

一种基于信任评估的云服务属性访问控制模型

王静宇^{1,2}, 赵山杉², 郑雪峰¹

(1 北京科技大学 计算机与通信工程学院, 北京 100083;

2 内蒙古科技大学 信息工程学院, 内蒙古 包头 014010)

摘 要: 针对云服务的安全访问控制问题, 提出一种基于信任评估的云服务属性访问控制模型. 该模型将信任与基于属性访问控制框架相结合, 采用一种基于服务质量指标的信任评估方法, 融合直接信任、间接信任和综合信任来评估云资源信任度. 仿真实验结果显示, 该模型能正确、有效地抑制云用户对恶意虚假服务的访问, 增强了云服务访问的安全性.

关键词: 云安全; 访问控制; 信任; 服务质量指标

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2015)12-0001-07

A Cloud Service Attribute Access Control Model Based on Trust Evaluation

WANG Jing-yu^{1,2}, ZHAO Shan-shan², ZHENG Xue-feng¹

(1 School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China; 2 School of Information Engineering, Inner Mongolia University of Science and Technology, Baotou 014010, China)

Abstract: Aimed at the problems of security access control cloud services in cloud computing, a cloud service attribute access control model based on trust evaluation was put forward. Combined with access control framework based on attribute, a trust evaluation method based on service quality indicators is proposed. Direct trust, indirect trust and comprehensive trust are utilized to evaluate the credibility of cloud resource. The simulation results show that the model can correctly and effectively prevent cloud users access to malicious and untrusted services. The security of cloud service access is improved.

Key words: cloud security; access control; trust; SQI

1 引言

云计算安全问题是当前的研究热点, 而访问控制是云计算安全的重要研究内容, 同时也给传统的访问控制机制^[1-3]提出了更加严峻的挑战. 要确保用户访问一个陌生可靠的资源, 仅仅依靠传统的身份安全访问控制是不可用的. 而基于属性的访问控制^[4], 为属性访问控制授权提供了依据, 尤其适合于云环境下的访问授权, 然而此模型尚没有引入与信任相关的属性, 忽略了交互过程中实体间的信任关系, 没有认识到信任对安全性决策授权的影响, 因

此, 将信任引入到访问控制模型之中, 增强云服务的安全性非常必要.

目前国内外学者基于现有的访问控制提出了各种适合于云计算环境下的访问控制模型, 例如: 文献[5]在传统的 RBAC 基础之上考虑了时态环境等约束条件, 通过引入主体角色和主客体属性的可变机制来实现访问控制的灵活性, 并应用在医疗保健系统之中, 但是此模型只是在传统的访问控制中扩展, 忽略了信任对机制的影响, 并未解决云服务安全性问题. 文献[6]中通过引入信任这一概念, 增强了节点间交互的安全性, 并且在信任计算方面增大了对恶意节点

收稿日期: 2015-02-03; 修回日期: 2015-03-31

基金项目: 国家自然科学基金项目(61462069); 内蒙古自然科学基金项目(2012MS0912, 2014MS0622)

的惩罚措施,在某种程度上有效地降低了任务执行失败的比率,但是,该模型只是在人际关系信任模型上的一种完善,简单地把服务质量引入模型中,并单一地应用信任度阈值进行控制,主观性评价所占比重较大.文献[7]中通过对用户信任进行评估,把信任作为二级访问控制引入到模型中,定义了一个基本的访问控制策略,依据信任度的比较结果来确定是否授权,实现了在服务计算环境下对策略的统一管理,但是此模型在 Web 环境下实现,同时没有考虑访问资源的安全性,信任度的评估主观性太强,简单地把信任作为一控制门槛.文献[8]在传统的 RBAC 基础上采用信任管理技术,通过使用 SAML^[9]和 XACML^[10]分别把认证模块和访问控制模块相结合,在特定的域内,服务提供者通过与访问请求者的直接交互信息和其他证人的推荐信息来评估信任度,然后与自身标准信任进行比较授权,但是文中主要是针对用户信任的评价,一定程度上防止了用户的恶意行为,却没有考虑虚假、恶意的资源给用户带来的不良影响.本文在文献[4]的基础上,提出了一种基于信任评估的云服务属性访问控制模型(CST-ABAC).

