基于信任合成的云服务动态组合机制研究

杨 震[1,3],杨甜甜[1],范科峰[2],王 勇[3]
(1. 北京工业大学计算机学院,北京 100124; 2. 中国电子技术标准化研究院,北京 100007;
3. 桂林电子科技大学广西高校云计算与复杂系统重点实验室,广西桂林 541004)

摘 要: 云计算为代表的新型计算模式以灵活的"服务合约"为核心商业特征,通过动态整合各类云服务为用户提供不同粒度的增值服务.但是传统以QoS(Quality of Service,服务质量)为核心约束的服务组合方法,无法满足用户对服务服务质量的深层要求,即对服务信任程度的规范.为此本文提出了一种基于信任合成的云服务动态组合方法,该方法通过定义云服务的信任属性,将其分解为基础信任和经验信任的集合.将基础信任评价问题建模为云服务属性判断问题,利用Bayes合情推理分析了属性不可穷举情况下基础信任的审定与反驳.将经验信任评价问题建模为云服务交互行为判断问题,利用Chebyshe和Bernstein定理给出经验信任的置信度,进而为经验信任的量化提供依据.实验结果表明,本文所提出的方法可以在持续变化的云环境下有效地组织和提供云服务,进而满足新型计算模式动态多样化应用需求.

关键词: 云服务; 服务组合; 信任合成; 基础信任; 经验信任
中图分类号: TP311 **文献标识码:** A **文章编号:** 0372-2112 (2018)03-0614-07
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.03.015

Cloud Service Composition Based on Trust Combination

YANG Zhen[1,3], YANG Tian-tian[1], FAN Ke-feng[2], WANG Yong[3]
(1. *College of Computer Science, Beijing University of Technology, Beijing* 100124, *China*;
2. *China Electronics Standardization Institute, Beijing* 10007, *China*;
3. *Guangxi Colleges and Universities Key Laboratory of Cloud Computing and Complex Systems, Guilin University of Electronic Technology, Guilin, Guangxi* 541004, *China*)

Abstract: With flexible SLA (Service Level Agreement) as the core business characteristic, cloud computing provides users with different value-added services through dynamic integration of various types of cloud services. However, in the traditional approach to service composition, with QoS (Quality of Service) as the core constraint, trust degree of the service can not be well regulated. This paper proposes a new approach to autonomous and flexible composition and management of could services with trust integration as its core feature. In this approach, the trust property of a cloud service consists in the combination of basic trust and experience trust. The basic trust is defined as the basic elements of the object with the Bayes reasoning analysis, while the experience trust defined as the behavior history between objects with its confidence given by Chebyshe and Bernstein inequality equation. A series of experiments on a prototype are conducted to verify the accuracy and validity of the mechanism proposed. The results show that the proposed approach is effective in composing and selecting services on the cloud.

Key words: cloud services; services composition; trust combination; basic trust; experience trust

1 引言

近年来,以云计算为代表的新型计算模式呈现出海量、动态、自主、协同、演化等特征,为了适应服务模式的改变和多样的应用需求,云计算需要以更加灵活、适应的方法来有效地管理和提供云服务[1].目前许多云服务提供商,包括亚马逊、阿里巴巴、Facebook、谷歌和百度等,已经部署了大规模云服务平台并进行商业运营.但随着服务模式的高度弹性和个性化发展,用户普遍希望云服务平台提供功能更加复杂、组合式、易扩展的云服务,这势必要求云计算以灵活的"服务合约"为核心商业特征,通过动态整合各类云服务为用户提供

收稿日期:2016-07-04;修回日期:2016-10-31;责任编辑:梅志强
基金项目:国家自然科学基金(No.61671030);北京市优秀人才,北京市属高校青年拔尖人才(No.CIT&TCD201404052);广西高校云计算与复杂系统重点实验室资助(No.15205)

不同粒度的增值服务.

从服务计算的角度看来,典型云计算系统,包括基础设施即服务(IaaS,Infrastructure as a Service)、平台即服务(PaaS,Platform as a Service)、软件即服务(SaaS,Software as a Service),都可以看成是某种服务,只是其提供的服务粒度不同而已. 早在 1961 年,计算机先驱 John McCarthy 就预见到"未来的计算能够如同公共设施一样组织管理"[2]. 时至今日,云服务计算已经达到极大的规模和极高的复杂性,Facebook 拥有超过十几亿个活跃用户,每年共产生 180PB 数据,每天上传 3 亿 5 千万张图片;淘宝注册会员超过 3.7 亿人,占中国网购市场 80% 的份额,每年的交易额超过了 1 万亿人民币,超过亚马逊公司和 eBay 之和. 要实现这样商业级的云服务,需要一种有效、灵活和自治的方法来管理这些服务资源. 因此,针对如何管理、组合及提供动态变化环境下的云服务资源以满足多样应用的需求,已经成为工业界和学术界关注的热点问题.

