基于经纪人的多云访问控制模型研究

赵 鹏[1] 吴礼发[2] 洪 征[1]

(陆军工程大学指挥控制工程学院 南京 210007)[1] (南京邮电大学计算机学院 南京 210023)[2]

摘 要 多云(Multicloud)无需改变提供商的技术方案及运营方式,以独立于提供商的方式自由组合云资源,是一种认可度较高、具有重要推广价值的互联云模型。云经纪人支持向云提供商和云用户提供透明服务,按需组合多个云提供商的资源,降低了跨云协作难度、提供商锁定风险和用户成本开销。然而,云提供商间的访问控制策略的异构性和信任机制的缺乏,极易造成隐私泄露和数据丢失等安全隐患,严重影响了多云的推广应用。文中综合考虑信任、上下文和服务等级协议(SLA)等因素,提出了基于经纪人的多云访问控制模型(MC-ABAC)。首先,构建了多云访问控制模型结构,该结构由虚拟资源管理器(VRM)、访问控制管理器(ACM)和云访问控制经纪人(CACB)等模块组成;其次,设计了多云访问控制模型,该模型定义了主体、资源、环境和操作等,形式化描述了信任、上下文、SLA 和授权策略等,实现了云提供商信任度量和跨云的授权;再次,设计了多云访问控制的工作流程,包括从本地提供商访问多云的工作流程和从 CACB 访问多云的工作流程;最后,利用 CloudSim 4.0 和 OpenAZ 搭建多云访问控制环境,验证该模型的请求成功率和响应时间等可用性指标。实验结果表明,当正常使用且请求数量较大时,该模型的请求成功率比 ABAC 模型提升了 18%左右,且响应时间性能优于 ABAC 模型。

关键词 多云,云经纪人,访问控制,信任管理,服务等级协议,上下文信息

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/jsjkx.190300112

Research on Broker Based Multicloud Access Control Model

ZHAO Peng[1] WU Li-fa[2] HONG Zheng[1]

(College of Command & Control, Army Engineering University of PLA, Nanjing 210007, China)[1]

(School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)[2]

Abstract Multicloud is increasingly accepted by industry and has great promotional value and development potential, since it combines cloud resources in a provider-independent way and there is no need to change the provider's original technology solutions and operation model. Cloud broker provides transparent service for providers and users, composes the resource of cloud providers on demand, and reduces the difficulty of Multicloud collaboration, the risk of vendor lock-in and the cost of cloud user. However, the loss of trust and the heterogeneity of access control policy among cloud providers can easily cause security problems, such as privacy leakage and data loss, and affect the promotion and application of Multicloud seriously. Based on the factors, such as trust, context and SLA, Multicloud access control model (MC-ABAC) was proposed. Firstly, the framework of MC-ABAC is constructed to collaborate in Multicloud environments, which consists of Virtual Resource Manager (VRM), Access Control Manager (ACM) and Cloud Access Control Broker (CACB). Secondly, MC-ABAC is designed to achieve trust measurement of cloud providers and authorization management in Multicloud. This model defines subject, resource, environment and operation, and formalizes trust, context, SLA and authorization. Thirdly, the workflow of MC-ABAC is designed to access the resource of multicloud from local provider and CACB respectively. Finally, the simulation environment of MC-ABAC is built by using CloudSim 4.0 and OpenAZ, and used to verify the availability, such as the success rate and the response time of the request. The results show the request success rate of MC-ABAC is about 18% higher than that of ABAC, and whose average response time is better than that of ABAC, when MC-ABAC is used normally and the number of requests is large.

Keywords Multicloud, Cloud broker, Access control, Trust management, Service level agreement, Context information

---

到稿日期:2019-03-22 返修日期:2019-06-03 本文受国家重点研发计划(2017YFB0802900),南京邮电大学科研项目(NY219004)资助。

赵 鹏(1983-),男,博士生,主要研究方向为网络安全,E-mail:zhpeng0729@163.com;**吴礼发**(1968-),男,教授,博士生导师,主要研究方向为网络安全、软件安全,E-mail:wulifa@njupt.edu.cn(通信作者);**洪 征**(1979-),男,副教授,主要研究方向为网络安全、协议逆向工程。

1 引言

多云经纪服务由第三方经纪人自由选择，组合多个云的服务资源，且无需改变提供商的技术方案和运营方式，是一种认可度较高、具有重要推广价值的互联云模型[1]。多云能够防止提供商锁定，提高数据和服务的容错能力，降低使用成本，缩短服务响应时间，实现资源跨云共享，为用户提供成熟稳定的多样化服务。用户服务和资源存放在多云环境中，增加了数据管理的复杂性，且存在信息安全隐患。由于多云间没有预先建立协议且缺乏协作工具，因此多云系统存在云提供商间缺乏信任、访问控制策略异构、数据存在安全隐患等问题[2]。

多云访问控制能够避免边信道攻击和未授权信息流问题[3]，是实现安全互操作和资源共享的重要技术手段。多云访问控制模型需要满足开放性、动态性、虚拟化与多租户、细粒度、信任与隐私性等特性。Theimer 等[4]提出了分布式环境下访问控制程序委托技术，利用第三方为用户提供访问服务。云服务经纪人[5]是云服务参与者，负责云服务消费者和云服务提供商间的协调工作。Anastasi 等[6]为多云经纪人 Contrail 设计了 UCON 访问控制方案，利用 XACML 实现代理的安全授权决策，但未考虑信任的影响。Sette 等[7]提出了授权策略联盟，允许异构的多云用户定义同构授权策略来实现跨云的访问，但未考虑信任和服务等级协议等。Zheng 等[8]提出了基于信任和信誉的异构访问控制架构，研究了 3 种基于信任和信誉保护云数据的方案，实现了安全可用的云数据访问，但未考虑云间服务等级协议。Ngo 等[9-10]提出了多云联盟的访问控制架构，利用云经纪人实现了信任管理和服务等级协议，但缺乏实验验证。