2 CST-ABAC 模型定义

CST-ABAC 是一种基于信任实现对访问请求进行决策的模型,其基本观点不是通过主客体直接授权,而是通过主体、客体、环境、动作以及信任为基础进行综合授权的,其中信任作为授权的一个关键因子,在模型中起着不可替代的作用,本模型给出如下形式化定义.

定义 1 (CST-ABAC) CST-ABAC 是由 (M, R, E, T, A) 组成的五元组,其中 M 代表主体, R 代表资源, E 代表环境, T 代表信任, A 代表相应的动作.

定义 2 (访问请求) Req 是由 $(Re, (Res, Act))$ 组成的二元组,其中 Re 是请求的发起者, Res 是 Re 所请求的资源, Act 是 Re 请求资源 Res 要进行的操作.当发起一条访问请求的时候可以表示为: $Req_i(Re, (Res, Act))$, 其中 Req_i 为第 i 个访问请求, $(Re, (Res, Act))$ 为访问请求的参数.

定义 3 (属性名值集) 属性由符号 tr 来表示,分别用 Mtr, Rtr, Etr, Ttr, Atr 表示主体、资源、环境、信任、动作属性名,其属性值分别用 $Mtrv, Rtrv, Etrv, Ttrv, Atrv$ 来表示, $m = \{Mtr = Mtrv_1, Mtr = Mtrv_2, \dots, Mtr = Mtrv_n\}$ 表示主体属性名值集;

$r = \{Rtr = Rtrv_1, Rtr = Rtrv_2, \dots, Rtr = Rtrv_n\}$

表示资源属性名值集;

$e = \{Etr = Etrv_1, Etr = Etrv_2, \dots, Etr = Etrv_n\}$

表示环境属性名值集;

$t = \{Ttr = Ttrv_1, Ttr = Ttrv_2, \dots, Ttr = Ttrv_n\}$

表示信任属性名值集;

$a = \{Atr = Atrv_1, Atr = Atrv_2, \dots, Atr = Atrv_n\}$

表示动作属性名值集.

定义 4 (信任) Trust: 信任是一种建立在自身经验基础之上,访问者对云服务资源可信程度的评价,其评估结果一般采用经过量化的信任度 T 来表示,其经决策后的属性有 $untrust, weak\ trust, trust, strong\ trust$ 等.

定义 5 (信任条件) Trust Conditon: 信任条件是指服务提供方必须满足的条件,当服务方的信任度满足某一信任条件时,请求方(主体)信任提供方(客体),反之,请求方不信任提供方.通常信任条件为一个信任阈值,当信任度不小于阈值则信任,小于阈值则不信任.

定义 6 (授权策略) Policy: 授权策略是由 $policy \leftarrow (purpose, combine\text{-}Algorithm, Rules)$ 三元组构成, $purpose$ 是访问控制请求的目标,由 $(Main, Resource, Environment, Trust, Action)$ 五个元素构成,用来判断所属策略是否符合此条访问请求,而 $combine\text{-}Algorithm$ 表示对 $Rules$ 的组合的算法, $Rules$ 表示合成策略的规则, $Rules = resu \leftarrow (MA, RE, EN, TV, AC)$, 其中 $resu$ 为返回的结果集,而 MA, RE, EN, TV, AC 分别代表主体、资源、环境、信任,以及动作对应的属性值的约束集合.授权策略的集合可以表示为 $Policy\text{-}set = \{policy_1, policy_2, policy_3, \dots, policy_n\}$. $Policy_i$ 为一个授权的策略.

定义 7 (策略判定) Police Decision: 当有一访问请求 $Req_i(Re, (Res, Act))$ 和访问策略 $policy \leftarrow (purpose, combine\text{-}Algorithm, Rules)$ 时,首先要进行策略符合判定,判定此访问策略是否能够适合此条访问请求,如果适合则返回 $resu$, 否则返回 $can_not_do_it$.

