云计算中基于 SLA 的服务可信协商与访问控制策略

胡春华^{①②*}, 陈晓红^②, 吴敏^③, 刘建勋^④

① 湖南商学院计算机与电子工程学院, 长沙 410205

② 中南大学商学院, 长沙 410083

③ 中南大学信息科学与工程学院, 长沙 410083

④ 湖南科技大学计算机科学与工程学院, 湘潭 412201

* 通信作者. E-mail: huch36@gmail.com

收稿日期: 2011-08-29; 接受日期: 2012-02-06

国家自然科学基金创新群体 (批准号: 70921001)、国家自然科学基金 (批准号: 61143004, 90818004)、湖南省自然科学基金 (批准号: 11FB004, 11JJ2033)、教育部人文社科基金 (批准号: 10YJC630080)、湖南省教育厅重点科研 (批准号: 11A062) 和湖南省重点学科建设资助项目

摘要 针对当前云计算中因服务提供者 (SP) 的信任保障机制缺失而容易被不可信服务消费者 (SC) 滥用的现象, 提出面向 SC 实体的服务可信协商及访问控制策略. 该策略首先依据系统信任规则来表达服务实体的可信程度, 然后通过求解 SC 实体的直接和间接信任推理空间建立信任证据的举证方法, 同时采用服务级别协议 (service level agreements, SLA) 构建交互双方的协商机制, 最后综合信任传递与迭代计算策略, 确定服务交互的 SLA 等级, 提供相应级别的服务, 从而达到访问控制的目的. 理论分析与实验结果表明, 该方法虽少量增加了协商的次数, 但能较好解决服务被滥用以及利用率不高的问题, 为云计算环境下信任协商研究提供一种有效的新方法.

关键词 云计算 服务级别协议 信任协商 访问控制 信任推理深度

1 引言

随着云计算技术的迅速发展, 网络中大量的计算、存储以及软件等各类资源均可封装转化为服务, 形成规模巨大的虚拟 IT 共享资源, 为计算机用户提供能力无限的资源服务^[1]. 由于在云计算这种分布式环境中既缺乏集中认证与授权中心来保障推荐信息来源的可靠性, 又因其高度开放的特征允许服务实体自由地加入或离开, 如服务发布或撤销等, 导致服务的可信问题面临着重大挑战^[1,2].

当前研究中, 常对服务消费者 (service consumption, SC) 如何选取最优的可信服务关注较多, 实际应用中, 服务提供者 (service provider, SP) 相对于 SC 实体来说显然更为重要. 现有服务访问机制下, SP 实体常只能被动接受 SC 实体的访问请求; 而 SP 实体由于自身信任机制的缺失, 容易被部分不可信的 SC 实体欺骗或攻击, 容易出现服务资源被浪费或滥用的问题^[3]. 因此, 如何提高 SP 实体辨识和判断 SC 实体的可信性, 避免不可信 SC 实体的攻击与欺骗, 从而有效保证 SP 实体的可用性具有非常

引用格式: 胡春华, 陈晓红, 吴敏, 等. 云计算中基于 SLA 的服务可信协商与访问控制策略. 中国科学: 信息科学, 2012, 42: 314-332, doi: 10.1360/112011-918

重要的研究意义. 目前, 针对 SC 实体的可信判断与评价机制的国内外研究依然较少, 从而导致目前的服务交互存在如下的矛盾: 一方面, 服务提供商需要尽可能的为 SC 提供有效服务; 另一方面, 不加区分的对所有 SC 提供服务就会导致被欺骗或资源被滥用^[3,4].

现实社会中, 常采用信任协商与评价机制来解决以上问题. 即先对资源的申请方进行信用评估, 然后依据信任评价的结果给予资源申请方相应的访问级别^[5]. 例如: 银行系统在用户申请信用卡时, 会先对用户进行评估, 其实质都在于获得对资源申请方的信任确认. 目前云计算中还较少见针对 SC 实体的信任评价及可信访问策略研究, 该类研究的开展有利于为该环境下的信任机制研究提供新思路.

本文针对以上不足, 提出了基于 SLA 的服务可信协商与访问控制的解决思路, 其核心思想为: 服务申请者只有递交能证明其访问某项资源的信任证明, 通过服务协商机制并依据 SC 实体的可信程度确定相应的服务级别协议 (service level agreements, SLA)^[6], 以达到访问控制的目的, 才可进行相关服务资源的访问, 实现对 SP 实体的保护, 提高服务资源的使用效率.

本文提出的解决策略主要如下: 首先根据 SP 和 SC 实体的交互行为来建立自己的信任与推理空间; 然后交互双方依据已有的信任关系进行推导, 按着要求进行信任举证, 通过双方协商的服务级别来获得有效的信任证据链; 最后通过开展综合信任传递与迭代计算, 确定两实体交互的服务级别协议 (SLA), 并提供相应级别的服务. 理论分析和实验结果表明, 该方法虽少量增加了服务双方协商的次数, 但能有效改变当前 SP 实体容易被欺骗和滥用的状况. 本文方法是对服务信任协商机制的有益补充, 为解决当前云计算环境下自动信任协商提供一种有益探索.

2 相关工作

关于云计算环境下服务的评价及访问方法, 国内外已开展了较深入研究, 归纳起来可分为以下两大类:

1) 不考虑服务实体可信的研究方法. 提出了如线性规划算法^[7]、启发式算法^[8]、HPSO 算法^[9]、迭代选择方法^[10]、协同动态调度^[11]等有效方法. 但这类方法都需具备以下条件: (i) 方法执行者对云计算中所有服务都了解; (ii) 服务提供的 QoS (quality of service) 信息都真实可信. 众所周知, 云计算环境下服务常动态变化, 访问机制难以对相关服务信息都知晓; 且在复杂的网络中常存在虚假甚至欺骗的服务实体, 因此假设所有服务宣称的 QoS 都真实显然不符合实际情况, 但不少方法能为可信环境下的服务访问提供参考.

2) 另一类研究认为互联网络中的服务实体不一定可信, 因此, 需要对服务实体进行信任表达、推理、评价及协商. 这类研究依据其研究的主题不同而有多种, 具体如下:

(i) 信任模型的表示方法研究. 对信任模型表示研究经历了较为长期的发展过程, 早期研究中, 对信任关系常采用一维的方法表示, 其属于社会关系的信任模型^[12]; 后来, Almenarez 等^[13]提出了二维或者三维的信任模型, 也称为信仰模型, 这些信任模型基于 Bayes 定理, 使用 $\text{belief}(b)$, $\text{disbelief}(d)$ 和 $\text{uncertainty}(u)$ 来表征其信任关系; 最近出现了利用 D-S 不确定推理理论^[14]或 Beta (β , β_a) 分布函数^[15]等表示多维信任模型, 并给出了信任关系传递、合并的计算方法较好地表征了信任关系.

(ii) 服务信任信息的获取与推理研究. 在实际中, 信任信息获取与演化对信任值的计算影响也非常大. 文献^[16]认为信任的推理与运算可根据实体的交互行为来判断, 因而将实体的交互行为看作其可信行为的重要度量标准, 基于这种思想的研究还有文献^[13]. 文献^[17]从服务提供者 and 使用者两个 QoS 数据来源的角度对质量属性进行分类获取和推理, 提高服务选择的准确性. 文献^[18]提出了基于

多代理器的解决策略, 它利用代理器与消费者和提供商之间的交互, 收集和管理全局信任信息, 这不失为一种解决方法.

