P_FACSM:PaaS 平台下公平的访问控制安全模型*

李 敏[1,2], 秦志光[1]
(1. 电子科技大学 计算机与工程学院, 成都 611731; 2. 四川师范大学 计算机科学学院, 成都 610101)

摘 要: 针对 PaaS(平台即服务)的安全需求,设计了 PaaS 下公平的访问控制安全模型(P_ FACSM)。该模型以 ABAC(基于行为的访问控制)为基础,引入公平化 QoS(服务质量)作为环境约束,并结合 OAuth(开放的授权)协议进行授权。P_ FACSM 不仅能保护 PaaS 中数据的完整性和保密性,也能最大化公平的保障平台访问者的 QoS,并能保护终端用户的账户隐私。经理论分析及相关项目中的实际应用表明,该模型在安全性保障及时间效率上都能到达较好效果。

关键词: 平台即服务; 基于行为的访问控制; 服务质量; 开放的授权; 账户隐私
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2013)01-0256-05
doi:10.3969/j.issn.1001-3695.2013.01.066

P_FACSM:fair access control safe model for PaaS

LI Min[1,2], QIN Zhi-guang[1]
(1. *School of Computer Science & Engineering*, *University of Electronic Science & Technology of China*, *Chengdu* 611731, *China*; 2. *College of Computer Science*, *Sichuan Normal University*, *Chengdu* 610101, *China*)

Abstract: Based on analysis the current popular PaaS, this paper brought some security requirements forward together with the P_ FACSM (PaaS_fair access control safe model). The model took ABAC as the foundation, the fairness QoS as environmental constraints, and combined with the authorization of the OAuth protocol. P_ FACSM not only could guarantee the integrity and confidentiality of data in PaaS, but also could ensure the maximum fairness of the QoS. Moreover, it could protect the terminal users' account privacy. After the theoretical analysis and related projects practical application, this model can reach good security guarantee and get high time efficiency.

Key words: platform as a service(PaaS); action based access control(ABAC); quality of service(QoS); open authorization (OAuth); account privacy

随着云计算[1]的发展,软件的开发、部署和使用模式都发生了巨大变化。PaaS 通过提供能力[2]、开发文档、测试环境和部署环境等,使得开发者无须为服务器、操作系统、网络和存储等资源的运维而操心,可以更为方便灵活地进行应用开发和部署,从而大大降低应用开发的门槛,推动了整个移动互联网及云计算的发展[3]。同时终端用户的数据存储也打破了传统方式,所有数据都可以存储在云中,PaaS 平台统一以能力 API 的形式进行开放。这种服务模式的转变会带来如开放接口的非法访问、账户隐私泄露等一系列安全威胁。因此搭建一个可信的安全模型成为了 PaaS 平台发展的重要任务之一。

由于所有的能力资源都存储在云端,PaaS 平台成为了所有访问者访问资源的单一的控制点。因此,PaaS 平台需要细粒度的访问控制,具体的安全需求包括: a)平台能力资源的可控性、完整性及机密性;b)能力资源分配的有效性,即最大化满足访问者的资源请求;c)当终端用户的私有能力资源被访问时,需要终端用户授权,及其授权时用户账户的隐私性要求。

1 相关研究

近年来,对于云端数据的安全性及用户隐私已经引起了广泛关注[4,5]。许多学者提出了一些云环境适用的安全模型,但是都不能综合考虑分配策略及用户账户的隐私保护。Vimercati 等人提出一种基于密钥推导的加密机制,保证了存储在云中数据的安全性[6]。这种方案使用了最少数量的用户私钥和文件加密密钥,但其复杂度随着用户数量的增加而增加,效率较低。有的研究者也提出跟访问控制相关的隐私安全模型。文献[7]提出一种两层的加密机制,用户隐私数据只提供给访问控制策略而不会泄露给云提供者,这样可以保证数据的安全性和隐私性。但用户属性的加密也会大大影响系统的效率。文献[8]提出将访问控制应用于保护用户隐私,会根据请求者及环境的不同而产生不同的隐私保护需求,但隐私的保护仅仅依赖于隐私访问控制策略数据库。这些模型没有完全考虑到 PaaS 平台的安全需求,不能完全照搬到 PaaS 平台中。