3 CST-ABAC 模型组成

在 CST-ABAC 模型中,访问者在访问资源时,以信任度的高低为手段,来避免恶意虚假的资源,同时在获得可靠的信任度的前提下,结合其他的属性进一步决策授权,并利用用户反馈机制使信任度处在不断的更新之中,更加接近真实的、可靠的环境.本模型主要由两个模块构成: 认证授权模块(CAM)和信任模

块(TM). CAM 主要接受访问请求,并对其分析转化,进行相关信息的收集,然后查询策略库,通过策略匹配作出最终的决策返回给用户;TM 主要负责对资源信任度的评估,通过收集历史交互记录,完成信任度的评估与决策,然后把决策结果返回给认证授权模块;CST-ABAC 模型的整体框架如图 1 所示.

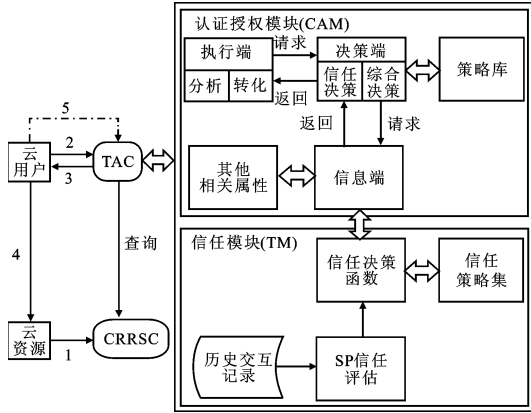


图 1 CST-ABAC 模型

(1)云资源提供者(SP)首先向 CRRSC(Cloud Resource Registration Service Center,云资源注册服务中心)注册自己宣称的服务质量及其指标.

(2)云用户请求者(SR)向 TAC(Trust Authorization Center,信任授权中心)提出一条访问请求 $Req_i(Re, (Res, Act))$, TAC 对此条访问请求做如下处理:

①执行端对该访问请求进行分析,转化为一条基于属性的访问请求并发送到决策端;执行端负责访问请求的分析与转换,再把请求发送给决策端;

②决策端向信息端发出属性查询请求;收到此请求后信息端收集环境、用户、资源、操作等其他相关属性返回给决策端,同时信息端也通过调用 TM 发出收集信任属性请求, TM 利用信任决策函数得到资源的信任属性;

③信息端把最终所有属性返回给决策端;

④决策端得到信息端返回结果后,首先判断资源信任属性是否满足用户访问,若满足,即提供的不是恶意虚假的服务,则查询策略库并结合其他属性做出最终决策,授予用户所应有的权限;反之,决策端直接拒绝用户访问;

⑤把决策端做出的决策返回给执行端.

(3)TAC 中的执行端将决策端做出的最终决策结果返回给云用户.

(4)云用户根据决策结果访问云资源.

(5)访问结束后,云用户向信任模块反馈所得到

的 SQL.

4 CAM 决策授权及 TM 流程

4.1 CAM 决策授权流程

决策授权主要通过策略决策端来完成,策略决策端通过信息端收集资源的信任属性来确定资源是否可靠,如若不可靠就拒绝访问,如若可靠则综合其相关的主体、客体、环境等属性进行进一步决策授权,其具体流程图如图 2 所示.

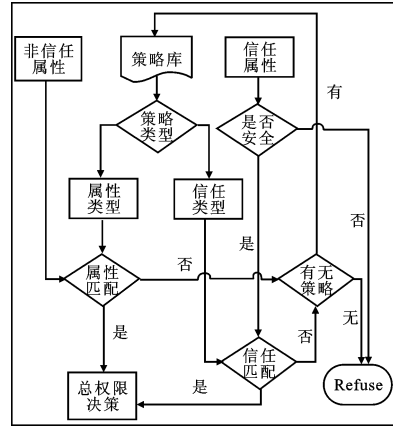


图 2 决策授权流程图

决策端作为 CAM 中决策授权的最重要部分,主要任务是在接受到访问请求后,查询策略库判定访问请求,其策略授权判定算法描述见图 3.

4.2 TM 流程框架

服务请求者向 TAC 提出访问请求 $Req_i(Re, (Res, Act))$ 后, TAC 通过 CAM 中的信息端收集相关属性信息为决策端奠定决策基础,而信任信息如何获得以及评估是本文的重点,图 4 中给出了 TM 中信任度获取的具体流程.