(iii) 服务实体的信任评价研究. 该类研究主要通过实体间的交互信息来对服务实体的可信度进行评价, 将虚假服务排除在服务选择之外. 相关研究有: 文献 [19] 提出基于单声誉的系统, 但不能处理服务消费者 (SC) 不回馈的情况. 文献 [20] 提出基于双层的声誉系统, 但反馈信息不一致时, 难确定谁是撒谎者. 文献 [3] 通过引入相关因子来量化不同上下文中的推荐信任关系, 通过信任传递与迭代计算, 确定高声誉值的推荐信息源. 文献 [21] 通过依赖 SC 回馈的信息来评价服务提供者的可信度, 且默认 SC 回馈的信息是真实可信的, 也不能处理 SC 不汇报回馈的场景.

(iv) 服务信任协商机制研究. 通过对 SC 进行身份验证, 再提供服务虽是通用做法, 但在开放的网络中仍面临不少困难 [5]. 近年来, 云计算和服务计算中引入了动态按需服务的方式, 即在服务开始前需通过协商机制形成供应商和消费者之间的承诺, 将 SLA 作为服务双方关于服务内容、质量等方面的约定, 是保障服务质量和顾客满意度的有效途径 [6,22]. SLA 的提出能有效改变了以往研究中 QoS 与可信性的计算方法和策略, 使得服务交互双方的服务级别可以通过协商来确定, 满足 SLA 的服务才是用户所需的可信服务; 但是服务协商过程导致可信计算变得更加复杂, 使得 SP 实体提供信任保障的可信策略更具有挑战性.

3 系统模型定义及信任值表示

3.1 系统模型

与许多研究相同, 本文假设服务交互双方都可将各自的评价向外公布 (例如在服务代理中, 或在服务注册中心). 设集合 $SP = \{sp_1, sp_2, \dots, sp_m\}$ 表示系统中的 m 个服务提供者 (SP) 实体, 称为 SP 实体域.

每个 SP 实体在向服务代理注册时, 将声明自己能提供一系列的服务水平级别. 设服务实体 A 在 ti 时宣称能提供的一系列服务级别, 如:

$$SLA_{A,set}^{ti} = \{SLA_A^{1,ti}, SLA_A^{2,ti}, \dots, SLA_A^{s,ti}\}, \quad (1)$$

其中 ti 时刻的第 i 个服务级别表示为

$$SLA_A^{i,ti} = \{Q_{A,set}^{i,ti}, \cos t_A^{i,ti}, \text{Credit}_A^{i,ti}\}, (i = 1, 2, \dots, m), \quad (2)$$

其中 $Q_{A,set}^{i,ti} = (q_{A,i}^{1,ti}, q_{A,i}^{2,ti}, \dots, q_{A,i}^{u,ti})$ 为服务级别相应的服务质量标准集合, 其中 $q_{A,i}^{j,ti} (j = 1, 2, \dots, u)$ 表示实体 A 在 ti 时, 在第 i 个服务级别下第 j 个 QoS 值, 其中 u 为 QoS 的维数, 表示不同维的质量信息, 例如可用性、响应时间、计算能力等. 不同质量指标具有不同意义, 如可靠性应不低于 $Q_{A,set}^{i,ti}$ 中规定的指标值; 而响应时间则应小于等于规定值. $\cos t_A^{i,ti}$ 为达到实体 A 提供服务水平级别 i 时支付的服务价格; $\text{Credit}_A^{i,ti}$ 为达到实体 A 提供服务水平级别 i 时 SC 实体需要达到的可信度.

所有 SP 实体存储最近 tw 时间段内宣称的服务水平级别在服务信息发布中心存储如下:

$$SLA_{all} = \begin{bmatrix} SLA_{1,set} \\ SLA_{2,set} \\ \vdots \\ SLA_{m,set} \end{bmatrix} = \begin{bmatrix} SLA_{1,set}^{t1} & SLA_{1,set}^{t2} & \dots & SLA_{1,set}^{tw} \\ SLA_{2,set}^{t1} & SLA_{2,set}^{t2} & \dots & SLA_{2,set}^{tw} \\ \vdots & \vdots & & \vdots \\ SLA_{m,set}^{t1} & SLA_{m,set}^{t2} & \dots & SLA_{m,set}^{tw} \end{bmatrix}. \quad (3)$$

表 1 服务交互后的评价信息
Table 1 Evaluation information after services interaction

	SP ₁	SP ₂	SP ₃	...	SP _m
SC ₁	SLA _{1,1} ^r	SLA _{1,2} ^r	SLA _{1,3} ^r	...	SLA _{1,m} ^r
SC ₂	SLA _{2,1} ^r	SLA _{2,2} ^r	SLA _{2,3} ^r	...	SLA _{2,m} ^r
⋮	⋮	⋮	⋮		⋮
SC _n	SLA _{n,1} ^r	SLA _{n,2} ^r	SLA _{n,3} ^r	...	SLA _{n,m} ^r

集合 $SC = \{sc_1, sc_2, \dots, sc_n\}$ 表示系统中的 n 个服务消费者 (SC) 实体, 称为 SC 实体域.

服务交互过程中评价结果如表 1 所示, 评价矩阵共有 n 行代表 n 个 SC 实体, m 列代表 m 个 SP 实体. 在表 1 中设 SP 实体 A 对 SC 实体 B 协商后服务级别为评价值 $SLA_{A,B}^r$. 其是一个多维向量, 代表了 SP 实体 A 对 SC 实体 B 的最近的 w 次交互记录, 相关参数的设定及物理意义与式 (2) 相同.

3.2 信任度量的表示方法

在以往研究中, 往往只对 SP 实体的进行信任评价. 由于 SP 实体常提供可度量的 QoS 值, 因而用户可根据 SP 实体应提供的 QoS 值与实际提供的 QoS 差值来确定 SP 实体的可信度. 但是本文研究的是对 SC 实体的信任评价, 相对来说对 SC 实体的可信度评价较为困难. 主要原因如下:

- 1) SC 实体相对于 SP 实体来说稳定性更差, 更难以评价;
- 2) SC 实体不提供服务, 不能通过常用的 QoS 值比较来确定其可信度, 只能通过服务行为交互来完成.

设在指定服务级别协议下, 实体 A 的信任度指标为 k 个, 具体权重已由用户给定, 在 t_i 时刻其值如下:

$$Ins_A^{t_i} = (ins_A^1, ins_A^2, \dots, ins_A^k). \quad (4)$$

如果实体 A 对实体 B 在实际交互过程中表现出来的实际值为

$$Ins_{A,B}^{t_i} = (ins_{A,B}^1, ins_{A,B}^2, \dots, ins_{A,B}^k), \quad (5)$$

则依据信任判断函数可得到实体 A 对实体 B 的信任度值, 即

$$C_{A,B}^{t_i} = fc(ins_{A,B}^{t_i}, ins_A^{t_i}). \quad (6)$$

式 (6) 中, fc 是个抽象化函数, 可依据实际信任度指标而具体化. 例如: 两者在达成服务价格的 SLA 后, 若协商的价格为 ω , 而 SP 实体提供相应服务后, SC 实体实际支付的价格为 ε , 可根据 $\varepsilon - \omega$ 的差值来映射出信任度, 若为负值则认为 SC 实体 B 不可信, 负值绝对值越大, 则越不可信; 若大于或等于 0 则认为可信.

在这里 fc 是两者差距的正相关映射函数, 为了处理问题简单, 本文将 fc 函数的构造方法采用均一化方法进行处理, 其中 $C_{A,B}^{t_i}$ 被分为 11 个档次来分析, 具体构造方法, 限于篇幅, 请见附录. 同时需要指出的是, 实际的云计算环境下每个 SP 实体制定的 fc 函数可以不同, 其可依据自身的 fc 函数进行信任度评测, 以使自己能获得较好的利益, 这也比较符合社会网络的实际.