多云访问控制需要解决策略异构性和云间相互不信任等问题，对此本文提出了基于经纪人的多云访问控制模型(Multicloud Attribute Based Access Control，MC-ABAC)，实现了多云访问控制的高效可用。本文的主要贡献如下：1)构建了基于经纪人的多云访问控制模型结构，该结构主要由虚拟资源管理器(Virtual Resource Manager，VRM)、访问控制管理器(Access Control Manager，ACM)和云访问控制经纪人(Cloud Access Control Broker，CACB)组成；2)描述了多云访问控制模型，该模型对信任、上下文、服务等级协议和授权策略进行了形式化描述；3)设计了多云访问控制工作流程，分别从本地提供商和 CACB 角度描述访问多云资源的工作流程。4)利用 CloudSim 4.0 和 OpenAZ 构建多云访问控制环境，验证了所提多云访问控制模型的有效性。

本文第 2 节介绍了云经纪人和分布式访问控制等相关工作；第 3 节介绍了多云访问控制模型，设计了多云访问控制模型架构，并对模型进行了形式化描述；第 4 节分别介绍了从本地提供商和 CACB 请求多云访问控制的工作流程；第 5 节介绍了系统的实验仿真，验证了多云访问控制模型的可用性和响应时间；最后总结全文。

2 相关工作

2.1 云经纪人

云经纪人将不同云服务聚集起来，形成商品市场，为用户提供服务[11]，并在多云资源配置管理、安全管理、记帐及审计管理、接口兼容技术等[12]领域取得了较多的成果，受到了多云安全领域研究人员的关注。云提供商在服务类型、访问策略和访问接口方面的差异为用户的跨云服务与互操作提出了挑战。NIST 认为云经纪服务是管理云服务的使用、性能和发布，协调云提供商和云用户关系的实体[13]，主要提供服务中介、服务集成和服务仲裁等 3 类服务。Gartner[14]将云服务经纪人定义为一种 IT 角色和业务模型，其代表消费者为多个云提供增值服务。云经纪人在安全领域的应用也非常广泛。Thomas 等[15]提出了基于代理的云经纪人架构，实现了分布式访问控制。Pramod 等[16]提出了经纪人架构模型，通过获取安全信息证据为云服务提供商建立了信誉框架。Halabi 等[17]提出了基于经纪人的框架来管理云安全 SLA。Liu 等[18]利用 CASB 实现了加密数据的搜索和共享。

2.2 分布式访问控制

分布式访问控制首先需要对用户的身份进行认证，然后对控制策略进行选用和管理，最后对非法用户和越权操作进行管理[19]。Almutairi 等[3]提出了一种通用的分布式访问控制架构，该架构融合了联盟、松耦合和自组织等协作方式，由虚拟资源管理器、分布式访问控制模块和服务等级协议等部件组成，满足多租户与虚拟化、分散管理、安全协作、身份联盟、约束规范等授权需求。Tolone 等[20]对协作系统环境下的访问控制模型进行研究，提出了协作系统访问控制的 8 个需求和 11 个评估指标。

为了解决多云异构性和安全互操作性，Demchenko 等[10]提出了一种基于经纪人的访问控制模型，解决了异构多云基础设施服务间的互操作和合成问题。Rizvi 等[21]提出了一种半分布式访问控制架构来实现多云协同工作。Anastasi 等[6]利用 UCON 模型实现互联云经纪服务系统 Contrail，利用 XACML 策略实现授权决策。Luo 等[22]在 OSM 项目中开发了最小相关的访问控制架构，使得 OpenStack 能加载不同访问控制模型。Ngo 等[9]提出了多云异构环境下的多租户 ABAC 模型，实现了云基础设施架构 GEYSERS 的动态访问控制。Sette 等[7]提出了异构多云环境下的授权策略联盟(APF)方案，实现了云访问控制策略与 DNF 策略的相互转换。Hilia 等[23]提出了基于语义的访问控制架构，实现了协作云环境下的互操作。Alansari 等[24]提出了云联盟环境下的新型身份和访问管理系统，利用区块链技术和 SGX 信任硬件保证策略评估过程的完整性。Li 等[25]提出了访问控制代理来实现端到端的信息机密性。为保证多云协作中的可用性，文献[26]将 OSAC 扩展至 ABAC，利用 PM 组件及概念在 OpenStack 中进行实现，增加了访问控制的灵活性。John 等[27]认为多云协作环境需要细粒度的访问控制机制，基于属性的访问控制更适合多云协作环境。

3 多云访问控制模型

本节主要介绍多云访问控制模型的结构和形式化描述。

3.1 模型结构

多云的参与者包括云用户(Cloud Consumer，CC)、云经纪人(Cloud Broker，CB)和云提供商(Cloud Provider，CP)。CC 是 CP 资源或服务的请求者；CB 处理 CC 的访问请求并为

CC 分配云资源,实现访问请求验证、授权决策和资源分配;CP 为 CC 的访问请求提供服务或资源,当收到 CC 的访问请求时,CP 对用户身份进行认证并验证访问权限,避免了非法或未授权用户的访问。CB 是负责管理云服务的使用、性能和交付以及协商 CP 和 CC 之间关系的实体,具备信任管理、用户信息管理、请求解析和身份管理等功能。

多云访问控制模型主要由 CACB,VRM 和 ACM 等构成,如图 1 所示。CACB 是该架构的核心组件,主要实现多云资源的管理、分配和共享。VRM 和 ACM 驻留在 CP 的各服务层。VRM 管理本地的云资源,根据请求为用户分配资源。ACM 执行本地的访问控制策略,实现本地的权限管理。当本地资源不足时,ACM 将请求转发至 CACB,实现跨云访问。