令人遗憾的是,传统以 QoS 为核心约束的服务组合方法,无法满足用户对服务质量的深层要求,特别是对云服务信任程度的规范. 目前,已经有众多研究者针对云服务组合开展了研究. Alrifai 等[3]将 QoS 全局约束分解为满足用户偏好的局部约束,通过混合整数规划方法获得最优的组合服务. Parejo 等[4]提出了一种 QoS 感知的 Web 服务组合方法 GRASP. 刘必欣等[5]提出一种基于角色的分布式动态服务组合方法,通过划分组合服务的全局流程模型产生各个角色的本地流程模型,从而使得组合服务的控制逻辑及执行负载能够对等地分布到多个结点. 夏亚梅等[6]针对服务组合优化及适应服务组合优化过程中 Web 服务的动态性,不稳定性以及多种 QoS 属性限制等问题,提出一种多信息素动态更新的蚁群算法 MPDACO. 从中不难发现,虽然云计算环境下服务资源非常丰富,但还存在动态变化、自治性强、安全难控等特征,使得用户要获得理想的组合服务异常困难. 究其原因,主要是因为传统以 QoS 为核心约束的云服务组合方法,无法满足用户对服务服务质量的深层要求. 云服务提供商通过同用户签订服务等级协议(SLA,Service Level Agreement)的形式,向用户提供服务,但传统 QoS 指标大多针对服务提供的计算能力、存储能力、服务时间以及计费形式进行约束,缺乏对即对服务信任程度的规范. 而信任属性作为重要的安全支撑属性,对于界定服务质量,并最终为用户提供安全可靠的云服务组合起到重要作用. 特别是,当考虑到云服务将跨越不同等级的计算资源(例如私有云、公共云等),组合高度差异性和自相似的服务的时候,对云服务信任属性的度量显得尤其重要.

综上所述,本文提出了一种云服务动态组合方法,该方法通过定义云服务的信任属性,将其分解为基础信任和经验信任的集合. 将基础信任评价问题建模为云服务分解属性判断问题,利用 Bayes 合情推理分析了属性不可穷举情况下基础信任的审定与反驳. 将经验信任评价问题建模为云服务交互行为判断问题,利用 Chebyshe 和 Bernstein 定理给出经验信任的置信度,进而为经验信任的量化提供依据. 最后结合一系列的仿真实验来验证本文提出机制的准确度和有效性. 实验结果表明所提出的方法可以在持续变化的云环境下有效地组织和提供云服务,进而满足新型计算模式动态多样化的应用需求.

2　基于基础信任和经验信任的信任评估机制研究

尼克拉斯·卢曼[7]认为信任是一种简化机制,将包围着我们的复杂性和不确定性变为二元关系,即可以相信还是不可以相信. 借由这样的简化机制,人们得以建立相互之间的合作与竞争关系. 目前关于信任的定义有许多讨论,不同的学者给出了不同的阐释,没有达成一致的意见. 多年来研究者从不同的角度,研究者对于信任的概念提出了很多不同的表述:社会科学家倾向于将信任归结于外部社会,环境和组织对人行为决定性影响,以及内在生物机制对个人决策的影响,并利用博弈理论对其进行研究[8]. 心理学家将信任看成一种关于实体在某一特定方面行为的可靠性观点,这种可靠性的观点并不是固定的,而是随着实体行为和时间的变化而变化的[9]. 本文在结合信任的生理学证据和社会学人际关系模型基础上,借鉴可信计算的概念,构造基于基础信任/经验信任的信任合成机制.

2.1　信任属性描述

结合信任的生理学证据和社会学人际关系模型基础上,借鉴可信计算的概念,将信任对象(TU,Trust Unit)抽象为基础信任(BT,Basic Trust)和经验信任(ET,Experience Trust)的二元组:

$$TU = (BT, ET) \tag{1}$$

概括而言,如果一个信任对象 TU 的行为总是与预期相一致,则可称之为可信的(trustworthy)[10,11]从服务计算的角度看来,信任对象 TU 的可信性的核心是基于身份的访问授权与控制,即要求确定身份的主体对资源进行合规操作. 这实际上包含两个层面的信任问题:

(1)信任对象的基础信任属性. 我们将信任的本质视为对象的客观属性,即信任依附于对象而存在,随着对象的产生而产生,随着对象的消亡而消亡. 不能脱离对象本身考虑信任问题,信任属性与对象身份绑定,由对象本身的所处的状态所决定. 因此在 2.2 节中将主体及其自然延伸的可信性定义为基础信任,并将其抽象

为系列属性的蕴含. 并利用 Bayes 合情推理模型分析了属性不可穷举情况下,基础信任的审定与反驳机制.