图 1 服务交互次数与可靠性的转换函数

Figure 1 Transform function between services interaction number and probability

在上面, SP 实体 A 得到了对 SC 实体 B 的信任度评价. 但对 SC 实体 B 的评价还不够全面, 例如: 两 SP 实体对同一 SC 实体的信任度评价都为 3, 但是, SP 实体 i 是进行了 9 次交互后得到的评价结果, 而 SP 实体 j 只进行了 1 次交互得到的结果. 显然, 两实体进行交互的次数越多, 对得到的评价结果更可靠, 而少数交互次数具有随机性. 因而 SP 实体 A 是进行多次交互后得到的评价结果具有更高的可信度.

本文中认为可信度是对服务实体的信任评价, 可靠性是对得到这些信任评价的自信程度; 而可信性是一个集合性术语, 它用来表示可用性及其影响因素: 可靠性、维修性及保障性等. 例如, 论文送到某专家去评审, 不同专家的打分都为 90 分, 但是熟悉该论文领域专家与不熟悉该论文领域专家给出的 90 分显然其可靠性是不相同的.

但是, 当前的可信评价中常没有考虑这些因素, 因此本文除了对实体进行信任评价时得到信任度外, 还给出得到此信任度是在多大可信条件下获得的. 为了与可信度相区分, 此处用可靠性来表示. 对此, 本文给出了可靠性的映射函数, 将服务交互的行为转化为可靠程度来表示, 具体如式 (7) 所示:

$$R(w) = w \cdot \frac{\zeta}{\sin 1} \cdot \sin \frac{1}{w}, \quad w > 0, \quad (7)$$

其中 w 为服务交互次数, 若 $w = 0$, 则 $R(w) = 0$; ζ 用来表示服务实体间初次交互值, 交互次数与可靠性的关系如图 1 所示. 式 (7) 是将交互次数映射为可靠性的函数, 其具有的特性是: 交互次数较少时有初始的可靠性, 且随着交互次数增多并增加.

综上所述, 我们把 SP 实体对 SC 实体的评价用二元组来表示

$$e_{A,B} = (T_{A,B}, R_{A,B}), \quad (8)$$

其中 $T_{A,B}$ 是实体 A 对实体 B 的可信评价, $R_{A,B}$ 是实体 A 对实体 B 的可靠性评价. $T_{A,B}$ 得到的方法如下: 设在时刻 tk 时, 实体 A 得到对实体 B 的信任度值为 $C_{A,B}^{tk}$, 那么 $T_{A,B}$ 的值如下式所示

$$T_{A,B} = \sum_{k=1}^w C_{A,B}^{tk} \cdot u(k)/w, \quad w \neq 0, \quad (9)$$

其中 w 为交互次数, $u(k) \in [0, 1]$ 是衰减函数, 用来对发生在不同时刻的直接信任信息进行合理的加权, 根据行为习惯, 对于新发生的服务交互行为应该给予更多的权重^[4], 衰减函数定义为

$$u(k) = \begin{cases} 1, & k = w, \\ u(k-1) = u(k) - 1/w, & 1 \leq k < w. \end{cases} \quad (10)$$

4 实体信任空间的建立

SC 实体向 SP 申请获得服务的前提是它向 SP 实体提供能证明自己信任度的信任证明 (证据链). SP 实体收到证据链后, 需对证据链的可信性进行检验和评价; 为了完成这些, SP 与 SC 实体都需依据信任演化机制, 从行为交互中得到实体间的信任关系, 建立各自信任空间, 从而识别和评价对方信任的真实性.

4.1 直接交互实体的信任评价

首先, SP 实体 A 记录了对其进行访问的 m 个 SC 实体的交互情况, 用矩阵 SLA_A^r 来表示. 矩阵 SLA_A^r 的第 k 行表示 SP 实体 A 对 SC 实体 k 在不同时刻交互情况的记录, 与式 (4) 的意义相同. 具体如式 (11) 所示

$$SLA_A^r = \begin{bmatrix} SLA_{A,1}^{i,t1}, & SLA_{A,1}^{j,t2}, & \dots, & SLA_{A,1}^{k,tw} \\ SLA_{A,2}^{i,t1}, & SLA_{A,2}^{j,t2}, & \dots, & SLA_{A,2}^{k,tw} \\ \vdots & \vdots & & \vdots \\ SLA_{A,m}^{i,t1}, & SLA_{A,m}^{j,t2}, & \dots, & SLA_{A,m}^{k,tw} \end{bmatrix}. \quad (11)$$

SP 实体 A 根据交互的情况, 依据式 (8) 给出每次交互行为后的信任评价, 形成下面的信任评价矩阵 $fc(A)$:

$$fc(A) = \begin{bmatrix} fc(SLA_{A,1}^{i,t1}), & fc(SLA_{A,1}^{j,t2}), & \dots, & fc(SLA_{A,1}^{k,tw}) \\ fc(SLA_{A,2}^{i,t1}), & fc(SLA_{A,2}^{j,t2}), & \dots, & fc(SLA_{A,2}^{k,tw}) \\ \vdots & \vdots & & \vdots \\ fc(SLA_{A,m}^{i,t1}), & fc(SLA_{A,m}^{j,t2}), & \dots, & fc(SLA_{A,m}^{k,tw}) \end{bmatrix}.$$

从而可以根据上述矩阵计算得到 SP 实体 A 的信任评价

$$C_A^r = \begin{bmatrix} C_{A,1}^{t1}, & C_{A,1}^{t2}, & \dots, & C_{A,1}^{tw} \\ C_{A,2}^{t1}, & C_{A,2}^{t2}, & \dots, & C_{A,2}^{tw} \\ \vdots & \vdots & & \vdots \\ C_{A,m}^{t1}, & C_{A,m}^{t2}, & \dots, & C_{A,m}^{tw} \end{bmatrix}. \quad (12)$$

式 (12) 表示了服务交互一段时间的信任评价值, 一般来说需转换为两个实体间总的信任评价值, 本文采用了如下方法将多个信任评价值综合为总信任评价值. 此时 SP 实体 A 对 SC 实体 B 总的构造方法如下

$$T_{A,B} = \mu(1)C_{A,B}^{t1} + \mu(2)C_{A,B}^{t2} + \dots + \mu(w)C_{A,B}^{tw}, \quad (13)$$

其中 $\mu(i)$ 函数与式 (10) 的定义相同. 由于 $C_{A,B}^{ti}$ 分为 11 个等级, 因而较高信任度的一次交互结果会使 T 成比例的增加, 就能使其信任度成比例的提高. 而 $\mu(i)$ 函数表示了时间因素对信任值的影响, 越是新的交互结果对结果影响越大, 而离现在远的交互行为对信任值的影响权重越小.

前面所述, 除了 SP 对 SC 实体的信任度评价, 还需得到信任评价的可靠性, 这与两实体的交互次数成函数关系, 可以通过对式 (12) 中一行的交互次数进行数值统计得到 $\gamma_{A,i}$. 采用式 (7) 的函数

$R(\gamma_{A,i})$ 计算出 SP 实体 A 对 SC 实体 i 的可靠性. 这样经过式 (13) 及式 (7) 的计算, 可将矩阵式 (12) 转换为对其的二元组评价.

$$\begin{bmatrix} C_{A,1}^{t1} & C_{A,1}^{t2} & \cdots & C_{A,1}^{tw} \\ C_{A,2}^{t1} & C_{A,2}^{t2} & \cdots & C_{A,2}^{tw} \\ \vdots & \vdots & & \vdots \\ C_{A,m}^{t1} & C_{A,m}^{t2} & \cdots & C_{A,m}^{tw} \end{bmatrix} \Rightarrow \begin{bmatrix} T_{A,1} & R_{A,1} \\ T_{A,2} & R_{A,2} \\ \vdots & \vdots \\ T_{A,m} & R_{A,m} \end{bmatrix}. \quad (14)$$

用下式表示 SP 实体 A 对所有交互过 SC 实体的信任评价为

$$C_A^{\text{all}} = [(T_{A,1}, R_{A,1}), (T_{A,2}, R_{A,2}), \dots, (T_{A,m}, R_{A,m})]. \quad (15)$$

4.2 间接交互实体的信任空间建立

经过前面的论述, SP 实体 A 能得到与其直接交互 SC 实体的信任评价向量 C_A^{all} , 但仅对有直接交互关系的信任判断还不够. 因此, 本小节研究 SP 实体如何向前进行信任推理, 建立更广泛的信任空间.