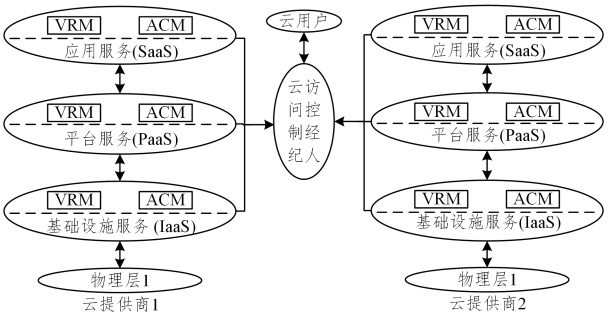

图 1　多云访问控制模型架构

Fig. 1　MC-ABAC architecture

3.1.1　虚拟资源管理器

VRM 部署于 CP 的各服务层,负责提供和发布虚拟资源,监视资源的分配和回收,并保证服务的合规性和可用性,使之满足云虚拟资源的异构性和细粒度要求。当用户请求资源时,VRM 在本地虚拟资源列表中查找合适的云资源,根据访问控制策略为用户分配资源;如果本地资源不能满足用户请求,VRM 将该请求转发给 CACB 并请求远程服务。

3.1.2　访问控制管理器

ACM 部署于 CP 的各服务层,验证用户身份和授权请求,并实现跨云访问。该模块包括访问控制网关(Access Gateway,AG)、策略决策点(Policy Decision Point,PDP)、策略执行点(Policy Enforcement Point,PEP)、策略管理点(Policy Administration Point,PAP)和属性权威(Attribute Authority,AA)等,如图 2 所示。AG 负责接收用户访问请求,解析并触发授权请求;PDP 是授权决策实体,依据访问控制策略和属性实现访问控制决策;PEP 是执行访问控制实体,将原始访问控制请求(origiNal Access Request,NAR)转换为基于属性的访问请求(Attribute Access Request,AAR),根据决策结果执行允许或拒绝操作;PAP 是产生和维护安全访问策略的实体;AA 是存储主体、资源、环境和行为属性信息的实体。

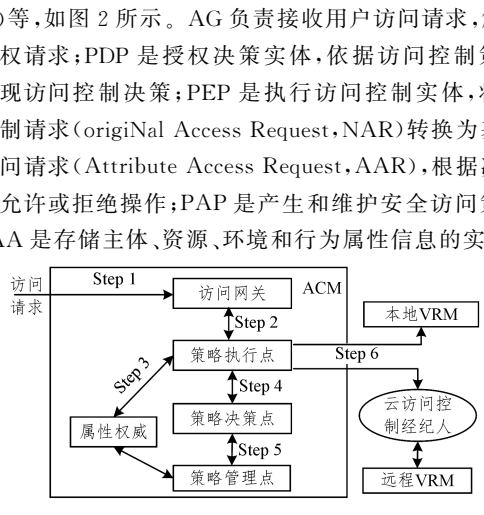

图 2　访问控制管理器结构

Fig. 2　ACM architecture

3.1.3　云访问控制经纪人

CACB 是多云资源使用、性能评估和服务投递的实体,帮助用户比较、选择和访问多云资源,通过开发和使用统一的接口来实现跨云互操作,包括身份提供商(Identity Provider,IdP)、PEP、PDP、策略管理器(Policy Manager,PM)、服务等级协议管理器(Service Level Agreement Manager,SLAM)、信任管理器(Trust Manager,TM)、上下文管理器(Context Manager,CM)和资源管理器(Resource Manager,RM)等,如图 3 所示。CACB 综合 SLA、信任度和上下文等属性信息,使用属性映射、策略集成和冲突消解等技术手段来实现跨云访问决策。

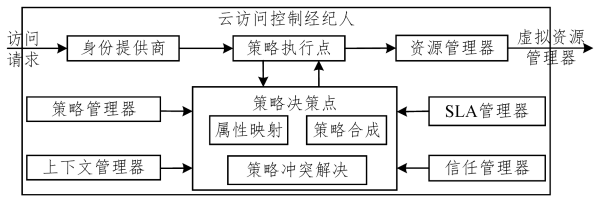

图 3　云访问控制经纪人结构

Fig. 3　CACB architecture

PM 负责提供主体、客体和环境的属性信息,分别向 CM,RM 和 SLAM 提供主体、客体和环境等属性信息,由策略管理工具、策略库和系统配置文件 3 个模块组成。策略管理工具是策略维护的工具,负责将用户制定的策略处理后存储到策略库,以供策略决策模块调用,管理员还可通过策略管理工具配置策略文件;策略库主要用于存储形式化的访问控制策略,以便于策略决策模块调用策略信息;系统配置文件主要用于系统配置,如设置策略合并算法和缺省授权。

RM 是多云资源管理的实体,负责汇集、选择、调度和分配多云的各类资源,采集 CP 的硬件、镜像、网络和存储等资源运行状态信息。当完成用户身份验证和访问授权后,RM 为用户选择并分配合适的云资源。访问权限随着用户、资源和环境等属性调整而动态变化,RM 也随着访问权限的动态变化而实时调整资源的大小、位置和操作。多云资源管理和访问授权方式使得多云具有可扩展性、动态性和灵活性。

TM 能够根据用户行为与 CP 的服务记录评估 CC 与 CP 的信任度,信任值可以由直接信任度、间接信任度和综合信任度综合计算获得。在多云环境下,TM 能够根据 SLA 监视、计算其满意程度,并利用信任评估模型对 CP 进行信任评估,实时更新信任值。

CC 访问云服务时,IdP 需要对 CC 的身份进行认证,防止非法用户的恶意攻击。通过认证后,IdP 保存用户标识,利用 SAML 协议与标识服务器进行交互,避免重复登录和验证,从而实现单点登录。在多云环境下,各 CP 与 CC 间共享用户身份信息,实现了 CC 在各 CP 间的安全互操作。