文献[9,10]均提出用户到角色的分配同行为、时态等环境状态相关,提出基于行为的访问控制(ABAC)能有效实现云中资源的安全性要求。由于该模型考虑到了环境因素,更适用于复杂的云环境。而在云中进行资源分配方面,文献[11]中提出用户在访问各种类型的资源需求时总有一种资源占支配地位(称为支配资源),该文献利用均衡化不同用户的支配资源思想,提出了一种适用于多类型的公平资源分配方法。因

收稿日期: 2012-06-08; **修回日期**: 2012-07-26 **基金项目**: 国家科技重大专项资助项目(2011ZX03002-002-03);国家自然科学基金资助项目(60903157);四川师范大学基金资助项目(11KYL03);中央高校基本科研业务费专项资金资助项目(ZYGX2011J064)

作者简介:李敏(1978-),女,四川峨眉人,博士研究生,CCF 会员,主要研究方向为移动互联网安全机制等(lm_turnip@126.com);秦志光(1956-),男,教授,博导,主要研究方向为计算机开放系统与网络安全性、信息系统安全等.

此,本文借鉴 ABAC 的思想,将各个用户的 QoS(服务质量)需求作为环境状态约束,考虑到第三方应用对于 QoS 有不同需求层次,可以计算出相应的支配需求,依据文献[11]的方法,实现平台对第三方应用的公平响应,从而最大化第三方应用的利益。

在 PaaS 平台中,许多能力 API 是由终端用户提供,在使用这些 API 时需要用户授权,如何保证授权的安全,即在授权的同时用户的账户信息不被泄露,这是 PaaS 平台面临的又一挑战。在传统的授权中,资源拥有者通常需要将自身的用户名和密码暴露给第三方应用,这样会带来几个安全问题:a)第三方应用可以随时访问用户的任意数据,也可以应用到其他服务中;b)如果账户信息被恶意应用获取,这将造成账户信息泄露,从而导致用户的隐私安全性受到极大威胁。而 OAuth 协议[12]能解决以上问题。该协议不需要资源拥有者在第三方应用中输入用户名及密码,而是将资源拥有者引导到认证鉴权服务器进行鉴权,保证了第三方无法触及到资源拥有者的账户信息,从而确保授权的安全。本文将 OAuth 授权加入到访问控制模型中,以实现数据的安全访问及用户账户的隐私保护。

2　P_ FACSM

根据以上分析,本文汲取了 ABAC 模型中行为的概念,将公平的 QoS 需求响应作为环境因素引入,并结合安全的 OAuth 授权协议,提出了图 1 所示的 P_ FACSM。该模型有三个主要贡献:a)利用基于行为的访问控制,有效地实现了能力资源的安全性;b)平台响应能力访问时除了考虑角色权限以外,还考虑到均衡化不同 APP 的 QoS 支配需求,从而实现了 QoS 的公平响应;c)引入安全的授权协议,保护了用户账户隐私。

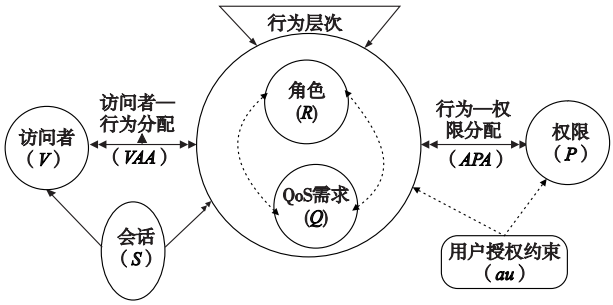

图1　访问控制安全模型

2.1　相关概念

PaaS 平台中的访问控制主要控制第三方应用对于能力资源的访问,其相关概念如下:

能力资源(resource):包括平台公有和终端用户私有能力,所有能力都在 PaaS 平台中以 Open API 形式统一提供给第三方应用,集合记为 R。

终端用户(user):私有能力资源的拥有者,集合记为 U。

访问者(victor):第三方应用(APP),能力资源的实际调用者,集合记为 V。

角色(role):开发者跟 PaaS 平台签约时所描述的权限的集合,该角色可以映射到开发者开发的 APP,集合记为 R。

会话(session):用户同激活角色的对应,在不同的会话中用户获得的权限可能是不同的,会话的集合记为 S。

权限(permissions):对能力资源的访问模式,主要有只读(r)、只写(w)、读/写(r/w)、执行(e)等权限集合,记为 P。

行为(actions):指某个角色在环境约束下实现某个功能所需权限集合的描述,集合记为 A。

终端用户授权约束(authorization constraints,AU):当 APP 调用用户私有能力时,需要用户进行授权访问,集合记为 AU。

除了这些基本的概念外,还涉及到以下映射:

a) VAA:$VA \subseteq V \times A$,多对多的访问者—行为分配,给访问者 v 分配行为 a 的过程。

b) APA:$AP \subseteq A \times P$,多对多的行为—权限分配,对行为 a 分配权限 p 的过程。在该过程中,会涉及到终端用户授权约束(au)。

c) sv:$S \rightarrow V$,函数 sv 将会话 s_i 映射到访问者 v_i,一次访问发起一次会话。

d) sa:$S \rightarrow 2^A$:函数 sa 将会话 s_i 映射到行为集合 $sa(s_i) \subseteq \{a \mid sv(s_i, a) \in VAA\}$,会话 s_i 具有权限 $\cup_{a \in sa(s_i)} \{p \mid (\exists a' \leqslant a)[(a', p) \in APP]\}$

2.2　模型

图 1 给出了适用于 PaaS 平台的 P_ FACSM。该模型对传统的 RBAC 进行了扩展,沿用了 ABAC 中行为(A)的概念,考虑各个 APP 对 QoS 的支配需求不同,采取支配需求的 QoS 公平响应机制(DRQ_fair)作为环境因素,对 APP 行为等级进行划分;再依据用户的角色最终确定用户的权限集及执行的先后次序。该模型还增加了用户授权的约束(au),如应用 A 已经分配到了拥有读能力 c 的角色 r,但是由于该能力是某终端用户的私有能力,需要受到终端用户的授权(au)限制。如终端用户使用一个照片编辑的应用,这就需要访问该用户在 PaaS 平台中的照片资源,该资源是私有资源,需要该终端用户的授权(AU)。

2.3　DRQ_fair 机制

在传统的访问控制中,系统通常会对访问者进行鉴权,确定其拥有相应权限的角色则给予相应的访问级别,但是极少考虑到访问者的信用评估和当前系统的开放能力,也极少考虑到系统响应的公平性。

本文针对以上不足,将根据不同应用对于 QoS 的不同需求作为环境因素引入到模型中,实现了云环境中对服务需求的公平响应。其核心思想为:在第三方应用访问能力资源时,首先根据其角色判断是否有权限访问该能力,如果通过鉴权,则根据均衡化 QoS 支配需求来对 APP 进行排序响应,从而实现 QoS 需求的公平性响应。

2.3.1　相关概念

对 QoS 的衡量在不同的系统中可以有不同的标准,在 PaaS 平台中,QoS 可以考虑如下几个参数:存储能力、带宽能力、响应时间等。不同的 APP 在调用能力时,对平台提供的 QoS 的主要关心点是不一样的。例如,一个地图应用主要关心 QoS 中的存储能力;而一个提供资源下载的应用更看重带宽;一个网络游戏应用则看重响应时间,这些主要关注点可以理解为 QoS 支配需求。这些不同 APP 的 QoS 支配需求将影响平台对 APP 的响应顺序。在说明该问题之前,有如下几个定义:

定义 1　平台可提供的 QoS 集合可表示为

$$Q = (q^1, q^2, \cdots, q^j, \cdots, q^n)$$

其中,$1 \leqslant j \leqslant n$,$n$ 为需求维度。

定义 2　第 i 个 APP 的 QoS 需求可表示为集合:

$$Q_i = (q_i^1, q_i^2, \cdots, q_i^j, \cdots, q_i^n)$$

其中:$1 \leqslant i \leqslant m$, m 为请求能力访问的 APP 数量,n 同定义 1,则 q_i^j 表示第 i 个应用的第 j 个 QoS 需求。