(2)信任对象的经验信任属性. 我们将经验信任定义为对象交互产生信任的主观测量. 信任虽然为对象的客观属性,但这样的属性可能难以表达、测量和评估. 其他主客体只能通过与对象的交互产生对其信任的主观测量. 因此在 2.3 节中基于人类社会交互和协作机制,给出了经验信任的定义. 利用 Chebyshe 不等式和 Bernstein 不等式,给出了样本容量、估计置信区间和置信度之间的关系:当确定置信区间 ε 后,当样本容量 $m \geqslant p^2(1-p)^2/\varepsilon^2$,对节点的信任度 P 进行估计的置信度开始为正,同时当 $m \geqslant \ln(4)(P^2(1-P)^2+\varepsilon/3)/\varepsilon^2$ 后,以指数速度逼近 1.

2.2 基础信任的审定与反驳

定义 1 为了保证信任对象 TU 所发出的操作均是其意图的如实反映,必须确保主体及其自然延伸属性的可信性. 主体自然属性包括主体的身份,计算能力等,其自然延伸包括其可能的运行平台,操作环境等. 这样一来,可以将基础信任抽象为其蕴含的系列结论 $\{C_i\}_{i=1}^{\infty}$. 即主体对象可以是基础可信的(T 状态)或基础不可信的($\overline{T}$ 状态). 当主体对象 TU 满足系列结论 $\{C_1, C_2, C_3, \cdots\}$,即

$$T \rightarrow \{C_1, C_2, C_3, \cdots\} \tag{2}$$

我们称其是基础可信的,或 T 状态. 当主体对象 TU 不能全部满足系列结论,我们称其是基础不可信的,或 $\overline{T}$ 状态.

这样可以通过判断信任对象 TU 蕴含的结论是否成立来断定其是否处于基础可信状态. 其中结论 C_1, $C_2, C_3, \cdots$,即为平台处于基础信任状态下所应具有的属性. 由于蕴含结论可能有多个,甚至是无数个相互关联的属性结论组成. 在属性结论无法穷尽的情况下,无法使用穷举的方法进行证明. 那如何选取属性结论验证从而对基础信任进行审定和反驳,就成为了一个关键的研究问题. 基于属性间概率计算关系的进行合情推理[12],我们给出命题 1.

命题 1(基础信任审定) 主体对象是基础可信的,或处于 T 状态,即:

$$T \rightarrow \{C_1, C_2, C_3, \cdots\} \tag{3}$$

那么,每个属性 C_i 的证实,都会使系统处于 T 状态的猜测变得更可靠,且其发生概率增加的程度和结论 C_i 本身发生的概率 $P(C_i)$ 及 $\overline{T}$ 状态下发生的概率 $P(C_i|\overline{T})$ 成反比.

证明 系统是基础可信的,即 $T \rightarrow \{C_1, C_2, C_3, \cdots\}$,得到

$$P(C_i|T) = 1 \tag{4}$$

由全概率公式可得

$$P(T|C_i) = \frac{P(T)P(C_i|T)}{P(C_i)} = \frac{P(T)}{P(C_i)} = \frac{P(T)}{P(C_iT)+P(C_i\overline{T})} = \frac{P(T)}{P(T)+(1-P(T))P(C_i|\overline{T})} \tag{5}$$

$P(T|C_i)$ 即表示证实 C_i 后,T 的可靠性. 由上式可得 $P(T|C_i) > P(T)$,即每个属性 C_i 的证实,都会使系统处于 T 状态的猜测变得更可靠,且其发生概率增加的程度和结论 C_i 本身发生的概率 $P(C_i)$ 以及 $\overline{T}$ 状态下发生的概率 $P(C_i|\overline{T})$ 成反比.

命题 2(基础信任反驳) 对每个属性 C_i 的反驳,都会使系统处于 T 状态的猜测变得更不可靠,即系统处于 $\overline{T}$ 状态的可能性增加,且其概率增加的程度和对结论 C_i 反驳概率 $P(\overline{C})$ 以及 T 状态下发生的概率 $P(\overline{C}_i|T)$ 成反比.

证明 由 $P(C_i|T)=1$,可得

$$P(\overline{C}_i|\overline{T}) = 1 - P(\overline{C}_i|T) = 1-(1-P(C_i|T)) = 1 \tag{6}$$

对属性 C_i 的反驳使得对系统处于 $\overline{T}$ 状态的可能性变为:

$$P(\overline{T}|\overline{C}_i) = \frac{P(\overline{T})P(\overline{C}_i|\overline{T})}{P(\overline{C}_i)} = \frac{P(\overline{T})}{P(\overline{C}_i)} = \frac{P(\overline{T})}{P(\overline{C}_iT)+P(\overline{C}_i\overline{T})} = \frac{P(\overline{T})}{P(\overline{T})+(1-P(\overline{T}))P(\overline{C}_i|T)} \tag{7}$$

对属性 C_i 的反驳使得对系统处于 $\overline{T}$ 状态 $P(\overline{T}|\overline{C}_i)$ 的猜测变得更可靠,且其发生概率增加的程度和对结论 C_i 反驳概率 $P(\overline{C})$ 以及 T 状态下发生的概率 $P(\overline{C}_i|T)$ 成反比.