PEP 将 NAR 转换为 AAR,根据访问策略执行判断结果,允许或拒绝用户请求。

PDP 依据访问控制策略及实体属性进行访问决策,实现跨云的属性映射、访问控制策略合成及冲突解决等功能。属性映射是将多云实体属性转化成标准的属性描述语言,并保存其映射关系,利用主体、客体、环境和信任度等属性进行授权决策;访问控制策略合成主要解决多云访问控制策略的异构问题,通过访问控制策略合成来实现跨云资源的共享或协

作;策略冲突解决模块负责多云访问控制策略合成过程中冲突策略的检测和消解,使得合成的访问决策满足安全性要求。

SLAM 主要实现 SLA 协商、管理和监视等功能。SLA 协商确定 CP 的服务等级,CC 通过 SLA 协商获得 SLA 验证、审计及过程信息,保证 CP 为 CC 提供的服务满足 SLA 要求。SLA 管理功能负责变更服务部署和调整资源分配,终止 CP 违反 SLA 的行为。SLA 监控功能收集 CC 和 CP 交互的性能参数,监控 CC 端服务的行为和性能,验证服务是否满足 SLA 的合规性。

3.2 模型的描述

MC-ABAC 是基于 ABAC 构建的多云安全互操作的访问控制模型,能够根据主体属性、客体属性、环境属性、信任度构造策略集,拒绝或允许主体对客体的操作。属性是 ABAC 策略授权判断的基础和依据,访问请求满足访问控制策略规定的属性条件即可获得策略规定的访问权限。本节将对主体、资源、行为、环境和信任度等属性进行形式化描述。

定义 1 属性是表示实体特征的变量,令 a 表示属性,$A=\{a_1,a_2,\cdots,a_n\}$表示含有 n 个属性的集合,主要包括主体属性、客体属性和环境属性等。属性由三元组 $a=\langle name, value, type\rangle$表示。

定义 2 主体是发起资源访问请求的实体,主要包括提供商、租户或用户,$S=\{s_k\mid 1\leqslant k\leqslant m\}$表示 m 个主体集合;主体属性表示主体具备的特征,包括标识、名称和组织等,$SA=\{a_i^u\mid 1\leqslant i\leqslant m\}$表示 m 个主体属性集合。$V_{a_i^u}=\{v_{ij}^u\mid 1\leqslant j\leqslant c_i^u, c_i^u\in Z^+\}\cup\{\text{NULL}\}$表示用户属性 a_i^u 值集,$\forall a_i^u, 1\leqslant i\leqslant m$。

定义 3 资源是主体要求访问的实体,利用标识属性表示,可处于空闲、保留和发布状态,$R=\{r_k\mid 1\leqslant k\leqslant l\}$表示 l 个资源集合;资源属性表示资源具备的特征,$RA=\{a_i^r\mid 1\leqslant i\leqslant l\}$表示 l 个主体属性集合。$V_{a_i^r}=\{v_{ij}^r\mid 1\leqslant j\leqslant c_i^r, c_i^r\in Z^+\}\cup\{\text{NULL}\}$表示资源属性 a_i^r 值集,$\forall a_i^r, 1\leqslant i\leqslant l$。

定义 4 行为表示主体对资源执行的操作类型,主要包括读、写、编辑、删除、拷贝、执行和修改等。行为属性集表示为 $OP=\{op_1,op_2,\cdots,op_m\}, i\in[1,n]$。

定义 5 环境表示主体请求访问客体的环境特征,主要包含当前时间、主体位置和系统安全等级等。环境属性集定义为 $EA=\{ea_1,ea_2,\cdots,ea_k\}$,其中 $i\in[1,k]$。

SLA 是 CC 和 CP 之间签订的保证服务质量的协议,CP 按照 SLA 标准为 CC 提供服务。云计算的 SLA 度量指标主要包括可靠性、可用性、相应时间和服务性能等。譬如,IaaS 的度量指标包括 CPU 能力、内存大小、启动时间、存储空间、扩展容量、扩展时间和响应时间等。

定义 6 CP 的 SLA 量化指标的形式化定义为 $SLA=\{SLA_1,SLA_2,\cdots,SLA_t\}$,其中 $i\in[1,t]$。文献[28]利用满意度量化 SLA 指标,过程如下。

利用 $AMV_{p_i^t}^{t-1}$ 表示参数 p_i 在 $t-1$ 时刻的平均值,在 t 时刻参数 p_i 的平均值如式(1)所示:

$$AMV_{p_i^t}=\frac{AMV_{p_i^t}^{t-1}+CMV_{p_i^t}}{n_i^{t-1}+1} \tag{1}$$

其中,$CMV_{p_i^t}$ 是 t 时刻参数 p_i 的瞬时值,n_i^{t-1} 是截止 $t-1$ 时刻参数 p_i 的监视的数量。

满意度是指主体对客体进行访问后,主体节点根据本次交互的服务质量做出的评价。满意度表示参数的平均监控值 $AMV_{p_i^t}$ 与 SLA 值的比,度量公式如式(2)所示:

$$C_{p_i^t}=\begin{cases}\dfrac{AMV_{p_i^t}}{SLA_{p_i}}, & AMV_{p_i^t}<SLA_{p_i}\\ 1, & AMV_{p_i^t}\geqslant SLA_{p_i}\end{cases} \tag{2}$$

其中,SLA_i 表示参数 p_i 的协议值。将监视值归一化为[0,1],如果 $AMV_{p_i^t}$ 大于或等于 SLA_{p_i},则 $C_{p_i^t}$ 的值为 1,表示合规度最大。

信任是主体使用信任模型预测客体服务能力的行为。根据来源,可将信任分为直接信任和推荐信任,满意度取值范围为[0,1],0 表示很不满意,1 表示很满意。

定义 7 信任度表示主体节点对目标节点的服务能力预期判断,信任度受到 SLA 满意度的影响,云经纪人评价 CP 服务能力的信任度的取值范围为[0,1],0 表示绝对不信任,1 表示绝对信任。由文献[29]可知,信任度主要包括直接信任度、间接信任度和综合信任度。