每个应用的某个 q_i^j 越大,代表应用对该参数的需求越高。部分 q_i^j 值需要进行一定转换,如时间需求是 0.1 s,可以转换为响应频率为 1/0.1 = 10 F,即频率越大,表示该应用对时间需求越高。于是某个 q_i^j 值占平台总供应值的比率最大者,则可以理解该 q_i^j 为某个 APP 的支配需求,支配需求越大,表明该应用的迫切程度越高。在平台中,各个应用的质量需求可以根据 APP 的历史需求数据进行统计。如在时刻 t 平台可提供的需求为 Q = (100 B,150 M,120 F),分别代表带宽能力、存储能力及时间响应能力。其中应用 A 的统计需求均值为 Q_A = (10 B, 50 M,20 F),占总供应量的比值分别为(1/10,1/3,1/6);应用 B 的统计均值为 Q_B = (20 B,15 M,10 F),占比率为(1/5, 1/10,1/12);应用 C 的统计均值为 Q_C = (10 B,30 M,10 F) 占比率为(1/10,1/5,1/12)。可以判断应用 A 和 C 更关注存储能力,而应用 B 更关注带宽能力。根据公平原则,可以让所有应用的支配需求达到统一水平,假设 A 执行 x 次,B 执行 y 次, C 执行 z 次可以使得各自的支配需求相等,即要求:

$$\frac{1}{3}x = \frac{1}{5}y = \frac{1}{5}z \tag{1}$$

由(1)式可得:

$$y = z = \frac{5x}{3} \tag{2}$$

x、y、z 值越小,证明该 APP 的支配需求值越大,应该先执行。由式(2)可知,A 的迫切度高于 B 和 C,B 和 C 具有相同迫切度。对于具有相同迫切度的则按照访问提交的先后次序进行排序。

2.3.2 DRQ_fair 算法

在一段时间内,有一些应用请求能力访问,该平台首先判断应用自身对于服务质量的需求是否是在平台可提供的范围之内;如果是,则加入就绪队列,在就绪队列中按公平响应的原则进行优先级排序;如果超出了平台响应范围,则将该请求进行阻塞。阻塞后有两种情况:a)在限定的等待时间范围内,平台再次满足该需求,则加入就绪队列;b)若超时,则直接返回。详细描述如算法 1。

算法 1 DRQ_fair 算法

```
1  InitQueue(Qu)//初始化就绪队列
2  while(Q_i)//在时刻 t 新请求 i 到达
3   {Q = (q^1, q^2, ···, q^n)
    //计算当前平台能提供的需求
4   if(Q > Q_i)
    //如果系统能提供的 QoS 值大于访问者 i 的 QoS 需求
5   {EnQueue(Qu, Q_i)
    //将该请求加入就绪队列,该队列中存储
    //了在 t 时刻系统中剩余未执行的请求
6   Sort(Qu)
    //对就绪队列(队列长度为 m)中按 APP
    //的 QoS 需求迫切度进行排序,确定 APP
    //的优先级,详见算法 2
7    return
     }
8  else
9  { Hold(r_i)
    //阻塞 ri 在一定时间间隔
10   if(在等待时间域值范围内)
11  go 3 //程序转向第 3 行
12  else
13  return
    // 超过时间域值范围则直接返回
     }
   }
```

在算法 1 中,实现按 APP 对 QoS 的支配需求的迫切度进行排序,而确定 APP 的执行优先级是 DRQ_fair 算法的核心,该思想详见算法 2。在算法 2 中,首先计算每个 APP 的占支配的 QoS 需求(见算法 2 第 2 行),然后根据等式(第 4 行)计算出各个 APP 的支配 QoS 需求达到相同水平时比值,比值越小的该 APP 对 QoS 支配需求迫切度越高,从而可以给出各个 APP 的优先级。整个访问控制模型会根据该优先级及角色来依次进行响应。

算法 2 按公平响应原则排序

1 {for(i = 1;i < = m;i + +)
//m 为待响应队列的长度

2 { $y_i = \text{maxindex}\left(\frac{q_i^1}{q^1}, \frac{q_i^2}{q^2}, \cdots, \frac{q_i^n}{q^n}\right)$
//求第 i 个应用的支配需求,将该支配需求的序号给 y_i

3 Init(x_i)
//设第 i 个 APP 执行 x_i 次可达到相同的支配需求,初始化 x_i 为 0
}

4 依据下式由小到大排序($x_1, x_2, \cdots, x_m$):

$$\frac{x_1 \times q_1^{y1}}{q^{y1}} = \frac{x_2 \times q_2^{y2}}{q^{y2}} = \cdots = \frac{x_m \times q_m^{ym}}{q^{ym}}$$