这样一来,我们能够给出在属性不可穷举状态下,信任对象 TU 的基础信任审定与反驳策略. 假设用户需要向云服务提供商验证服务 T 的基础可信性. 已知 T 蕴含的不可穷举系列结论 $\{C_i\}_{i=1}^{\infty}$. 那么如图 1 所示,用户对云服务的属性结论发随机挑战,以实现对信任对象 TU 的基础信任审定与反驳.

具体流程如下(如图 1 所示):

步骤 1 ***U-C* Challenge**

用户发起对云服务对象 T 的挑战,由于 T 蕴含的不可穷举系列结论 $\{C_i\}_{i=1}^{\infty}$,按照命题 1 和命题 2 结论,用户依据先验性判断 $1/(P(C_i|\overline{T}) * P(\overline{C}_i|T))$,由高至低生成的 n 个需要审定或反驳的属性结论 $\{C_{j_k}\}_{k=1}^{n}, j_k \in [1, \infty]$. 并向云服务提供商提出认证请求.

步骤 2 ***C-U* Response**

云服务提供商收到用户对服务 T 的属性 $\{C_{j_k}\}_{k=1}^{n}$ 认证请求,生成相应的验证脚本发起验证,并将验证结果 $\{R_{j_k}\}_{k=1}^{n}$ 返回用户.

步骤 3 ***U-V* Response**

在用户收到来自云服务提供商的认证响应 $H(\{R_{j_k}\}_{k=1}^{n} \| r_u \| r_c)$ 后,连同服务 T 及需要认证属性 $\{C_{j_k}\}_{k=1}^{n}$ 一同发送给验证服务器.

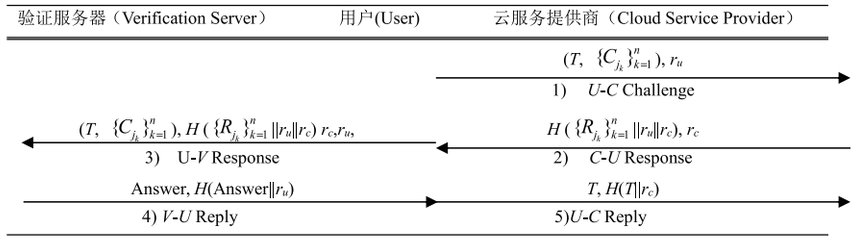

图 1　基础信任审定与反驳策略

步骤 4　*V-U* Reply

验证服务器通过在后端数据库中查找属性 $\{C_{j_k}\}_{k=1}^{n}$ 的响应信息,验证服务将验证结果(合规或不合格)Answer 返回给用户.

步骤 5　*U-C* Reply

用户根据验证结果 Answer,决定是否继续向云服务提供商请求 T 服务. 当 $P(T|C_i)$ 和 $P(\bar{T}|\bar{C}_i)$ 何者累积先过实现给定的阈值,即相应判定给定云服务对象 T 处于基础可信/不可信状态.

2.3　经验信任的评价与估计

借鉴心理学者将信任看成一种关于实体在某一特定方面行为的可靠性观点,基于经典的 BBK 模型[13]、Abdul 模型[14]、Jøsang 模型及其改进[15,16]等,本节提出经验信任的评价和估计方法.

命题 3　设网络中两个可信主体 S_i, S_j,可以用 0-1 分布描述其每次交互结果,用随机变量 ξ 表示,其均值为 $E(\xi)=P$,方差为 $\sigma^2(\xi)=P(1-P)$. 设其交互总次数为 m,成功次数为 u,那么主体 S_i 对主体 S_j 的经验信任度的估计可表示为:

$$T_{S_j}^{S_i} = u/m \tag{8}$$

命题 3 给出了经验信任度的计算方法. 在理想情况下式(8)是无偏估计. 但是当节点间缺乏交互历史的情况下,需要确样本容量、估计置信区间和置信度之间的关系.