CAM 收到访问请求 $Req_i(Re, (Res, Act))$ 后,信息端访问 TM, TM 首先查询对云用户反馈信息进行过预处理的历史交互记录,判断资源访问者是否与资源提供者有过直接的历史交互. (1)如果没有进行过交互,那么,通过间接信任度的计算方法进行信任度的评估从而获得间接信任度,然后由信任决策函数查询信任策略集对信任度进行决策,最后把信任决策结果返回给 CAM 中的信息端; (2)如果有过交互,那么就要判断特定时间段内交互的次数 n , 如果交互次数 $n \geq N$ (N 表示证据充分阈值), 表明历史直接交互历史证据非常充分, 应用直接信任的计算即可, 不需要借助间接的推荐; 如果交互次数 $0 < n < N$, 表明历史交互历史证据不足, 必须要借助

间接的推荐,那么就要应用综合信任度的计算来获得信任度;最后把得到的信任度做类似(1)的决策处理,把决策结果返回给 CAM 中.

```

PolicyDecision(Req,(Re,(Res,Act))),purpose(Main,Resources,
Environments,Trust,Actions))
{ //此访问请求是否符合判定
if CAM.Policy_Trust-core-algorithm(Re,(Res,
Act))==untrust
Return can_not_do_it
else
if(m.Mtr∈Main&&r.Rtr∈Resources
&&e.Etr∈Environments&&t.Ttr∈Trust
&&a.Atr∈Actions)
{
PolicyMade(); //整体策略判定
}
else
Return can_not_do_it
}
PolicyMadce(Req,;(Re,(Res,Act)),Rule[])
{
//整体策略判定
for(j=1;j≤Rule.length;j++)
{
if(Rule[j].tr==Req.tr
&&Req.trv<Rule[j].trv)
{
Result[j]=Rule[j].resu;
}
}
Result=Combining(Result,combine-
Algorithem); //合并判定结果
return Result; //返回策略判定结果
}

```

图 3 策略授权判定

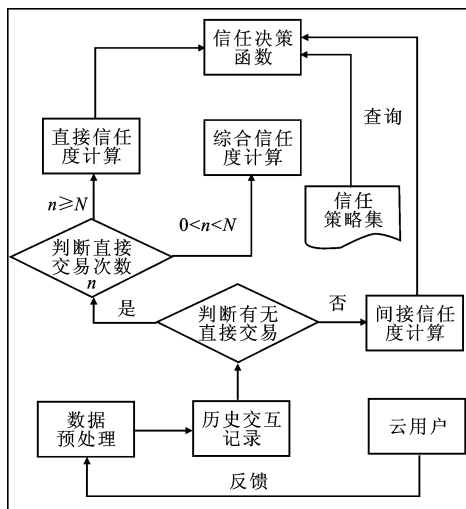


图 4 TM 流程

5 TM 中 SQI 信任评估算法

为了保证用户访问安全且无虚假的云服务资

源,实体间的信任显得尤为重要,本文通过只有资源提供者的信任度达到信任阈值才能进一步决策授权的这一思想,给出了基于 SQI 信任度计算方法,主要分为三个部分:直接信任度计算,间接信任度计算以及综合信任度计算. 本文主要采用文献[11]中给出的部分 SQI 作为 CST-ABAC 模型信任度计算的基础,其中, SQI 主要包括执行时间、执行费用、可靠性、可用性等,下面给出与信任相关联的一些定义:

定义 8 服务提供者向 CRRSC 宣称的 SQI 集合为 $Q^{\text{Claim}} = \{Q_1^{\text{Claim}}, Q_2^{\text{Claim}}, \dots, Q_n^{\text{Claim}}\}$, 其中 Q_k^{Claim} 表示第 k 个 SQI 参数.

定义 9 资源访问者在交互中所得到的服务提供者提供的 SQI 集合表示为 $Q_{ij}^{\text{Iter}} = \{Q_{ij}^{\text{Iter},1}, Q_{ij}^{\text{Iter},2}, Q_{ij}^{\text{Iter},3}, \dots, Q_{ij}^{\text{Iter},n}\}$, 其中 $Q_{ij}^{\text{Iter},k}$ 表示实体 i 与实体 j 交互过程中所获得的第 k 个 SQI 参数. 在以上定义基础之上, 本文将 SQI 应用到信任度算法中, 为决策授权提供可靠的依据.