5 以此次序决定各个 APP 的优先级

6 return
}

两个算法的时间复杂度主要取决于对 x_i 的排序算法,可以选择时间效率较好的排序算法;又由于相同的需求迫切度的 APP 要求按照访问提交的先后顺序进行排序,即要满足排序的稳定性。综合考虑时间效率和稳定性,可以选择堆排序,时间复杂度为 $O(m \log m)$(m 为待响应队列的长度)。

2.4 安全的授权约束机制

2.4.1 基本概念

当一个 APP 经过角色权限鉴别和等级划分后访问能力资源时,如果该能力是公共资源,平台直接提供该能力;如果是私有资源,还需要授权限制(AU)。该模型采用 OAuth 授权机制,它是不会将用户名和密码告诉第三方应用的安全的授权方式。OAuth 授权机制的组成元素见表 1。

表 1 OAuth 的组成元素

元素	元素含义
APP key	第三方应用需要注册的唯一 ID
APP secret	第三方应用的私钥,通过秘密通道获取
hash	APP secret 加上时间戳的哈希值
redirect_uri	重定向地址
authorization code	授权码,为了换取访问令牌
access token	访问令牌,换取能力资源

2.4.2 协议流程

当用户 A 想利用一个提供照片打印应用去访问在云端的照片,则该打印应用需要用户 A 授权,如果用户 A 在线,考虑应用是否有后台服务器,可以分成授权码(authorization code)及隐式(implicit grant)两种不同的授权方式。本文主要以授权码的方式为例说明该授权过程,授权码授权流程如图 2 所示。

具体步骤如下:

a)应用将终端用户的浏览器引导至认证鉴权服务器接口,并提交必需的各个参数;

b)认证服务器向用户呈现授权页面,提示用户需要授权

的应用、授权的范围以及是否请求付费信息;

c)用户在授权页面上输入自己的身份认证信息与授权决策,并传递给认证鉴权服务器;

d)认证鉴权服务器认证用户身份认证信息;

e)如果身份认证信息错误,则返回“登录失败”错误码;

f)如果身份认证信息正确,则将用户浏览器重定位到步骤 a)提交的 redirect_uri,并附加 authorization code,从而将 authorization code 提交给应用;

g)应用持 authorization code 及其他必要参数向认证鉴权服务器请求 access token;

h)认证鉴权服务器校验 authorization code 合法性;

i)如果 authorization code 不合法,则向应用返回“授权码无效”错误;

j)如果 authorization code 合法,则向应用发放 access token,并附加令牌访问作用域与生存期信息;

k)应用持 access token 及其他参数访问资源。

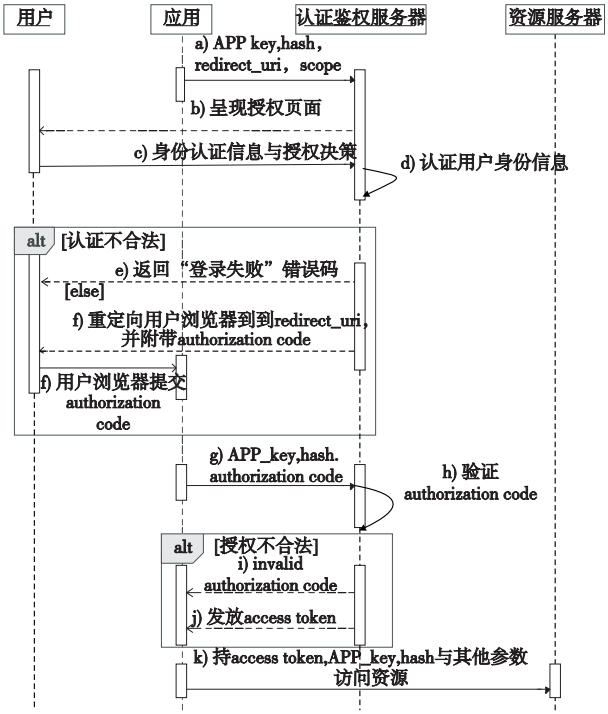

图2　授权码授权流程

如果应用是无后台的服务器支持的桌面、移动终端或脚本应用,可以利用 Implicit grant 进行授权。其授权流程在图 2 的基础上,将步骤 f)改为直接附带 access token 给应用,此时流程直接跳到步骤 k),应用持该 access token 及相应参数去获取资源。