命题 4　设网络中两个可信主体 S_i, S_j,可以用0-1分布描述其每次交互结果,用随机变量 ξ 表示,其均值为 $E(\xi)=P$,方差为 $\sigma^2(\xi)=P(1-P)$. 设其交互总次数为 m,成功次数为 u,那么 u/m 是 P 的无偏估计. 样本容量 m,估计置信区间 ε,估计置信度之间的关系为:当样本数满足 $m \geqslant p^2(1-p)^2/\varepsilon^2$ 时,置信度开始为正,当 $m \geqslant 2(\sigma^2+\frac{1}{3}\varepsilon)/\varepsilon^2$ 后,以指数速度逼近 1.

证明　基于 F. Cuker, S. Smale 等研究者[17]对样本容量与学习能力的讨论框架. 设 ξ 为满足0-1分布的随机变量,显然:

$$E(\xi) = P \tag{9}$$

$$\sigma^2(\xi) = P(1-P) \tag{10}$$

设 $\xi(z_i), i=1,\cdots,m$ 为来自总体的样本,定义样本均值

$$\bar{\xi} = \frac{1}{m}\sum_{i=1}^{m}\xi(z_i) = \frac{u}{m} \tag{11}$$

因为 $E(\bar{\xi})=E(\xi)=P$,因此 u/m 是 P 的无偏估计.

根据切比雪夫(Chebyshe)不等式,有

$$\operatorname*{Prob}_{z\in Z^m}\left\{\left|\frac{u}{m}-P\right|\leqslant\varepsilon\right\}\geqslant 1-\frac{P^2(1-P)^2}{m\varepsilon^2} \tag{12}$$

由上式可知,当确定置信区间 ε 后,当样本容量 $m \geqslant p^2(1-p)^2/\varepsilon^2$,用 u/m 估计 P 的置信度开始为正.

同时,根据 Bernstein 不等式,有

$$\operatorname*{Prob}_{z\in Z^m}\left\{\left|\frac{u}{m}-P\right|\leqslant\varepsilon\right\}\geqslant 1-2\mathrm{e}^{-\frac{m\varepsilon^2}{2(P^2(1-P)^2+M\varepsilon/3)}} \tag{13}$$

其中,$\xi(z)$ 取值范围为(0,1),$0\leqslant E(\xi)\leqslant 1$,则对几乎所有 $z\in Z$,满足

$$|\xi(z)-E(\xi)| = |\xi(z)-P| \leqslant 1 \tag{14}$$

那么,式(13)可重写为

$$\operatorname*{Prob}_{z\in Z^m}\left\{\left|\frac{u}{m}-P\right|\leqslant\varepsilon\right\}\geqslant 1-2\mathrm{e}^{-\frac{m\varepsilon^2}{2(P^2(1-P)^2+\varepsilon/3)}} \tag{15}$$

由式(15)可知,当

$$m \geqslant \ln(4)(p^2(1-p)^2+\frac{1}{3}\varepsilon)/\varepsilon^2 \tag{16}$$

的时候,$1-2\mathrm{e}^{-\frac{m\varepsilon^2}{2(P^2(1-P)^2+\varepsilon/3)}}$ 开始以指数速度逼近 1.

综上所述,确定置信区间 ε 后,当样本容量 $m \geqslant p^2(1-p)^2/\varepsilon^2$,用 u/m 对节点信任度进行估计的置信度开始为正,同时当 $m \geqslant \ln(4)(p^2(1-p)^2+\frac{1}{3}\varepsilon)/\varepsilon^2$ 后,以指数速度逼近 1.

上述结论对于审定经验信任具有指导意义,如式(8)所示,我们通常使用交互成功概率来模拟经验信任. 但需要注意的是,通常样本容量,即交互次数的影响并没有被考虑. 简单来说,假设 A 和 B 共交互 10 次,成功 4 次,所得到的成功概率 0.4,与 C 和 D 共交互 100000 次,成功 40000 次,所得到的成功概率 0.4 是不可相提并论的. 式(21)通过引入置信度,对估计的信度转化为对样本容量的要求,即确定置信度后,可以对交互次数进行定量规范. 给经验信任的计算提供了新的

切入点和计算方法.

3 基于信任传播的云服务动态组合机制研究

基于基础信任和经验信任的信任评估机制可以对单个实体进行信任评估与审定,但仍需解决如何对云服务组合进行信任评估与审定的问题.

假设每个云服务提供商 W_i 可以提供多类具有不同功能的云服务 S_{ij}. 定义二元组(S,L),其中 S 表示参与组合的云服务集合,L 代表云服务组合路径的集合. 需要指出,只有通过基础信任和经验信任筛选出的可信云服务才能参与云服务组合计算. 我们需要按服务等级协议(SLA),从不同云服务商中选取最优的服务组合 L 实现约定功能.