直接信任是节点根据本地的数据做出判断的行为,A 对 B 直接信任的信任度记为 $DT(A\rightarrow B)$,计算式如式(3)所示:

$$DT(A\rightarrow B)=\begin{cases}\sum\limits_{i=1}^{dn}\dfrac{cr_i}{\sum\limits_{j=1}^{dn}cr_j}sat_i, & dn>0\\ 0.5, & dn=0\end{cases} \tag{3}$$

当没有历史记录时,信任度取 0.5,表示既非“信任”也非“不信任”。

推荐信任是节点综合多个其他节点的直接信任做出判断的行为,A 对 B 推荐信任度记为 $RT(A\rightarrow B)$,计算式如式(4)所示:

$$RT(A\rightarrow B)=\sum_{i=1}^{m}\frac{rc_i}{\sum\limits_{j=1}^{m}rc_j}rdt_i \tag{4}$$

综合信任由直接信任和推荐信任构成,如式(5)所示:

$$T(A\rightarrow B)=\alpha DT(A\rightarrow B)+(1-\alpha)RT(A\rightarrow B) \tag{5}$$

其中,α 表示直接信任权重。

上下文信息用于表征实体和服务之间交互相关的所有信息,主要包括时间、地点、活动、关系和个性等 5 个基本类型。多云访问控制的上下文信息主要包括主体、客体、环境、操作和信任等类型,形式化定义如下。

定义 8 多云的上下文信息的定义如式(6)所示:

$$\begin{aligned}C&=SA\times RA\times EA\times OP\times T\\&=\{(sa_i,ra_j,ea_k,op_n,t_m)\mid sa_i\in SA, ra_j\in RA,\\&\quad ea_k\in EA, op_n\in OP, t_m\in T\}\end{aligned} \tag{6}$$

其中,SA 表示主体属性集,RA 表示资源属性集,EA 表示环境属性集,OP 表示操作属性集,T 表示信任度。

定义 9 用户-用户属性分配关系 $SSA=\{(s_k:\langle a_1^s=x_1, a_2^s=x_2,\cdots,a_n^s=x_n\rangle)\mid x_i\in V_{a_i^s}, 1\leqslant k\leqslant m, 1\leqslant i\leqslant n\}$将属性-值对与用户关联起来,而资源-资源属性分配关系 $RRA=\{(r_k:\langle a_1^r=y_1, a_2^r=y_2,\cdots,a_q^r=y_q\rangle)\mid y_i\in V_{a_i^r}, 1\leqslant k\leqslant p, 1\leqslant i\leqslant q\}$将属性-值对与资源关联起来。

定义 10 授权请求 q 表示主体 S 在上下文 C 下请求访问资源 R 的属性集合。请求集 Q 定义为 $Q=S\times R\times C=\{(s_i,r_j,c_k)\mid s_i\in S, r_j\in R, c_k\in E\}$。

定义 11 基于属性的策略可使用策略描述语言表示,策

略包括授权请求 Q、决策域 D 以及映射函数 f。映射函数 f 表示为 $f:Q\rightarrow D$。其中,决策集表示为 $D=\{\text{Permit},\text{Deny},\text{NotApplicable},\text{Conflict}\}$。

定义 12　多云由多个 CP 协同工作,各 CP 表示物理相对独立的安全域,具有独立访问控制策略。CP 集合表示为 $CP=\{CP_1,CP_2,\cdots,CP_n\}$,其中 CP_i 表示第 i 个 CP,各个 CP 元素可利用 CP 名称作前缀来表示。

定义 13　如果将 ABAC 作为多云环境下的访问控制模型,访问控制模型定义为元组$\langle S,SA,SSA,R,RA,RRA,OP,P\rangle$。访问关系 AR 表示 CP 间允许或拒绝的访问,$AR\subseteq S\times R\times OP\times D$。安全许可规则仅允许合法访问,非安全许可规则则允许合法访问和非法访问。跨云规则表示主体 S 属于 CP_i,而资源-操作对$\langle R,OP\rangle$属于 CP_j。

例如,从 CP_1 到 CP_2 的跨域规则定义为:

$$r_i=[W,op,D] \tag{7}$$

$$W=\langle CP_1.a_1^s=x_1,CP_1.a_2^s=x_2,\cdots,CP_1.a_n^s=x_n\rangle,\ \langle CP_2.a_1^r=y_1,CP_1.a_2^r=y_2,\cdots,CP_1.a_m^r=y_m\rangle \tag{8}$$

$$D=\{\text{Permit},\text{Deny},\text{NotApplicable},\text{Conflict}\} \tag{9}$$

4　多云访问控制的工作流程

用户请求多云服务有两种方式:1)用户向本地 CP 请求云服务,当本地资源不足时,向 CACB 转发资源请求,由 CACB 选择满足用户请求的多云资源;2)用户向 CACB 请求多云服务,CACB 选择多个 CP 中满足用户请求的资源。这两种服务请求方式互为补充,当 CACB 不能提供服务时,用户可直接向提供商发起访问请求。

4.1　从本地提供商请求多云服务

从本地 CP 发起访问请求时,访问请求首先进入本地 CP 的 AG,然后 ACM 将 NAR 转换成 AAR,并判断本地 CP 能否为用户提供云服务,如果能够满足访问请求,则由本地 CP 提供云服务;否则将访问请求转发至 CACB,选择远程 CP 资源,如图 4 所示。具体执行流程如下:

Step1　CC 访问云资源时,发送访问凭证和请求到 AG。

Step2　AG 收到访问请求后,分离访问凭证和访问请求信息,并向 IdP 提交身份验证申请。

Step3　IdP 提取访问凭证,调用本地凭证库对访问凭证进行评估,如果访问凭证未通过身份认证机构的评估,则 IdP 将认证结果返回给 AG 和用户;否则将 NAR 转发至本地 ACM 进行访问决策。决策过程如下:

1)PEP 利用 AA 将收到的 NAR 转化为 AAR,并将 AAR 传递至 PDP。AAR 由主体、资源、环境和行为等属性值对组成,描述了属性为 SA 的主体在属性为 EA 的环境下对资源为 RA 的资源进行属性为 OA 的操作。

2)根据 AAR 和 AA 中的属性,PDP 向 PAP 发送策略匹配请求,查找并判断 AAR 请求的策略集。

3)PDP 利用策略集对 AAR 请求进行评估,利用策略合成算法对策略评估结果进行合成,生成策略集对 AAR 的评估结果,并将结果返回给 PEP。

4)PEP 判定本地 VRM 能否满足访问请求,如果本地 VRM 能满足访问请求,则本地 VRM 为用户分配资源;否则将访问请求转发至 CACB。

5)CACB 的 PEP 收到访问请求后,CACB 的 PEP 将请求转发至 CACB 的 PDP,CACB 的 PDP 根据 PM,SLAM,TM,CM 判定访问请求决策结果,并将结果传至 CACB 的 PEP;如果允许访问,则由 RM 为用户分配多云资源,并将资源分配请求转发至远程的 CP,否则将结果返回给本地 PDP。

Step4　远程的 PEP 将判定结果返回给 CC。

Step5　CC 根据判定结果执行访问操作。

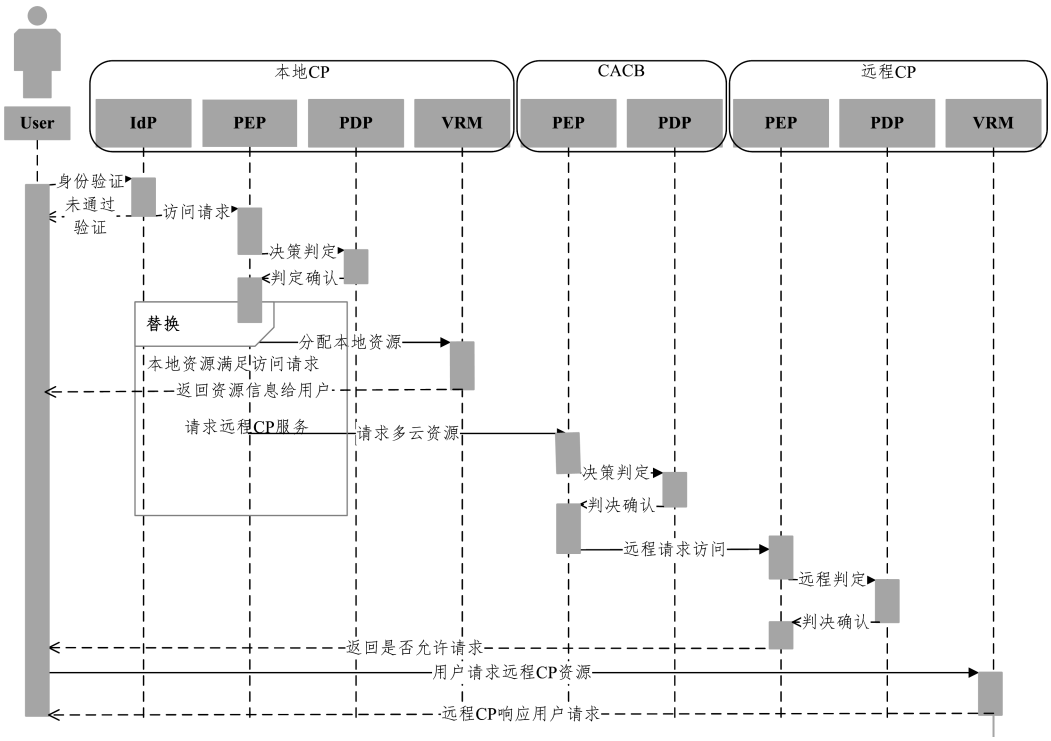

图 4　从本地请求多云工作的流程

Fig. 4　Request workflow from local CP

4.2 从 CACB 请求多云服务

CC 从 CACB 请求多云服务时，CACB 内的 IdP 对用户身份进行认证，RM 选择多云资源，TM，SLAM，PM，CM 判断用户是否具备授权条件，如图 5 所示。具体执行流程如下：

Step1 CC 向 CACB 提出访问请求时，发送访问凭证和请求到 CACB。

Step2 CACB 收到访问凭证和请求后，CACB_IDP 对用户身份进行验证。如果验证通过，则执行 Step3；否则给用户返回身份认证失败应答。

Step3 CACB_PEP 利用 CACBP_AA 中存储的属性，将 NAR 转化为 AAR，并将其传递至 CACB_PDP。

Step4 根据 AAR 和 CACB_AA 中的属性，CACB_PDP 向 CACB_PAP 发送策略匹配请求，CACB_PAP 在策略库中查找匹配目标的策略集。如果找到匹配的策略集，则将该策略集返回 CACB_PDP 进行判定。

Step5 CACB_PDP 根据 PM，SLAM，TM，CM 判定访问请求决策结果，并将结果传至 CACB_PEP。如果允许访问，则 RM 为用户分配多云资源，并将资源分配请求转发至远程的 CP，跳转至 Step6；否则将结果返回用户。

Step6 CACB_PDP 调用策略集对访问请求进行评估，并使用策略合成算法对策略评估结果进行合成，生成决策结果，并将结果返回给 CP_PEP。

Step7 CP_PEP 判定 CP_VRM 能否满足访问请求，如果本地能满足访问请求，则由 CP_VRM 为用户分配资源，并保障云服务，否则将访问请求转发至 CACB。