考虑到终端用户有可能不在线,其授权不能以页面的形式呈现,而将步骤 b)改成用短信形式确认,当用户在步骤 c)回复短信后,后面发放 authorization code 和 access token 的过程均由认证鉴权服务器直接交由应用,而无须用户再参与,此后的过程对用户透明。

2.4.3　安全性分析

在以上的授权过程中,终端用户的账户信息没有直接交由应用,这样可以很好地保证用户账户的隐私安全性。在 OAuth 协议中,为了防止第三方应用的假冒,应用在向认证鉴权服务器提交身份信息时,会计算 hash = h(APP secret||timestamp)作为身份标志。该哈希函数可以是任意常用哈希函数,如 MD5、Sha1 等。由于其他应用不可能获取该应用的 APP secret,所以不可能产生该 hash 值,从而确保了该应用身份的真实性。

2.5　实验

实验硬件环境是 4 个刀片的 IBM 服务器,在 Redhat 企业版系统上安装了 Hadoop,搭建了一个 PaaS 平台,进行了相关实验测试。在 2.5.1 节中测试了该模型授权安全性,在 2.5.2 节中测试了公平 QoS 响应机制同简单考虑带宽公平或内存公平的响应机制的比较,DRQ_fair 算法在平均响应时间上有明显优势。

2.5.1　安全授权测试

本文以 OAuth 作为安全授权协议进行了实验,利用一个名为 test 的第三方应用做了相关测试,测试的结果充分证明了该授权能很好地保证终端用户的账户隐私。下面以 authorization code 方式为例,具体流程及相关参数如下:

a)第三方应用 test 注册,获取 APP key 和 APP secret,如图 3 所示。

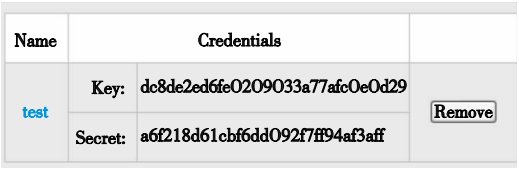

图3　第三方应用注册

b)Test 选择授权方式。有四种方式(图 4)可选。

图4　选择授权方式

c)如果选择 authorization code 方式,则终端用户会收到授权页面请求授权,如图 5 所示。该终端用户授权时不需要将账户信息泄露给第三方应用,从而保证了其隐私安全。

d)如果终端用户授权通过,test 会得到以下 authorization code(图 6),应用会持该授权码及相关参数获取 access token(图 7)。到此,一次完整的授权过程结束。

2.5.1　QoS 公平响应机制测试

为了讨论 QoS 公平响应机制的性能,实验将 DRQ_fair 算法同单一 QoS 需求属性(如带宽、内存等)的响应机制进行简单的性能比较。

本文实验设置了两大类的 APP:第一类是 100 个 QoS 需求较小的 APP(10 B,5 M),另一类是 100 个 QoS 需求较大的 APP(20 B,20 M)。在试验中,本文是将 APP 按照随机模式提交到 PaaS 平台中,每个 APP 运行时记录其响应时间,以便计算平均