如图 2 所示,实线箭头代表某云服务和箭头所指云服务存在服务提供的交互历史. 路径中显然存在两种典型的信任传播途径:直接传递和推荐传递. 直接传递即两个主体有直接的交互经验,不需要经过第三方推荐形成信任关系,云服务 S_{12} 和 S_{21} 之间有直接的交互经验,信任就可以直接传递. 间接传递即两个主体没有直接的交互经验,需要经过第三方推荐形成信任关系,S_{12} 到 S_{63} 之间没有直接交互经验,需要通过 S_{35} 或者 S_{52} 间接传递形成正向传播路径 $S_{12}\rightarrow S_{35}\rightarrow S_{63}$ 或者 $S_{12}\rightarrow S_{52}\rightarrow S_{63}$ 传递信任. 但在信任的推荐传递途径中,信任并不总是正向传递的. 如 S_{12} 和 S_{46} 之间不存在正向的信任传递路径. 借鉴文献 0 中的相关概念,我们给出如下定义.

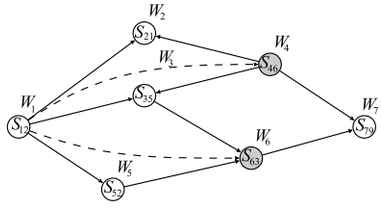

图2 服务组合信任传播路径图

定义 2 可达证信节点. 两个没有直接交互经验的主体可以通过可达证信节点的推荐进行信任评估,并且形成正向信任传播路径. 如 $A\rightarrow B,B\rightarrow C,A\rightarrow B\rightarrow C$,那么我们称 B 为可达证信节点.

如果在信任传播过程中存在可达证信节点情况下. 假设 A 到 C 的信任有两条推荐正向传播路径 $A\rightarrow B\rightarrow C,A\rightarrow D\rightarrow C$. 我们分别设定这两条路径得到的信任值为 $T1_C^A,T2_C^A$. 对于路径 $A\rightarrow B\rightarrow C$,设 A 对 B 的信任值为 T_B^A,B 对 C 的信任值为 T_C^B. 基于文献[15,16]所提出的信任算子,可得 $T1_C^A=T_C^A\otimes T_C^B$. 同理,求得 $T2_C^A=T_D^A\otimes T_C^D$,那么,最后总体信任值 $T_C^A=T1_C^A\oplus T2_C^A$.

如果在信任传播过程中不存在可达证信节点情况下. 假设 A 到 D 有两条信任推荐方向传播路径 $A\rightarrow B\leftarrow C,A\rightarrow D\leftarrow C$. 我们分别设定这两条路径得到的信任值为 $T1_C^A,T2_C^A$. 对于路径 $A\rightarrow B\leftarrow C$,设 A 对 B 的信任值为 T_B^A,C 对 B 的信任值为 T_C^B. 基于文献[20]信任算法,可以计算出 $A\rightarrow B$ 和 $C\rightarrow B$ 的信任紧密度 q_1,$A\rightarrow D$ 和 $C\rightarrow D$ 的信任紧密度 q_2,得到 $T1_C^A=\langle q_1,1-q_1\rangle$,$T2_C^A=\langle q_2,1-q_2\rangle$,这里不再赘述. 如果 A 和 C 有 n 个共同交互对象,则最后总体信任值 $T_C^A=\langle\sum_{n=1}^{N}q_n,\sum_{n=1}^{N}(1-q_n)\rangle$. 这样即可对所有满足服务等级协议(SLA)的候选云服务组合路径 L 按进行信任评估,从不同云服务商中选取最优的服务组合 L 实现约定功能.

4 实验验证

4.1 实验设置

为了验证本文所提出的基于信任合成的云服务动态组合机制方法的可行性和有效性,本文模拟一个拥有 100 个主体的云环境,共进行 500 轮仿真模拟实验. 实验使用 Netlogo 5.1.0 与 MATLABR2012a 仿真工具进行模拟实验,其他仿真参数如表 1 所示.

表 1 实验参数设置

参数	数值
Number of agents	100
Number of service types	20
Max number of interaction agent	50
Max number of untrusted agent	90
Total simulation rounds	500

首先,为每个主体随机设置用户信任值,并且每个主体随机初始化 n 个属性,属性值只能为 0 或者 1,若属性值为 1,则表明此属性成立;若属性值为 0,则表明此属性不成立. 基于图 1 基础信任审定与反驳策略,我们可以判断主体是否处于基础可信状态. 然后,为每个主体设置一定数目的交互对象,最大值为 50. 主体间随机生成 m 次交互,其中成功交互 u 次. 基于上文提到的经验信任的相关概念,我们设定置信区间 ε 的精度为 0.05,依据式(16),我们反推得到满足置信区间的最低交互次数 k,若主体的交互次数 $m<k$,则将该不可信主体筛除. 最后,为每个主体随机分配 v 个种类的云服务,$v\in[1,20]$.