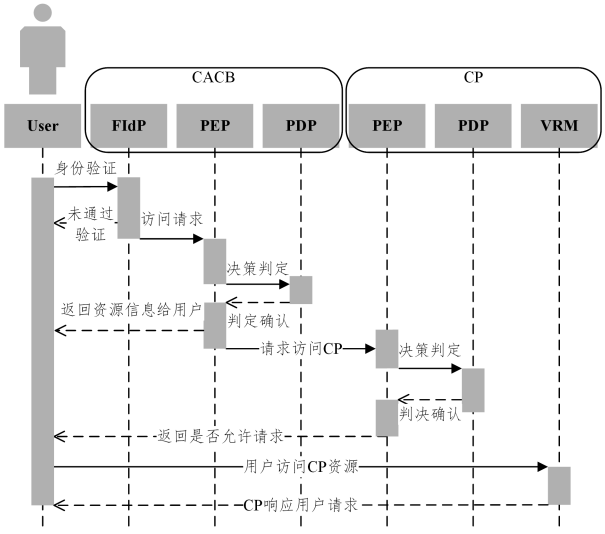

图 5 从 CACB 请求多云服务的流程

Fig. 5 Request workflow from CACB

5 实验及分析

在 MacBook Pro 计算机上开展实验来验证 MC-ABAC 模型的有效性，处理器为 2.6GHz Intel Core i5，内存为 8GB，操作系统为 MacOS High Sierra。利用 CloudSim 4.0 和 OpenAZ 搭建多云访问控制环境。CloudSim 4.0 是墨尔本大学开发的云计算仿真软件，支持云基础设施的建模与仿真。利用 DataCenter 构建多个 CP，利用 DatacenterBroker 构建 CACB，ACM 和 VRM，搭建了多云访问控制模型的结构。OpenAZ 是开源 XACML 软件，用于开发 ABAC 的工具，实现了多云访问控制的 PDP，PAP 和 PEP 等。MyEclipse 2017 CI 8 和 JDK1.8.0 是模型的开发环境。在该环境下，创建 10 个 CP 和 1 个 CACB，从请求成功率和平均响应时间两方面来验证所提模型的有效性，并与 ABAC 模型进行对比。

为了验证 MC-ABAC 模型在多云环境下访问请求的成功率，模拟用户从 CACB 分别发起 100 和 200 个访问请求，访问请求的属性随机生成，对多云环境进行了 10 轮访问请求，统计访问请求的成功率，如图 6 所示。该结果表明：当多云使用 MC-ABAC 模型时，第 1 轮访问请求的成功率为 50%左右，随着实验的进行，请求成功率逐渐增加并稳定地保持在 85%左右；当多云使用 ABAC 模型时，请求成功率基本保持在 67%左右。因此，MC-ABAC 模型在长期运行中的成功率相比 ABAC 模型提高了大约 18%，其原因是 MC-ABAC 模型能够根据用户的请求选择合适的云资源为访问请求提供服务，保证了访问具备较高的成功率。

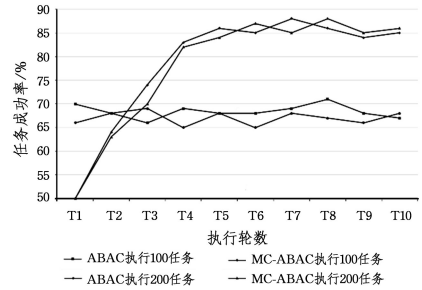

图 6 多云请求的成功率

Fig. 6 Request success rate of multicloud

为了验证 MC-ABAC 模型和 ABAC 模型在多云环境下访问请求的平均响应时间，模拟用户分别从本地提供商和 CACB 请求多云资源，结果如图 7 所示。

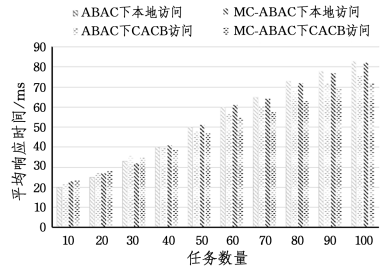

图 7 多云请求的平均响应时间

Fig. 7 Request average response time of Multicloud

该实验结果表明：当请求数量较少时，与 ABAC 模型相比，MC-ABAC 模型的平均响应时间略长；随着请求数量的增加，在部署 MC-ABAC 模型的多云环境下，从本地提供商和 CACB 发起的访问请求的平均响应时间均显著减少，这主要是由于 MC-ABAC 模型在云资源分配时需要综合考虑多种属性，增加了访问请求的响应时间，但随着访问数量的增加，MC-ABAC 模型在处理多任务时的优势逐渐显现。从本地提供商和 CACB 访问多云的角度看，当请求数量少时，从本地提供商和 CACB 请求多云的平均响应时间的差别不大，随着访问请求数量的增加，从 CACB 访问多云资源比从本地提供商请求多云资源的平均响应时间明显缩短，这主要是由于访问任务数量增加后，本地提供商需要通过 CACB 请求多云资源造成的访问时间增加。因此，在 MC-ABAC 模型下访问的

请求数量越大,从 CACB 请求多云资源的平均响应时间的优势就越明显。

综上可知,在用户数量大的多云环境下,MC-ABAC 模型能够显著地提高用户访问多云的成功率和平均响应时间,较好地解决了多云访问控制的需求。

结束语　本文重点研究了多云的访问控制技术,提出了基于经纪人的多云访问控制模型,综合考虑了多云环境下的 SLA、信任、上下文等因素,设计了多云访问控制模型的结构,包括 VRM,ACM 和 CACB,并对该模型进行了形式化描述,设计了从本地提供商和 CACB 请求多云资源的工作流程,最后在 CloudSim 4.0 和 OpenAZ 搭建的模拟环境下验证了 MC-ABAC 模型的有效性。未来将对多云环境下的访问控制策略合成、策略冲突解决及属性加密技术进行研究。

参 考 文 献

[1] PETCU D. Multi-Cloud:expectations and current approaches [C]// International Workshop on Multi-Cloud Applications and Federated Clouds. ACM,2013:1-6.