图5 授权页面

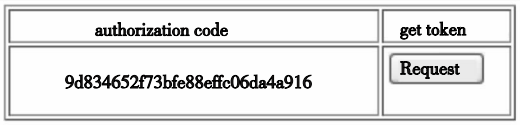

图6 获取authorization code

图7 获取access token

值。图 8 列出了支配需求的 QoS 公平(DRQ_fair)、带宽公平(BandW_fair)及内存公平(Mem_fair)平均响应时间。

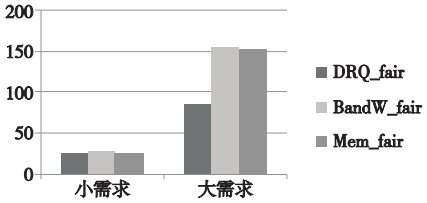

图8 不同QoS需求在三种机制中的平均响应时间

由图 8 可见,当 APP 的需求较大时,本文提出的 DRQ_fair 算法具有明显优势。

3 结束语

PaaS 平台中能力开放带来如接口越权访问、账户隐私信息泄露等安全问题,这也是云发展的核心问题之一。本文结合 ABAC、QoS 公平响应及 OAuth 安全授权,提出了 P_FACSM,阐述了该模型的组成部分,同时进行了效率分析及安全性分析,并进行了安全授权测试。该模型在相关项目中已得到了实现,该 PaaS 平台部署于 IBM 刀片服务器上,多个刀片服务器作为 AppServer 承载第三方应用,在该 PaaS 平台中进行了一系列安全及性能测试。运行结果表明该模型能较好地应用在 PaaS 平台中,具有如下优点:a)保证了 ABAC 中行为约束,实现了接口访问的安全性;b)平台在响应能力访问时,能依据各个 APP 不同的 QoS 支配需求进行公平响应,保证了各个 APP 利益的最大化;c)在访问终端用户数据需要授权时,利用 OAuth 协议保证了账户的隐私安全。

P_FACSM 中行为的层次还有待更进一步研究。同时,云计算下 SaaS(software as a service)同样面临越权访问及公平响应的问题,下一步工作可以研究 P_FACSM 在 SaaS 下的适应性,提出适用于 SaaS 的公平访问控制模型。

参考文献:

[1] DONG Xiao-xia, LU Ting-jie. Review of the cloud computing and its future development[J]. Journal of Beijing University of Posts and Telecommunications,2010,12(5):76-80.

[2] KIM E, KIMK K, IN H P. A multi-view API impact analysis for open SPL platform[C]//Proc of the 12th International Conference on Advanced Communication Technology. Piscataway: IEEE Press, 2010: 686-691.

[3] 徐鹏,陈思,苏森. 互联网应用 PaaS 平台体系结构[J]. 北京邮电大学学报,2012,35(1):120-125.

[4] BU Wen-jun, ZOU Chao-bin, YU Jia-lin. Hot cloud computing platform recommendations[J]. Silicon Valley,2011,5:10-11.

[5] 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.

[6] Di WIMERCATI S D C, FORESTI S, JAJODIA S, *et al*. Over-encryption: management of access control evolution on outsourced data [C]//Proc of the 33rd International Conference on Very Large Data Bases. [S. l.]:ACM Press,2007:123-134.

[7] ZHOU Miao, MU Yi, SUSILO W, *et al*. Privacy-preserved access control for cloud computing[C]//Proc of the 10th International Conference on Trust, Security and Privacy in Computing and Communication. Washington DC:IEEE Computer Society,2011:83-90.

[8] 徐菲,何泾沙,徐晶,等. 保护用户隐私的访问控制模型[J]. 北京工业大学学报,2012,38(3):406-409.

[9] 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,2012,33(3):59-67.

[10] 李凤华,王巍,马建峰等. 基于行为的访问控制模型及其行为管理[J]. 电子学报, 2008,3(10):1881-1890.

[11] GHODSI A, ZAHARIA M, HINDMAN B, *et al*. Dominant resource fairness: fair allocation of multiple resource types[C]//Proc of the 8th USENIX Conference on Networked Systems Design and Implementation. Berkeley:USENIX Association,2011:10-24.

[12] Network Working Group. The OAuth 2.0 authorization protocol draft-ietf-oauth-v2- 20 [EB/OL]. http://tools. ietf. org/html/draft-ietf-oauth-v2-20.

下期要目

- 多核处理器硅后测试技术研究最新进展
- 无线体域网节能策略综述
- 无线传感器网络的拓扑维护
- 同时送取火车路径问题算法研究综述
- 去身份识别技术综述
- 基于行程时间多步预测的实时路径导航算法
- 双层车辆路径问题的混合启发式算法
- 基于轨迹安全性评价的免疫遗传路径规划算法
- 混合遗传算法求解应急抢修点选址问题
- 基于单亲遗传禁忌搜索算法的手术排程问题研究
- 面向大型场馆疏散的改进多蚁群算法
- 一种新的约束优化遗传算法及其工程应用
- 带粒子释放和速度限制的粒子群算法
- 基于遗传算法的城市公交骨架线网优化设计
- 基于二阶段相似度学习的协同过滤推荐算法
- 基于混合策略的关联分类方法
- 跨领域中文评论的情感分类研究
- 一种高效的连续不确定 XML 小枝模式匹配算法
- 基于分类挖掘的网格资源分配研究