实验对比 5 中不同的信任评估方法:(1)Sharon[18],(2)Huang[19],(3)Shin[20],(4)Shin(Shin + BT)方法加入基础信任,以及(5)Shin(Shin + BT + ET)方法加入基础信任和经验信任,即为本文所提机制的实现. 每轮实验给定一个服务组合请求 request,作为仿真实验中固定的输入. 通过比较服务组合成功率和执行的时间复杂度,观察所提出方法的有效性;通过设定不同的不可信主体比例和置信区间,观察所提方法的稳定性. 评价指标包括:(1)

服务组合成功率:执行各实验方法,计算成功形成服务组合路径的次数和实验总次数的比值.(2)时间复杂度:执行各实验方法,定量描述该算法的运行时间.

4.2　实验结果和分析

每一轮实验中,程序系统都会随机发出一个服务组合的请求,之后通过不同的实验方法使主体参与进来提供相应的服务,最终形成满足请求的可信任云服务组合.本文将信任阈值设定为 0.5,若两主体之间的信任值小于阈值,则判定主体交互不成功.如图 3,图 4 所示,我们可以得到以下结论:

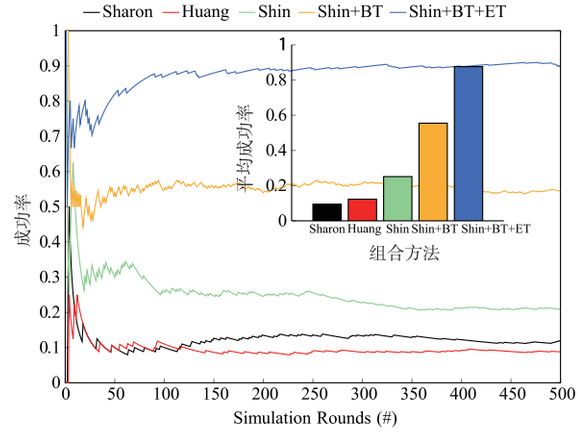

图3　组合服务成功率比较

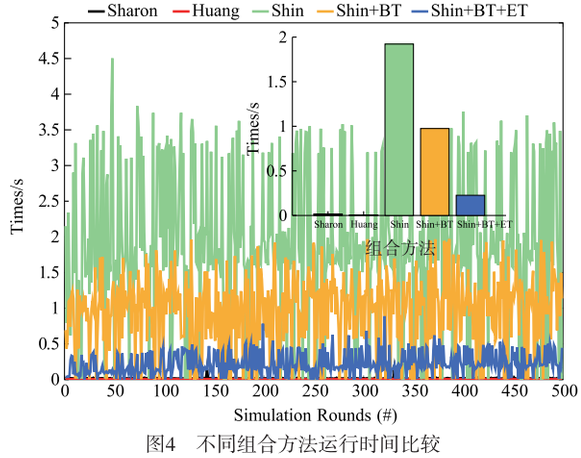

图4　不同组合方法运行时间比较

(1)信任传播和计算方法的仿真对比.图 3 给出了不同信任传播计算方法的仿真对比,其中 Sharon 方法[18]考虑到云服务组合中主体的用户信任值以及云服务组合请求的执行顺序.在云服务组合请求的执行顺序确定的情况下,选择用户信任值最大的主体参与组合;Huang 方法[19]不仅考虑到主体的用户信任值还考虑到有数据依赖关系的主体之间的交互信任值;Shin 方法来自文献[20],该方法提出信任传播的多种途径和计算方法,但上述方法都没有考虑到本文所提出的基础信任和经验信任.由仿真结果可以看出,Shin 提供的服务组合方法的效率明显高于前两种,这也是我们选择 Shin 算法作为仿真基线系统的原因.

(2)基础信任能够有效提升服务组合性能(Shin + BT).图 3 给出了基于上述 Shin 方法加入基础信任的仿真对比.从仿真结果来看,随着实验次数的增加,加入基础信任因素的 Shin 方法形成服务组合的效率优于 Shin 方法.

(3)经验信任能够显著提升服务组合性能(Shin + BT + ET).图 3 给出了基于上述 Shin 方法加入基础信任和经验信任的仿真对比.从仿真结果来看,随着实验次数的增加,加入基础信任和经验信任因素的 Shin 形成服务组合的效率明显优于其他所有方法.

(4)算法复杂度随着分析.图 4 给出了 5 种算法运行 500 次的运行时间比较.可以出时间复杂度 Shin > Shin + BT > Shin + BT + ET > Sharon > Huang. Shin 算法由于考虑了方向传播路径,因而时间复杂度较高.需要注意基础信任和经验信任的引入降低了算法的时间开销,这是因为基础信任和经验信任都会考察服务主体的信任属性,把不符合要求的服务排除在外,从而降低了算法需要考虑的服务组合数目,因而时间复杂度降低.