首先选取式 (15) 中信任度大于一定阈值的 SC 实体, 设其集合为 $SC_{\text{set}}^{T>\phi}$, 表示与 SP 实体 A 直接交互的且其信任度大于 ϕ 的 SC 实体集合. 而 $SC_{\text{set}}^{T>\phi}$ 集合中与未知的 SP 实体 z 交互的信息如式 (16) 所示. 式 (16) 中的矩阵表示了 $SC_{\text{set}}^{T>\phi}$ 集合与 SP 实体 z 直接交互的服务级别评价.

$$SLA_{I,z}^r = \begin{bmatrix} SLA_{Z,1}^{i,t1} & SLA_{Z,1}^{j,t2} & \cdots & SLA_{Z,1}^{k,tw} \\ SLA_{Z,2}^{i,t1} & SLA_{Z,2}^{j,t2} & \cdots & SLA_{Z,2}^{k,tw} \\ \vdots & \vdots & & \vdots \\ SLA_{Z,g}^{i,t1} & SLA_{Z,g}^{j,t2} & \cdots & SLA_{Z,g}^{k,tw} \end{bmatrix}. \quad (16)$$

而 SP 实体 z 公开对外宣称的 SLA 值为式 (3) 所示矩阵中的一行. 这样, 将 SC 实体给出的 $SLA_{I,z}^r$ 与 SP 实体 z 宣称值进行对比, 就可得对 SP 实体 z 的可信度. 例如 SC 实体 i 对 SP 实体 z 的可信度 $C_{Z,i}^{\text{ti}}$ 计算如下:

$$C_{i,z}^{\text{ti}} = \text{fc}(SLA_{Z,i}^{k,\text{ti}}, SLA_z^{k,\text{ti}}), \quad (17)$$

其中 $SLA_{Z,i}^{k,\text{ti}}$ 表示 SC 实体 i 对 SP 实体 z 在 ti 时刻服务水平级别为 k 的评价值; 而 $SLA_z^{k,\text{ti}}$ 表示 SP 实体 z 在在 ti 时刻宣称的服务水平级别, fc 函数表示对照 SC 给出的服务水平级别与 SP 实体宣称的服务水平级差异给出的 SP 实体 z 的信任度评价 $C_{i,z}^{\text{ti}}$. 这样综合所有 $SC_{\text{set}}^{T>\phi}$ 集合对 SP 实体 z 的信任值为式 (18) 所示

$$C_z^r = \begin{bmatrix} C_{1,z}^{t1} & C_{1,z}^{t2} & \cdots & C_{1,z}^{tw} \\ C_{2,z}^{t1} & C_{2,z}^{t2} & \cdots & C_{2,z}^{tw} \\ \vdots & \vdots & & \vdots \\ C_{g,z}^{t1} & C_{g,z}^{t2} & \cdots & C_{g,z}^{tw} \end{bmatrix}. \quad (18)$$

同样, 利用式 (13) 和数值统计得到 $\gamma_{A,i}$ 可以计算出 SC 实体对 SP 实体 z 的信任评价

$$C_{I,z}^{\text{all}} = [(T_{1,z}, R_{1,z}), (T_{2,z}, R_{2,z}) \cdots (T_{g,z}, R_{g,z})]. \quad (19)$$

图 2 服务实体的信任评价及推理过程

Figure 2 Reasoning process and trust evaluation of services entity

同时需要对上述不同 SC 实体的信任向量进行综合, 从而得到对 SP 实体 z 的信任评价. 综合方法为: 由于不同 SC 实体的可靠性不同, 显然可靠性高的实体评价结果更具有稳定性, 因而其权重越大; 反之, 则越小. 而整体的可靠性为所有 SC 实体可靠性的平均值.

$$C_{I,z} = (T_{I,z}, R_{I,z}), \quad (20)$$

其中, $T_{I,z} = \sum_{i=1}^g (T_{i,z} R_{i,z} / \sum_{i=1}^g R_{i,z})$, $R_{I,z} = \sum_{i=1}^g R_{i,z} / g$.

这样, 采用与本小节类似的计算方法推理出与其他 SP 实体的信任评价. 从而可得如图 2 所示的第 I 层所有 SP 服务实体的信任评价.

首先 SP 实体 A 推理出与其直接交互的 SC 实体的信任评价, 这些 SC 实体是属于与 SP 实体 A 信任推理的第一层. 因此, 在图 2 中用 I 表示信任推理 SC 深度为 I; 然后, 从第 I 层 SC 中选取信任度大于阈值 ϕ 的 SC 实体继续向前进行信任推理^[22], 因为只有可信实体才能得到较为可信的结论, 从而过滤掉可信度较低的实体, 用“×”表示该链路不可用; 依据本小节先前论述, 推理得到 SP 实体的信任评价, 由于此时推理出来的 SP 实体距离信任推理的出发点在 SP 实体中位于推理深度的第 I 层, 故标记为 SP 的第 I 层.

下面给出如何根据第 I 层的信任评价结果继续向前推理, 得到第 II 层 SC 与 SP 实体的信任评价. 式 (16) 的矩阵给出了第 I 层 SC 实体与第 I 层 SP 实体交互的服务水平级别情况. 第 I 层 SP 实体 Y 的可信服务水平级别可以从这些 SC 实体的评价中得到

$$SLA_Y^{j,t1} = \sum_{i=1}^g \left(SLA_{Y,i}^{j,t1} R_{i,z} / \sum_{i=1}^g R_{i,z} \right). \quad (21)$$

则依据式 (21) 可得实体 Y 的其他 SLA 值, 再对其他 SP 采用类似方法可得对第 I 层所有 SP 的

SLA 评价:

$$SLA_I^{\text{all}} = \begin{bmatrix} SLA_1^{i,t1}, & SLA_1^{j,t2}, & \dots, & SLA_1^{k,tw} \\ SLA_2^{i,t1}, & SLA_2^{j,t2}, & \dots, & SLA_2^{k,tw} \\ \vdots & \vdots & & \vdots \\ SLA_k^{i,t1}, & SLA_k^{j,t2}, & \dots, & SLA_k^{k,tw} \end{bmatrix}. \quad (22)$$

第 II 层的 SC 实体对第 I 层 SP 实体的信任评价类似于式 (16) 的评价, 而信任推理深度第 I 层的 SP 实体与第 II 层 SC 实体交互的服务水平级别可以从表 1 中获得, 同样, SP 实体 A 认为自己信任推理出来对第 I 层 SP 实体的信任评价是可信的, 用它来检验第 II 层 SC 实体的可信性.

这样, 综合式 (17)~(20) 的方法, 计算可得到对第 II 层 SC 实体的信任评价值为

$$C_{II,SC} = \{C_{I,1}C_{I,2}, \dots, C_{I,h}\}.$$

推理出第 II 层 SC 实体的信任评价后, 从而可类似于第 I 层 SC 实体向前推理一样, 可推导出第 II 层 SP 实体的信任评价, 如此递推, 由于信任评价的可信度会随着推理深度的加深而减弱; 因此, 一般会根据需要限定出最大信任的推理深度 len . 下面给出服务实体如何获得自己的信任空间算法.