[2] SINGHAL M,CHANDRASEKHAR S,GE T,et al. Collaboration in Multicloud Computing Environments: Framework and Security Issues[J]. Computer,2013,46(2):76-84.

[3] ALMUTAIRI A A,SARFRAZ M I,BASALAMAH S,et al. A Distributed Access Control Architecture for Cloud Computing [J]. IEEE Software,2012,29(2):36-44.

[4] THEIMER M M,NICHOLS D A,TERRY D B. Delegation through access control programs[C]// International Conference on Distributed Computing Systems. IEEE,1992:529-536.

[5] GUZEK M,GNIEWEK A,BOUVRY P,et al. Cloud Brokering: Current Practices and Upcoming Challenges[J]. IEEE Cloud Computing,2015,2(2):40-47.

[6] ANASTASI G F,CARLINI E,COPPOLA M,et al. Usage Control in Cloud Federations[C]// IEEE International Conference on Cloud Engineering. IEEE,2014:141-146.

[7] SETTE I S,CHADWICK D W,FERRAZ C A G. Authorization Policy Federation in Heterogeneous Multicloud Environments [J]. IEEE Cloud Computing,2017,4(4):38-47.

[8] ZHENG Y,LI X,KANTOLA R. Heterogeneous Data Access Control Based on Trust and Reputation in Mobile Cloud Computing[M]// Advances in Mobile Cloud Computing and Big Data in the 5G Era. Springer International Publishing,2017.

[9] NGO C,DEMCHENKO Y,LAAT C D. Multi-tenant attribute-based access control for cloud infrastructure services[J]. Journal of Information Security and Applications,2016,27-28:65-84.

[10] DEMCHENKO Y,NGO C,LAAT C D,et al. Federated Access Control in Heterogeneous Intercloud Environment:Basic Models and Architecture Patterns[C]// IEEE International Conference on Cloud Engineering. IEEE,2014:439-445.

[11] MEI J,LI K,TONG Z,et al. Profit Maximization for Cloud Brokers in Cloud Computing[J]. IEEE Transactions on Parallel & Distributed Systems,2018,30(1):190-203.

[12] FOWLEY F,PAHL C,JAMSHIDI P,et al. A Classification and Comparison Framework for Cloud Service Brokerage Architectures[J]. IEEE Transactions on Cloud Computing,2016,6(2):358-371.

[13] HOGAN M D,LIU F,SOKOL A W,et al. NIST Cloud Computing Standards Roadmap[R]. NIST Special Publication,2011,35.

[14] GUZEK M,GNIEWEK A,BOUVRY P,et al. Cloud Brokering: Current Practices and Upcoming Challenges[J]. IEEE Cloud Computing,2015,2(2):40-47.

[15] THOMAS M V. Agent-Based Cloud Broker Architecture for Distributed Access Control in the Inter-Cloud Environments[J]. International Journal of Information Processing,2014,8(1):107-123.

[16] PAWAR P S,NAIR S K,ELMOUSSA F,et al. Opinion Model Based Security Reputation Enabling Cloud Broker Architecture [C]// International Conference on Cloud Computing. Springer,2012:103-113.

[17] HALABI T,BELLAICHE M. A broker-based framework for standardization and management of cloud security-SLAs[J]. Computers & Security,2018,75(6):59-71.

[18] LIU C,WANG G,HAN P,et al. A Cloud Access Security Broker based approach for encrypted data search and sharing[C]// International Conference on Computing. Networking and Communications. IEEE,2017:422-426.

[19] AI H. Distributed access control[J]. Computer Engineering and Design,2007,28(21):5110-5111.

[20] TOLONE W,AHN G J,PAI T,et al. Access control in collaborative systems[J]. Acm Computing Surveys,2005,37(1):29-41.

[21] RIZVI S,MITCHELL J. A Semi-distributed Access Control Management Scheme for Securing Cloud Environment[C]// IEEE International Conference on Cloud Computing. IEEE,2015:501-507.

[22] LUO Y,LUO W,TIAN P,et al. OpenStack Security Modules:A Least-Invasive Access Control Framework for the Cloud[C]// IEEE International Conference on Cloud Computing. IEEE,2017:51-58.

[23] HILIA M,CHIBANI A,WINTER T,et al. Semantic Based Authorization Framework For Multi-Domain Collaborative Cloud Environments[J]. Procedia Computer Science,2017,109:718-724.

[24] ALANSARI S,PACI F,MARGHERI A,et al. Privacy-Preserving Access Control in Cloud Federations[C]// IEEE International Conference on Cloud Computing. IEEE,2017:757-760.

[25] LI F,LUO B,LIU P,et al. In-broker Access Control: Towards Efficient End-to-End Performance of Information Brokerage Systems[C]// IEEE International Conference on Sensor Networks,Ubiquitous,and Trustworthy Computing. IEEE,2006:252-259.

[26] BHATT S,PATWA F,SANDHU R. An Attribute-Based Access Control Extension for OpenStack and Its Enforcement Utilizing the Policy Machine[C]// IEEE International Conference on Collaboration and Internet Computing. IEEE,2017:37-45.

[27] JOHN J C,SURAL S,GUPTA A. Authorization Management in Multi-cloud Collaboration Using Attribute-Based Access Control[C]// International Symposium on Parallel and Distributed Computing. IEEE,2017:190-195.

[28] SINGH S,SIDHU J. Compliance-based Multi-dimensional Trust Evaluation System for determining trustworthiness of Cloud Service Providers[J]. Future Generation Computer Systems,2017,67:109-132.

[29] YOU J,SHANG J L,XU S K,et al Distributed Dynamic Trust Management Model b ased on Trust Reliability[J]. Journal of Software,2017,28(9):2354-2369.