5.1 直接信任度计算

根据历史交互记录是否充分有直接信任度的计算公式如下:

$$T_{\text{Direct}}^{ij} = \sum_{k=1}^N \frac{1}{N} H(k) T_{ij}^k \quad (1)$$

式(1)中利用交互双方的历史交互记录来计算资源访问者对服务提供者的信任度, 其中, T_{Direct}^{ij} 被定义为经多次交互后实体对服务提供者的直接信任度, N 为最大交互有效历史记录次数, $H(k)$ 为时间衰减函数, 且 $0 < H(k) < 1$, 其中 $H(k)$ 可以定义为

$$H(k) = \begin{cases} 1, & k = N \\ H(k-1) + \frac{1}{N}, & 1 \leq k < N \end{cases} \quad (2)$$

根据人们的认知, 离现在时间越短的交互行为越应该被赋予相对大的权重, 使发生在不同的时刻的历史交互信任信息加权更加合理. 而 T_{ij}^k 表示一次交互的可信度 (T_{ij}^N 表示离现在发生交互行为最近的一次, T_{ij}^1 表示离现在发生交互行为最远的一次) 其计算可以用如下公式获得:

$$T_{ij}^k = \sum_{h=1}^n \omega_h \left(\frac{1}{|Q_{ij}^{\text{Iter},h} - Q_h^{\text{Claim}}|} \right)^2 \quad (3)$$

式中, ω_h 为每个 SQI 的重要程度即权重, 其重要程度是客观存在的, 故利用信息熵^[12] 的思想对权重进行客观的确定且满足如下条件:

$$\begin{cases} 0 \leq \omega_h \leq 1 \\ \sum_{h=1}^n \omega_h = 1 \end{cases} \quad (4)$$

$Q_{ij}^{iter,h}$ 为交互历史记录中的第 h 个指标值,其值可通过查询预处理量化后的历史交互记录表(格式见表1)得到.其中执行价格、响应时间、可靠性及可用性是 SQI 的部分指标, Q_h^{claim} 为提供者宣称的第 h 个 SQI,可通过查询 CRRSC 获得. $Q_{ij}^{iter,h}$ 与 Q_h^{claim} 的差值越小说明信任度越高.反之,信任度越低.

表1 历史交互记录

信任者	被信任者	执行费用	响应时间	可靠性	可用性
SR1	SP1	2	1.2	0.6	1.5
SR1	SP1	3	1.4	0.7	2.6
SR2	SP1	5	2	0.3	1.2
SR2	SP2	4	3	0.1	0.9

5.2 间接信任度计算

对于没有过交互的两个实体之间信任度的计算利用信任的传递性^[13]来获得,假设 A 和 C 没有过交互,但是 A 和 B 有过交互, A 对 B 的信任程度为 T_{AB} ,而且 B 和 C 有过交互, B 对 C 的信任度为 T_{BC} ,那么 A 对 C 的信任度就可以通过 T_{AB} 和 T_{BC} 的乘积获得,在这个思想下我们根据有无历史交互记录进行间接信任度计算,其公式如下:

$$T_{Indirect}^{ij} = \frac{\sum_{k=1}^n (W(k) * T_{Direct}^k) * \frac{1}{\sum_{i=1}^n W(k)}}{1} \quad (5)$$

式中, $T_{Indirect}^{ij}$ 表示间接信任度, T_{Direct}^k 表示要评估实体的前一实体对要评估实体的信任度, $W(k)$ 为间接推荐路径中的权重,其定义如下:

$$W(k) = \prod_{i=0}^k T_{Direct}^i \quad (6)$$

式中, T_{Direct}^i 表示访问实体 E_0 到要被访问实体的信任路径上第 i 个实体对下一个实体的直接信任度,为了直观的表达可以把历史交互记录构建成一颗 IDT(间接信任树)如图5所示.

例如,实体 E_0 要得到实体 E_6 的信任度,但是 E_0 与 E_6 没有直接的交互,然而, E_0 与 E_1 有交互, E_1 与 E_3 和 E_4 分别有过交互, E_3 和 E_4 分别与 E_6 有过交互,那么,根据式(6)可以获得权重

$$W(1) = 0.7 * 0.5 = 0.35, W(2) = 0.7 * 0.6 = 0.42.$$

根据式(5)可以计算出间接信任度为 $(0.35 * 0.9 + 0.42 * 0.7) / (0.35 + 0.42) = 0.79$.