本文的信任评价是采用层次推理法来进行的. 算法 1 是依据层次推理思路推导出相邻层 SP 和 SC 间的信任评价, 是第 I 层 SP 实体 A 对第 I 层 SC 实体的信任评价, 而不是对后续各层实体信任度的综合评价. 因此, 综合信任评价还需对这些实体的信任评价进行递推迭代计算. 具体如算法 2 所示.

经过算法 1 与算法 2 后, 即可得两两直接交互的信任空间以及 SP 实体 A 对信任空间内实体的综合信任评价. 下面即可依据 SP 实体的信任空间进一步与 SC 实体进行服务级别的信任协商及访问控制.

5 基于 SLA 的服务可信协商与访问控制策略

5.1 策略的主要思想

本文提出策略的主要思想为: SC 实体要访问 SP 实体提供的资源, SC 实体就必须提供能够证明自己可信度的“证据链”; 而 SP 实体依据自己建立的信任空间来判断 SC 实体提供的证据链是否满足 SC 访问资源所需的最低限度. 若满足, 则提供相应服务水平级别的服务; 若不满足, SC 实体可降低其服务水平级别的要求, 进行下一轮“证据链”举证, 直到满足 SP 实体访问的信用级别要求; 或因为 SC 实体无法给出新的“证据链”, 且已达到最大举证次数后, 仍不能达成协商, 则终止交互.

上述基于 SLA 的服务可信协商与访问控制策略中, 存在如下 3 个主要问题需解决:

1) 证据链包含的内容. 在云计算环境下, 无法采用严格的身份认证方式. 因此, SC 实体可提供自己以往的一些交互结果, 以及自己对其他实体的服务水平级别判断和评价; 然后 SP 实体根据 SC 实体的证据链给出其信任度.

2) SP 实体要求 SC 实体提供的“证据链”. 与社会交互活动类似, SC 实体越提供具有个体特征的“证据链”, 越容易证明其可信性, 不在于提供的多少, 而在于具有证明力.

因此, 本文中 SP 实体依据交互情况判断 SC 实体提供“证据链”的有效性, 用 $E_{A,B}^{\text{ev}} = \text{fe}(\text{evidence})$ 表示. $E_{A,B}^{\text{ev}}$ 表示 SP 实体 A 对 SC 实体提供的证据链 evidence 的有效性评价结论, 其值为 0 到 1 间

算法 1 服务实体信任空间的建立算法

```

1. begin
2. length ← I;
3. for each SCi in SCset(length)
4.   get all SCi.SLAA,is,tj; //得到每次 SC 实体与 A 交互的 SLA 评价
5.   get all CA,itj by using function fc; //得到 SP 实体 A 对每次交互的信任评价
6.   get (TA,i, RA,i) by using formula 13
7. end for
8. output of trust evaluation of SCset(length) //得到所有第 I 层 SC 实体的信任评价
9. while length < len // len 为最大信任推理深度
10.  for each SPj in SPset(length)
11.   for each SCi in SCset(length) and Ci.Credit > σ
12.    get SCi.SLAi,js,tj; //得到 SC 实体与 i 与 SP 实体 j 交互的 SLA 的评价
13.    compute Ci,jtj by using function fc; //依据式 (17) 得到 SC 实体 i 与 SP 实体 j 在 tj 时的信任评价
14.    compute (Ti,j, Ri,j) by using formula (13);
15.   end for
16.   compute CI,j by using formula (20); //计算出对第 length 层 SP 实体 SPj 的综合信任评价 CI,j
17. end for
18. output of trust evaluation of SPset(length) //计算出对第 length 层所有 SP 实体的综合信任评价
19. for each SPj in SPset(length)
20.  compute SLA evaluation SLAji,t1, SLAjj,t2, ..., SALjk,tw all of SC on entity SPj; // 计算所有 SC 实体对 SPj
    的 SLA 评价
21. end for
22. length = length + I
23. for each SCi in SCset(length)
24.   for each SPi in SPset (length-1)
25.    if SPi.Credit > σ
26.     compute Ci,jtj by using function fc
27.     compute (Ti,j, Ri,j) by using formula (13)
28.    end for
29.    compute Clength,i by using formula (20)
30.   end for
31. output of trust evaluation of SCset(length)
32. end while

```

的一个实数, evidence 为 SC 实体提供的证据链. fe 为 SP 实体 A 对证据链的判断函数, 不同的 SP 实体其 fe 函数不同, 具有个体差异, 这也符合复杂网络的现实.

3) SC 实体提供的证据链的可信度分析. 依据算法 1 和算法 2 得到 SP 实体的信任空间, 同时根

算法 2 SP 实体 A 对 SC 实体的综合信任评价算法

```

1. begin
2. run algorithm 1
3. Compute whole trust evaluation of  $SC_I$  by using approximately formula 20 for all of SC in  $I$ th layer;
4.   length= $I$ 
5.   while length<len
6.     for each SC entity  $SC_i$  in length layer
7.        $SP_i.C = \prod_{i=I-1}^{length-1} SP_i \prod_{i=I-1}^{length-1} SC_i \times SC_i.C$  //  $SP_A$  为  $SP_0$ , 其信任度为 1,  $SC_0$  也为 1
8.     end for
9.     for each SP entity  $SP_i$  in length layer
10.       $SP_i.C = \prod_{i=I}^{length} SC_i \prod_{i=I-1}^{length-1} SP_i \times SP_i.C$ 
11.    end for
12.    length=length+1
13.  end while

```

据式 (22) 得到对 SC 实体的 SLA 评价, 然后用类似于式 (17) 的方法计算出 SC 实体提供某一证据的信任值. 若 SC 实体提供的证据链中包含的证据较多, 有些证据可能没落到的 SP 实体信任空间中, 则只能依据实体自身宣称的 SLA 值来判断; SC 实体提供证据的可靠性则由 fe 函数得到值 $E_{A,B}^{ev}$, 对 SC 实体的整体评价为对多个证据的可靠性与可信度的加权平均. 显然, 证据链落在 SP 实体信任空间中和未落在该信任空间中这两种情况下得到信任值的重要程度是不一样的, SP 实体显然更愿意相信自己信任空间推理得到的信任值.

5.2 算法描述

算法的流程如图 3 所示. SC 实体首先发起服务请求, 并附上申请的服务水平级别以及初始的证据链; SP 实体收到服务请求后, 依据信任评价策略进行信任评价, 结果存在如下 3 种可能:

- 1) SC 实体信任度满足访问所需的服务水平级别要求, 则 SLA 协商成功, 并提供服务;
- 2) 若不满足服务水平级别的信任度, 且协商次数 m 小于最大协商次数 $S(\delta)$, 则与 SC 实体继续下一次的“证据链”举证; 如果 SC 实体能够提供更多的“证据链”, 则 SP 实体再次进行信任评估以决定下一步的行动, 如果 SC 实体没有更多的“证据链”可提供, 则协商不成功, 交互中止;
- 3) 协商次数达到最大的 $S(\delta)$, 则协商失败.

算法 3 给出基于 SLA 的服务可信协商与访问控制算法描述.

