bhatti R, Ghafoor A, Bertino E, Joshi JBD. X-GTRBAC: An XMLbased policy specification framework and architecture for enterprise- wide access control. ACM Trans. on Information and System Security, 2005,8(2):187−227. [doi: 10.1145/1065545.1065547]

[73] Zhang H, He YP, Shi ZG. Spatial-Context role-base access control. Science in China (Series E), 2007,37(2):254−271 (in Chinese with English abstract).

[74] Santos N, Gummadi KP, Rodrigues R. Towards trusted cloud computing. In: Proc. of the Workshop on Hot Topics in Cloud Computing. 2009.

[75] Tan ZJ, Tang Z, Li RF, Sallam A, Yang L. Research on trust-based access control model in cloud computing. In: Proc. of the 2011 6th IEEE Joint Int'l Information Technology and Artificial Intelligence Conf. Chongqing, 2011. 339−344. [doi: 10.1109/ITAIC.2011.6030345]

[76] Tim M, Subra K, Shahed L. Cloud Security and Privacy. O'reilly, 2009.

附中文参考文献:

[3] 冯登国,张敏,张妍,徐震.云计算安全研究.软件学报,2011,22(1):71−83. http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[4] 林闯.封富君,李俊山.新型网络环境下的访问控制技术.软件学报,2007,18(4):955−966. http://www.jos.org.cn/1000-9825/18/955.htm [doi: 10.1360/jos180955]

[15] 邓集波,洪帆.基于任务的访问控制模型.软件学报,2003,14(1):76−82. http://www.jos.org.cn/1000-9825/14/76.htm

[16] 李凤华,苏芒,史国振,马建峰.访问控制模型研究进展及发展趋势.电子学报,2012,40(4):805−813.

[17] 王小威,赵一鸣.一种基于任务角色的云计算访问控制模型.计算机工程,2012,38(24):9−13.

[18] 黄毅,李肯立.一种面向云计算的任务-角色访问控制模型.计算机应用研究,2013,30(12):3735−3737.

[20] 李晓峰,冯登国,陈朝武,房子河.基于属性的访问控制模型.通信学报,2008,29(4):90−98.

[24] 王小明,赵宗涛.基于角色的时态对象存取控制模型.电子学报,2005,33(9):1634−1638.

[27] 初晓博,秦宇.一种基于可信计算的分布式使用控制系统.计算机学报,2010,33(1):93−102. [doi: 10.3724/SP.J.1016.2010.00093]

[31] 林果园,贺珊,黄皓,吴吉义,陈伟.基于行为的云计算访问控制安全模型.通信学报,2012,33(3):59−66.

[40] 孙国梓,董宇,李云.基于 CP-ABE 算法的云存储数据访问控制.通信学报,2011,32(7):146−152.

[43] 洪澄,张敏,冯登国.AB-ACCS:一种云存储密文访问控制方法.计算机研究与发展,2010,47(增刊):259−265.

[73] 张宏,贺也平,石志国.一个支持空间上下文的访问控制形式模型.中国科学(E 辑:信息科学),2007,37(2):254−271.

王于丁(1984－),男,河北石家庄人,博士生,主要研究领域为云计算安全.

凌晓(1987－),男,博士生,主要研究领域为云计算.

杨家海(1966－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为计算机网络,网络管理与测量,云计算.

杨洋(1980－),男,博士生,主要研究领域为 SDN 数据中心流量工程.

徐聪(1986－),男,博士生,主要研究领域为云计算性能分析.