5.3 综合信任度计算

当 SR(资源访问者)与 SP(资源提供者)存在历

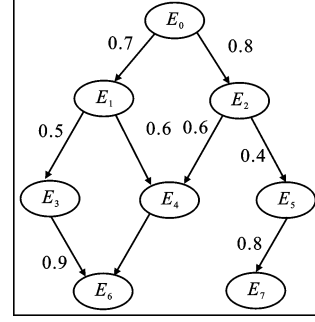


图5 IDT树

史交互记录,但是历史交互记录不充分(小于阈值 N)时,选择综合信任度计算公式来计算其信任度,根据人们的心里认知预测^[14],其公式如下:

$$T_{cp}^{ij} = \frac{1}{1 + \partial(i)} T_{Direct}^{ij} + \frac{\partial(i)}{1 + \partial(i)} T_{Indirect}^{ij} \quad (7)$$

式中, T_{cp}^{ij} 为综合信任度, $\partial(i)$ 为出度度, $\partial(i) \in [0, 1]$,反馈者个数越多说明出度度越高,在一定程度上它反映了其稳定性与活跃度. $\partial(i)$ 的计算公式如下:

$$\partial(i) = \frac{1}{2} [\theta(p_i) + \theta(n_i)] \quad (8)$$

式中, $\theta(y)$ 的表达式如下:

$$\theta(y) = 1 - \frac{1}{y + A} \quad (9)$$

式中, p_i 为反馈历者的个数, n_i 为与实体 j 有过交互的所有实体总数, A 为一任意常数的调节因子,主要用于调节趋近与 1 的速度的快慢,可以明显地看出,出度度由两个变量共同的决定,并且,与实体有过交互的其他实体个数越多,反馈者的个数越多,那么其出度度越大,即 $\partial(i)$ 越大.而且,直接信任度的权重一直大于间接信任度的权重,符合人的认知.

5.4 TM 核心算法描述

信任模块的主要功能是对云服务资源进行信任评估,核心是基于 SQI 评估算法对资源进行客观计算,把计算得到的信任度与 TM 中信任策略集决策匹配,获得信任属性.部分核心算法见图6.

6 实验及结果分析

实验硬件环境说明,服务器配置如下:4 颗 8 核 cpu,主频 1.86 GHz,内存为 64 GB,存储为 10 TB,VMware 虚拟化平台.

仿真实验软件如下:开发平台 My Eclipse 8.5,采用 CloudSim^[15] 进行仿真实验,并在 CloudSim 中进行模块扩展,引入基于 SQI 的信任度评估计算算法,实现了 CAM 模块和 TM 模块.

实验做如下设定:设置了 1 000 个实体来模拟

```

Trust-core-algorithm(Re,(Res,Act))
Begin
Let N=k
For(i=0;i<histoty,length,i++)
//统计历史交互记录的条数
{ i=i+1;
n=i;
}
If(n!=null)
//判断历史交互记录条数是否为空
If(0<n<k)
//如果不是空且记录交互记录在0到k之间,
式(7)计算信任度

$$T_{cp}^i = \frac{1}{1+\delta(i)} T_{Direct}^i + \frac{\delta(i)}{1+\delta(i)} T_{Direct}^i$$

Return  $T_{cp}^i$ 
If(n>k)
//若交互记录大于n执行如下

$$T_{Direct}^i = \sum_{k=1}^N \frac{1}{N} H(k) T_{ij}^k$$

Return  $T_{Direct}^i$ 
Else  $T_{Indirect}^i = \sum_{k=1}^N (W(k) * T_{Direct}^k) * \frac{1}{\sum_{k=1}^N W(k)}$ 
//若无交互记录执行如下
Return  $T_{Indirect}^i$ 
End
Policy_Trust-core-algorithm(Re,(Res,Act))
Begin
TrustPolicyset=TM.Find_TrustPolicyset(Req(Re,(Res,Act))) //访问信任策略集
for(j=0,j<TrustPolicyset.length,j++)
//从策略集中检索所有子策略并获取
{ //信任值决策
Decision[j]=TrustPolicyset[j]
if TM.Trust-core-algorithm(Re,(Res,Act))
∈ Decision[j]
Return com
break
}
End