5.3 算法性能分析

本文 SP 对 SC 实体的信任评价与访问控制主要有如下 3 个关键点:

- 1) 服务交互双方建立如何各自的信任及推理空间;
- 2) 根据已有的信任关系进行推导, 并针对关键的信任证据进行举证及协商, 得到更准确的信任评价;

图 3 服务协议流程

Figure 3 Flow of services protocol

算法 3 基于 SLA 的服务可信协商与访问控制算法

1. begin
2. let $m=1$ //当前交互次数的计数
3. send a resource request to SP entity A with the "Chain of evidence" $SLA_{A,set}^{ti} = \{SLA_A^{1,ti}, SLA_A^{2,ti}, \dots, SLA_A^{s,ti}\}$
4. compute the trust level of SC entity B by using formula (17) with accumulative evidence
5. judge the trust level of SC entity B
 - case: meet the trust requirement and $m \leq S(\delta)$ then
 - go to step 6 /* 若满足当前 SLA 级别的信任度, 则协商成功, 更新 SC 的信任评价以及相关服务实体的信任度 */
 - case: $m > S(\delta)$ then go to step 8 // 如果协商次数达到最大次数 n , 则转结束;
 - case: other then do bellow /* 若当前提供的“证明”无法达到 SP 实体要求的可信度, 则继续进行协商 */
- 5.3.1 SP_A requests SC_B provider new evidence with "negotiation reference";
 - /* SP 实体依据协商信息将可靠性高实体作为“协商参考”, 减少协商的盲目性 */
- 5.3.2 if SC_B have new evidence then do bellow:
 - SC_B provide new evidence to SP_A
 - Goto step 4.
 - Else goto step 8.
 - end if /* SC_B 有新证据可提交, 则提交进行新一轮协商, 否则协商不成功, 转 step 8 */
6. SP_A negotiation SC_B with SLA success
7. SP_A provider service to SC_B
8. End.

3) 依据信任评价的结果, 确定 SP 与 SC 实体交互的服务级别协议 (SLA), 以提供相应级别的服务.

由上述可知, 本文提出的策略与以往研究主要不同在于第 2) 和 3) 点上有较大不同. 以往策略中都只对 SC 实体的访问请求进行信任评价, 再依据评价结果进行访问控制, 可被认为就是本文第 2) 点中的信任协商只进行 1 次交互的情况, 而本文策略相当于进行了 $k \geq 1$ 次交互的情况, 即为了提高信任评价的准确性需进行 k 次交互的情况. 客观来说, 性能评价及分析主要是对信任协商所付出的代价及对性能提高的分析.

现有策略归纳起来主要有如下 3 种情况:

1) 采用信任推理及 $k \geq 1$ 次信任协商来确定 SLA, 决定是否接纳 SC 实体的访问请求, 即为本文提出的策略; 记为 policy A.

2) 仅通过历史记录推理出信任度值, 采用信任推理策略决定是否接纳 SC 实体的访问, 并不进行信任协商, 如 STI^[21] 以及 ESBT^[23] 等; 该类方法统一记为 policy B.

3) 不进行信任推理的服务访问策略, SP 实体接纳每个 SC 实体的访问请求; 记为 policy C.

设 policy A 与 policy B 的 1 次信任评价结果的准确性是相同的, 而 policy A 要求 SC 实体 1 次访问 SP 实体时, 携带能证明自己可信性的信任凭证; 同时设这 3 种策略对 SC 实体信任度评价的准确性分别为 β_A , β_B 及 β_C . 下面对以上 3 种策略的信任识别准确率分析如下:

定理 1 设 SC 实体中可信实体的比例为 α , Policy A 设定信任识别的准确率为 δ , 则这 3 种策略的信任识别准确率为 $\delta \geq \beta_A \geq \beta_B \geq \beta_C = \alpha$.

证明 对于 Policy A, 设定最大的交互次数为 $S(\delta)$, 则其信任识别的准确率就可达到用户设定的值 δ , 显然多次交互获得的 δ 值不少于 1 次识别的 β_A , 从而可得 $\delta \geq \beta_A$.

由于 Policy A 服务交互时已携带了能证明其可信性的信任凭证, 而 Policy B 只能根据历史记录获得 1 次交互的信任识别准确率 β_B , 无法进行信任协商, 从而可得 $\beta_A \geq \beta_B$. 而 Policy C 没有进行任何信任识别; 因此, Policy C 的信任识别准确率可认为是交互的 SC 实体中可信实体的比例 α , 即 $\beta_C = \alpha$, 显然 Policy B 是在进行信任推理的基础上得到的信任识别准确率 β_B 不会小于 Policy C 的信任识别准确率 β_C , 即有 $\beta_B \geq \beta_C$.

综上所述有: $\delta \geq \beta_A \geq \beta_B \geq \beta_C = \alpha$. 定理 1 得证.

为了更清楚地给出定理 1 所表达的服务交互次数与信任识别准确性的关系, 下面通过数字分析方法给出一个具体例子. 如图 4 所示, 假设 Policy A 的信任识别准确率为 β_A , 其值从 0.5 增长到 0.85; 而应用需求的信任识别率 δ 分别为 0.9 和 0.95. 那么在这种情况下, Policy B 和 Policy C 不能解决这个问题; 而 Policy A 可以采用多次信任协商的办法来达到应用的需求, 当然付出了多次交互的代价.

那么 Policy A 付出的交互次数代价可用图 5 表示. 图 5 表示了 δ 分别为 0.9 和 0.95 下 Policy A 次数的最大交互次数与平均交互次数. 从图中可看出即使在 β_A 只有 0.5 的情况下, δ 达到 0.9 和 0.95 下的最大交互次数也分别只有 4 和 5 次, 而平均交互的期望值不到 2 次. 当获得的信任识别率上升时, 即 β_A 增大时, 从图 5 可看出, 其最大和期望交互次数均下降. 可见 Policy A 在付出交互次数代价不高情况下, 显著提高了信任评价的准确性. 其原因是在 SLA 信任协商中, SP 实体要求 SC 实体针对关键且其不能确认的证据链进行举证, 因而第 k 次信任识别准确率显然不会小于第 $k-1$ 的识别准确率. 即有 $\beta_A^k \geq \beta_A^{k-1}$.

下面对 policy A 策略的服务交互次数与复杂度的关系分析如下:

定理 2 设 SC 实体中可信实体的比例为 α , Policy A 设定信任识别的准确率为 δ , 则 Policy A

图 4 β_A 与 δ 的关系Figure 4 Relation between β_A and δ 图 5 交互次数与 δ 的关系Figure 5 Relation between interaction number and δ

策略的复杂度与服务交互次数的关系如下:

$$O(A) = n[1 - (1 - \beta_A)^{S(\delta)}] / \beta_A, \text{ 其中 } S(\delta) = \lceil \log(1 - \delta) / \log(1 - \beta_A) \rceil.$$

证明 由于 policy A 1 次识别的准确率为 β_A , 设系统每次交互的准确性都相同, 均为 β_A , 同时设系统需要的最少信任识别准确率为 δ , 则 $S(\delta)$ 为准确率设定为 δ 时的最大交互次数. $S(\delta)$ 的推导过程如下:

设最大的交互次数为 N , 相当于 N 个独立的 Bernoulli 实验, 它是服从服务交互次数最大为 N , 而且准确性都为 β_A 二项分布 (binomial distribution).

因此, $\delta(N, P) \cong P(X_p > 1) = 1 - (1 - \beta_A)^N$, 从而得到最大交互次数 $S(\delta) = \lceil \log(1 - \delta) / \log(1 - \beta_A) \rceil$.

但是信任评价的实际交互次数并不是每次为 $S(\delta)$, 在交互过程中, 只要 SP 实体能收集到信任凭证要求, 信任协商过程将终止. 因此, 服务交互行为实际的交互次数是一个截短几何分布 (truncated geometrically distributed *r.v.*). 它以识别准确性的概率为 β_A 从 $\{1, \dots, S(\delta)\}$ 中取值. 因此, policy A 策略对每个 SC 实体的平均交互次数 (期望的交互次数) 为下式:

$$E(x) = [1 - (1 - \beta_A)^{S(\delta)}] / \beta_A.$$

从而得到 Policy A 的复杂度 $O(A) = n[1 - (1 - \beta_A)^{S(\delta)}] / \beta_A$. 综上所述, 可得定理 2.