```

图6 TM 核心算法

服务提供者与访问者,服务者与访问者是相对独立的,一个实体既可以是服务提供者也可能是访问者,但是其身份是相对独立,互不影响的,并定义提供真实可靠服务的实体所占比例为 80%,恶意虚假的服务提供者实体所占的比例为 20%,假设非虚假的实体总是提供良好的服务,这样设置的真实可靠的服务实体比恶意虚假的服务实体比例要大,与实际的情况较为相符,其中实体之间有直接历史交互记录的占 30%,参数 N 设置为 100,初始信任值与信任阈值都设置为 0.3:

实验一:信任度计算与恶意服务节点识别.

为了说明本模型引入 SQI 的有效性,本实验首先随机选取 5 个服务节点计算其信任度,从而得到服务节点信任度随着次数增多的变化图,如图 7 所示.从图中可以看出,服务节点 1 到 3 随着访问次数的增多,信任度逐渐增强,说明这 3 个节点为可靠的服务提供者,而服务节点 4 和 5 随着访问次数的增

多,信任度逐渐下降,说明节点 4 和 5 提供恶意虚假的服务,意味着本模型对服务节点信任评估的有效性.然后对所有节点进行模拟统计,获得识别恶意服务节点图,如图 8 所示.从图中可以看出开始由于访问次数较少识别恶意节点比例较小,但是随着访问次数增加到 75 时,恶意节点的识别比例加快,当恶意节点的识别比例增加到一定程度时,由于恶意节点大幅度减少,随着访问次数的增多识别比例变缓,符合人们的认知,从而说明此模型对恶意虚假的服务有着良好的识别能力.

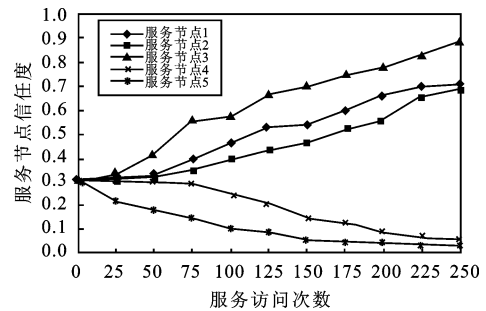


图7 服务节点信任度图

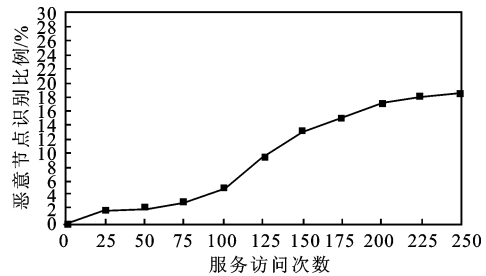


图8 识别恶意服务节点图

实验二: CST-ABAC 模型的正确性及有效性对比.

本实验以轮(rounds)为单位进行交互,每轮交互的实体个数为 25,并规定一个周期为三轮,并通过与文献[4]中没有信任机制下的访问控制模型 UnTrust-ABAC 进行对比,得出服务成功率和请求周期的变化如图 9 所示,在 CST-ABAC 中,开始的时候由于存在 20%的恶意虚假资源,服务成功率逐渐下降,但随着 SQI 信任机制的对资源信任的不断动态评估,恶意虚假的节点逐渐得到有效抑制,所以在以后的交互中,服务成功率逐渐回升,仍能维持较高的成功率;而 UnTrust-ABAC 中没有类似评估实体信任的机制,所以它对恶意服务节点的反应比本文叙述的方法要低.同时,本实验在实体平均交互 3 轮情况下,通过提高恶意节点比率来观察服务失败率,从图 10 中可以看出服务的失败率都随着恶意虚

假的节点比率的增多而上升,但是由于 UnTrust-ABAC 没有信任机制,服务失败率的增大速率要低于 CST-ABAC,说明本文中的 SQI 信任机制对恶意虚假的节点有着有效的抑制作用,增强了云服务访问的安全性。

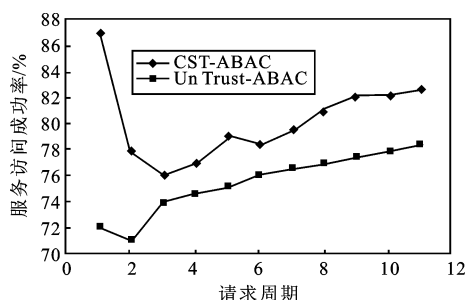


图9 服务访问成功率图

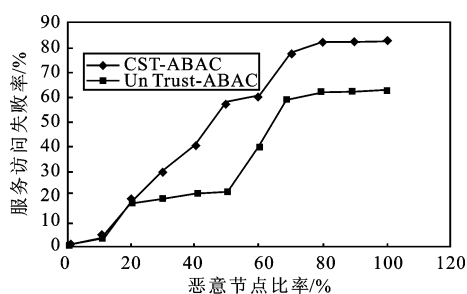


图10 服务访问失败率图

7 结束语

本文结合属性机制提出了一种基于信任评估的云服务属性访问控制模型,该模型依据服务提供者的信任度作为访问控制安全的门槛,然后结合当时所处的主客体、环境以及信任属性再次决策授权,确保了云资源服务的安全性。在信任度计算上,本文采用 SQI 作为评估信任度的基础,该方法不仅能够更加客观合理地对信任进行评估,而且能有效遏制恶意虚假的服务。实验结果验证了把信任作为访问控制的重要因子是可行的,并且是行之有效的。

参考文献:

- [1] Bygkues M, Colazzo D, Crafa S, et al. A type system for discretionary access control[J]. Mathematical Structures in Computer Science, 2009, 19(4): 839-875.
- [2] Ray I, Kumar M. Towards a location-based mandatory access control model[J]. Computers & Security, 2006, 25(1): 36-44.
- [3] Martínez García C, Navarri Arrribas G, Borrell J. Fuzzy Role-based access control[J]. Information Processing Letters, 2011, 111(10): 483-487.
- [4] 李晓峰,冯登国,陈朝武,等. 基于属性的访问控制模型[J]. 通信学报, 2008, 29(4): 90-98.
- [5] 赵明斌,姚志强. 基于 RBAC 的云计算访问控制模型[J]. 计算机应用, 2012, 32(Sup2): 267-270.
- [6] 吴慧,于炯,于斐然. 云计算环境下基于信任模型的动态级访问控制[J]. 计算机工程与应用, 2012, 48(23): 102-106.
- [7] 吴明峰. 基于属性和信任评估的服务计算安全模型研究[D]. 济南: 山东师范大学, 2013.
- [8] 殷晓玲,夏后寿,王汝传. Web Services 中基于信任的动态访问控制[J]. 计算机应用研究, 2011, 28(11): 4331-4334.
- [9] OASIS. Profiles for the OASIS security assertion markup language (SAML) version 2.0[EB/OL]. (2005-03-15). <http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip>.
- [10] OASIS. Extensible access control markup language (XACML) version 2.0, working draft 09[EB/OL]. (2004-04-16). <http://www.oasis-open.org/committees/download.php/10577/XACML-2.0-os-all.zip>.
- [11] 张旭云. Web 服务组合中 QoS 评估及服务选择的关键技术研究[D]. 南京: 南京大学, 2011.
- [12] 姜燕强,宋如顺,马永彩. 基于不完全信息动态博弈的入侵容忍技术[J]. 计算机工程与设计, 2010, 31(11): 2430-2431.
- [13] 胡祥培,尹进. 信任传递模型研究综述[J]. 东南大学学报: 哲学社会科学版, 2013, 15(4): 46-51.
- [14] 李小勇,桂小林. 动态信任预测的认知模型[J]. 软件学报, 2010, 21(1): 163-176.
- [15] Calheiros R N, Ranjan R, Beloglazov A, et al. CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms[J]. Software: Practice and Experience, 2011, 41(1): 23-50.

作者简介:

王静宇 男, (1976-), 博士研究生. 研究方向为云计算与信息安全.

赵山杉(通讯作者) 男, (1989-), 硕士研究生. 研究方向为云计算访问控制. E-mail: calmshan@sina.com.

郑雪峰 男, (1951-), 教授, 博士生导师. 研究方向为信息安全.