6 仿真实验与性能分析

为了更好地说明本文提出策略的有效性, 采用澳大利亚墨尔本大学 (The University of Melbourne) 开发的云计算仿真平台 CloudSim^[24] 开展仿真实验, 运用 BRITE 模拟服务拓扑结构. 为了使实验环境贴近真实开放的云计算实际场景, 设置了服务交互场景以及相应的 SP 与 SC 实体, 其中 SP 实体设置成 3 种类型, SC 实体设置成 4 种类型, 具体设置场景与作者在文献 [4] 的设置相同, 限于篇幅, 此处不在赘述. 下面验证本文策略是否能识别这 4 类 SC 实体, 保障 SP 实体不受或少受不可信服务实体的欺骗、滥用或攻击, 提高服务利用率.

本节实验设置的 SP 实体总数是 1000 个, 其中 SP(1) 类实体占 80%, SP(2) 类和 SP(2) 类实体各占 10%. SC 实体的总数是 2000, 其中 Sc(1) 类实占 60%, Sc(2) 类和 Sc(2) 类各占 10%, Sc(4) 类占 20%. 这样设置的真实服务实体大于恶意实体比例, 与实际情况较相符. 实验的交互过程是以轮 (rounds) 为单位, SP 实体 A 与 SC 实体 B 在每轮中交互的个数为 10 个, 每轮结束后, 再统计此轮中的交互情况.

图 6 不同策略对 SC(2) 实体的识别率

Figure 6 Ratio access with SC(2) under different policies

图 7 不同策略对 SC(1) 实体的识别率

Figure 7 Ratio access with SC(1) under different policies

图 8 不同 SC 实体的平均可信度变化

Figure 8 Change ratio of average trust of different SC

图 9 不同策略下 SC(1) 实体的平均可信度变化

Figure 9 Change ratio of average trust of SC(1) under different policies

图 6 给出了 3 种不同策略下, SP 实体与 SC(2) 实体交互的情况. 从图中可看出, 由于 SC(2) 实体存在恶意欺骗且有共谋主体的特征, SP 实体 A 给出自己可靠性 >0.7 的实体, 让 SC(2) 实体“协商参考”, 从而在协商过程确保其可信度. Policy A 能较快识别不可信的 SC 实体, 因而与 SC(2) 实体进行交互次数将快速减少; 之所以有交互行为是网络开始时 SC(2) 从未与其他实体交互过, 无法确定其可信性; 而当该类 SC 实体提出访问请求时, 无法确定可信性的情况给予其最低的访问级别, 即在确定其可信性低于 0 时, 禁止其访问.

各类服务实体的活动频率基本相等情况下, 对于 Policy B 策略, 由于进行了信任推理, 因而也能随着服务交互的进行, 受到 SC(2) 实体欺骗的概率将下降, 但下降速度不如 Policy A. 至于 Policy C, 由于是没有任何机制进行识别和访问控制, 因而受到 SC(2) 欺骗的概率与 SC(2) 实体在网络中的比例相类似.

图 7 给出的是在 3 种不同策略下与 SC(1) 实体交互的情况. 从图中可看出与上面类似的规律, 在 Policy A 的策略下, 经过较少交互次数就将 SP 实体与 SC(1) 的交互比例提高到较高的场景, 说明本文提出的策略能较快地识别真实的 SC 实体, 从而与这些可信实体的交互比例非常高. 同样也可得到 SP 实体与 SC(2) 与 SC(4) 实体的交互规律, 限于篇幅不能一一给出.

图 8 为本文策略下不同 SC 实体类型的平均可信度变化情况. 从图中可看出在交互次数不多时, SC 实体的可信度都不高, 接近于 0. 但是随着交互次数的增长, SC(1) 实体的平均可信度向上增长, 而恶意实体 SC(2) 的平均可信度下降较快, 而随机实体 SC(4) 的平均可信度在 0 上下波动. 说明本文提出的策略能有效甄别不可信服务实体和可信服务实体的信任度.

图 9 给出的是不同策略下 SC(1) 实体的可信度变化情况. 与前面的规律类似, 本文提出的策略能在较少交互次数情况较好地确定服务实体的可信度.

图 10 不同类别实体得到的服务水平级别

Figure 10 Services lever of different sort entity obtained

图 11 SP 实体与可信实体交互的关系

Figure 11 Relation between SP entity and trust interaction

图 12 信任协商次数统计

Figure 12 Stat. of trust negotiate number

图 13 信任推理深度与性能的关系

Figure 13 Relation between trust inference depth and capability

图 10 给出是不同类别 SC 实体得到的平均服务水平级别情况. 图 10 中服务水平级别是依据本文策略依据信任度而给 SC 服务实体分配的资源访问等级, 而 Policy B 与 Policy C 并没有服务水平级别. 图 10 的数据是依据 Policy A 的策略换算出来的, 表明可信服务实体能得到更好的服务水平级别, 而不可信实体得到的服务水平级别很低. 由上述可见, 本文提出的策略能保障服务资源的有效利用.

图 11 给出了不同策略下 SP 实体与可信实体交互的比例, 实际上是指 SP 服务实体不受欺骗或攻击访问的次数, 它反映了服务资源没有被攻击、滥用或欺骗的情况, 也反映了服务资源有效利用的问题.

图 12 给出了本文提出的策略中协商次数的统计情况. 表明协商大部分在 2 次以后即可完成, 说明本文提出的策略虽增加了协商次数, 但交互代价不大, 其付出的代价完全可以接受, 且与图 5 分析的情况相近.

图 13 中的上图给出了推理层次深度与推导出的实体个数关系图. 表明采用层次推理方法可在很小推理层次时获得对较多实体的信任评价, 呈几何级数增长. 图 13 中的下图给出了不同推理深度与实体信任评价准确性的关系. 可见开始阶段随着推理层次增多, 推理得到的可信度也随之增长, 但推理深度超过 4 后, 其可信度不升反而下降. 表明随着推理层次增多, 评价中干扰和不确定因素增多, 影响了评价的准确性.

7 结束语

本文针对当前云计算中 SP 实体常得不到保护, 采取了面向 SC 实体的 SLA 服务可信协商及访问

控制的新方法来解决该问题. 虽增加了服务交互的协商次数, 但能较好地保护 SP 实体, 减少 SP 实体被不可信 SC 实体欺骗及滥用等现象, 提高了服务资源的利用率. 本文的策略是对服务信任协商机制的有益补充, 较适合于开放、弱认证的可信服务环境, 能为当前云计算环境下自动信任协商提供一种有效探索.

下一步研究准备通过满足实际的复杂应用来完善服务可信的协商机制, 如加入混沌加密等密码技术, 防止协商双方不断暴露证书与访问控制策略时, 受到外界的破坏与攻击; 同时引入更好的结果反馈机制, 提高信任协商的成功率等.

致谢 本文有幸获得“第二届中国云计算与 SaaS 大会”的最佳论文奖, 在此对所有提出宝贵意见的论文审稿人以及现场答辩的专家表示感谢.

参考文献

- 1 Armbrust M, Fox A, Griffith R, et al. A view of cloud computing. *Commun ACM*, 2010, 53: 50–58
- 2 Michael H, Munindar P S. Service-oriented computing: key concepts and principles. *IEEE Internet Comput*, 2005, 9: 75–81
- 3 Zaki M, Athman B. Reputation bootstrapping for trust establishment among Web services. *IEEE Internet Comput*, 2009, 13: 40–47
- 4 Hu C H, Luo X X, Wang S C, et al. Approach of service evaluation based on trust reasoning for cloud computing. *J Commun*, 2011, 32: 72–81 [胡春华, 罗新星, 王四春, 等. 云计算环境下基于信任推理的服务评价方法. *通信学报*, 2011, 32: 72–81]
- 5 Liao Z S, Jin H, Li C S, et al. Automated trust negotiation and its development trend. *J Softw*, 2006, 17: 1933–1948 [廖振松, 金海, 李赤松, 等. 自动信任协商及其发展趋势. *软件学报*, 2006, 17: 1933–1948]
- 6 Zulkernine F, Martin P, Craddock C, et al. A policy-based middleware for Web services SLA negotiation. In: *Proceedings of the IEEE International Conference on Web Services*, Los Angeles, 2009. 1043–1050
- 7 Cardoso J, Sheth A, Miler J, et al. Quality of service for workflows and Web service processes. *J Web Semantics*, 2004, 13: 281–320
- 8 Oh S C, Lee D W, Kumara R T S. Effective Web service composition in diverse and large-scale service networks. *IEEE Trans Serv Comput*, 2008, 1: 15–32
- 9 Hu C H, Wu M, Liu G P. QoS scheduling algorithm based on hybrid particle swarm optimization strategy for Web services workflow. In: *Proceedings of the 6th International Conference on Grid and Cooperative Computing*, Urumchi, 2007. 330–337
- 10 Su S, Li F, Yang F C. Iterative selection algorithm for service composition in distributed environments (in Chinese). *Sci China Ser E-Inf Sci*, 2008, 38: 1717–1732 [苏森, 李飞, 杨放春. 分布式环境中服务聚合的迭代选择算法. *中国科学 E 辑: 信息科学*, 2008, 38: 1717–1732]
- 11 Jiang W J, Zhang L M, Wang P. Dynamic scheduling model of computing resource based on MAS cooperation mechanism. *Sci China Series F- Inf Sci*, 2009, 52: 1302–1320
- 12 Marsh S. Formalizing trust as a computational concept. *Doctoral Dissertation*. Stirling: University of Stirling, 1994
- 13 Almenarez F, Marin A, Campo C. TrustAC: Trust-Based access control for pervasive devices. In: *Hutter D, Ullmann M, eds. SPC 2005*. Berlin: Springer-Verlag. 2005. 225–238
- 14 Rosenberg F, Celikovic P, Michlmayr A, et al. An end-to-end approach for QoS-aware service composition. In: *Proceedings of the 13th IEEE International Enterprise Distributed Object Computing Conference*, Auckland, 2009. 151–160
- 15 Zheng Z B Michael R. Optimal fault tolerance strategy selection for Web services. *Int J Web Serv Res*, 2010, 7: 21–40
- 16 Suryanarayana G. Selection and architecture-based composition of trust models in decentralized applications. *Doctoral Dissertation*. Irvine: University of California. 2007

- 17 Damiani E, Vimercati S D, Paraboschi S. A reputation based approach for choosing reliable resources in P2P networks. In: Proceedings of ACM conference on Computers and Communications Security. New York: ACM Press, 2002. 18–22
- 18 Liman N, Boutaba R. Assessing software service quality and trustworthiness at selection time. IEEE Trans Softw Eng, 2010, 36: 559–574
- 19 Jurca R, Faltingsi B. Eliciting truthful feedback for binary reputation mechanisms. In: Proceedings of the 2004 IEEE/WIC/ACM International Conference on Web Intelligence. Los Alamitos: IEEE Computer Society Press, 2004. 214–220
- 20 Pan J, Xu F, Lu J. Reputation-based recommender discovery approach for service selection. J Softw, 2010, 21: 388–400
[潘静, 徐锋, 吕建. 面向可信服务选取的基于声誉的推荐者发现方法. 软件学报, 2010, 21: 388–400]
- 21 Li L, Wang Y. Subjective trust inference in composite services. In: Proceedings of the 24th AAAI Conference on Artificial Intelligence, Atlanta, 2010. 1377–1384
- 22 Skene J, Raimondi F, Emmerich W. Service-level agreements for electronic services. IEEE Trans Softw Eng. 2010, 36: 288–304
- 23 Tian L Q, Lin C, Ni Y. Evaluation of user behavior trust in cloud computing. In: Proceedings of the 2010 International Conference on Computer Application and System Modeling, Taiyuan, 2010. 567–572
- 24 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. Softw Pract Exp, 2011, 41: 23–50

附录 fc 函数的构造方法

在本文中为了处理问题的简单, 采用均一化的方法进行处理, 将不同的信任度量单位化成统一信任度量单位, 在本文中将 $C_{A,B}^{ti}$ 分为 11 个档次, 正的 1 到 5 表示正向的信任度的值, 负的 1 到 5 表示负向的信任度的值, 0 表示中性的信任度的值, 具体分为以下 3 步:

1) 首先对信任信息进行均一化处理:

$$S_A^i = \xi_i(\text{ins}_A^i) \quad // \text{表示实体宣称的信任值,}$$

$$S_{A,B}^i = \xi_i(\text{ins}_{A,B}^i) \quad // \text{表示实际交互中实体获得的信任值.}$$

2) 假设由用户来指定 k 中的权重值, 并按权重记差值

$$J_{A,B} = \frac{\sum_{i=1}^k \{\omega_i(S_{A,B}^i - S_A^i)\}}{k} \quad \text{其中} \quad \sum_{i=1}^k \omega_i = 1.$$

3) 转换成信任度为

$$C_{A,B}^{ti} = fc(\text{ins}_{A,B}^{ti}, \text{ins}_A^{ti}) = \begin{cases} 5, & \text{if } J_{A,B} \geq 5\Delta, \\ 4, & \text{if } J_{A,B} \geq 4\Delta \wedge J_{A,B} < 5\Delta, \\ 3, & \text{if } J_{A,B} \geq 3\Delta \wedge J_{A,B} < 4\Delta, \\ 2, & \text{if } J_{A,B} \geq 2\Delta \wedge J_{A,B} < 3\Delta, \\ 1, & \text{if } J_{A,B} \geq \Delta \wedge J_{A,B} < 2\Delta, \\ 0, & \text{if } J_{A,B} \geq 0 \wedge J_{A,B} < \Delta, \\ -1, & \text{if } J_{A,B} \geq -\Delta \wedge J_{A,B} < 0, \\ \dots & \\ -5, & \text{if } J_{A,B} \leq -5\Delta. \end{cases}$$

采用上述方法可以得到评价的信任值.

A service trust negotiation and access control strategy based on SLA in cloud computing

HU ChunHua^{1,2*}, CHEN XiaoHong², WU Min³ & LIU JianXun⁴

1 School of Computer and Electronic Engineering, Hunan University of Commerce, Changsha 410205, China;

2 School of Business, Central South University, Changsha 410083, China;

3 School of Information Science and Engineering, Central South University, Changsha 410083, China;

4 School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 412201, China

*E-mail: huch36@gmail.com

Abstract The paper is concerned with the problem that the service is easily abused by dishonesty SC (service consumer) because of the lack of trust security mechanism for SP (service providers) in current cloud computing environment. A trust negotiation and access control strategy of SC Oriented is proposed in this paper. Firstly, the credible degree of services entity is expressed by the system trust rule in this strategy. Secondly, quoted method of trust evidence is established through solving the direct and indirect trust reasoning domains of service entity, and the negotiation mechanism of mutual sides is designed through SLA (service level agreements). Finally, the methods of trust transfer and iterative calculation are synthesized for ascertaining the SLA level of service intercommunion between SP and SC entity, and providing corresponding levels of service. It may achieve the purpose of service access control. Theoretical analysis and experimental results indicate that the method may increase the times of both sides negotiation, but can better resolve the problems of current service abused and low utilization. It is a new effective method for the study of trust consultation in cloud computing environment.

Keywords cloud computing, service level agreements, trust negotiation, access control, trust reasoning depth

HU ChunHua was born in 1973. He received his Ph.D. degree in computer science from Central South University, Changsha in 2007. Currently, he is an Associate Professor in the School of Computer and Electronic Engineering at Hunan University of Commerce. His research interests include cloud computing, service computing and dependability computing. Dr. Hu is a member of China Computer Federation.