5　结论

本文提出了一种基于信任合成的云服务动态组合机制,即通过定义主体的信任属性,将其分解为基础信任和经验信任的集合.将基础信任评价问题建模为对主体分解属性的判断问题,将经验信任评价问题建模为对主体交互行为的判断问题,并将其应用到云服务的信任传播和计算的过程中.仿真实验结果表明,本文提出基础信任和经验信任能有效地提高服务组合的成功率,筛除不可信的服务主体,提高服务选择过程的质量及准确性,从而为用户提供更优质的云服务.

参考文献

[1] 侯富,毛新军,吴伟.一种基于多 Agent 系统的云服务自组织管理方法[J].软件学报,2015,26(4):835 - 848.
HOU Fu, MAO Xin-Jun, WU Wei. Self-organizing management approach for cloud services based on multi-agent system[J]. Journal of Software, 2015, 26(4): 835 - 848. (in Chinese)

[2] FOSTER I, ZHAO Y, RAICUI, et al. Cloud computing and grid computing 360-degree compared[A]. Proceedings of Grid Computing Environments Workshop (GCE08), 2007[C]. Austin, USA: IEEE, 2007. 1 - 10.

[3] ALRIFAI M, RISSE T, NEJDL W. A hybrid approach for efficient Web service composition with end-to-end QoS constraints[J]. ACM Transactions on the Web (TWEB), 2012, 6(2): 1 - 31.

[4] PAREJO J A, SEGURA S, FERNANDEZ P, et al. QoS-a-

ware web services composition using GRASP with path relinking[J]. Expert Systems with Applications, 2014, 41(9):4211 – 4223.
[5] 刘必欣,王玉峰,贾焰,等. 一种基于角色的分布式动态服务组合方法[J]. 软件学报,2005,16(11):1859 – 1867.
LIU Bi-xin, WANG Yu-feng, JIA Yan, et al. A role-based approach for decentralized dynamic service composition[J]. Journal of Software, 2005, 16(11):1859 – 1867. (in Chinese)
[6] 夏亚梅,程渤,陈俊亮,等. 基于改进蚁群算法的服务组合优化[J]. 计算机学报,2012,35(2):270 – 281.
XIA Ya-mei, CHENG Bo, CHEN Jun-liang, et al. Optimizing services composition based on improved ant colony algorithm[J]. Chinese Journal of Computers, 2012, 35(2): 270 – 281. (in Chinese)
[7] 尼克拉斯卢曼. 信任:一个社会复杂性的简化机制[M]. 瞿铁鹏,等,译. 上海:上海人民出版社,2001.
[8] KOSFELD M. Trust in the brain: Neurobiological determinants of human social behavior[J]. EMBO Reports, 2007, 8(S):S44 – S47.
[9] 马礼,郑纬民. 信息网格环境下的综合信任度评价模型[J]. 清华大学学报(自然科学版),2009,49(4),599 – 603.
MA Li, ZHENG Weimin. Synthesize trust degree evaluating model for an information grid environment[J]. Journal of Tsinghua University (Sci & Teh), 2009, 49(4), 599 – 603. (in Chinese)
[10] 王怀民,唐扬斌,尹刚,李磊. 互联网软件的可信机理[J]. 中国科学(E 辑:信息科学),2006,36(10):1156 – 1169.
WANG Huai-min, TANG Yang-bin, YIN Gang, et al. Trustworthy theory and key technologies of internet software[J]. Science in China (Ser E: Information Sciences), 2006, 36(10):1156 – 1169. (in Chinese)
[11] 沈昌祥,张焕国,王怀民,等. 可信计算的研究与发展[J]. 中国科学(E 辑:信息科学),2010,40(2):139 – 166.
SHEN Chang-xiang, ZHANG Huan-guo, WANG Huai-min, et al. Research and development of trusted computing[J]. Science in China (Ser E: Information Sciences), 2010, 40(2):139 – 166. (in Chinese)
[12] 波利亚. 数学与猜想(第二卷):合情推理模式[M]. 北京:科学出版社,2003.
POLYA G. Mathematics and Plausible Reasoning: Patterns of Plausible Inference (2) [M]. Beijing: China Science Publishing & Media Ltd, 2003. (in Chinese)
[13] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open network[A]. Proceedings of the European Symposium on Research in Security (ESORICS'94)[C]. Brighton, UK: Springer-Verlag, 1994. 3 – 18.
[14] ABDUL-RAHMAN A, HAILES S. A distributed trust model[A]. 1997 New Security Paradigms Workshop[C]. Cumbria, UK: ACM Press, 1998. 48 – 60.
[15] JØSANG A. A subjective metric of authentication[A]. Proceedings of the European Symposium on Research in Security (ESORICS'98)[C]. Louvain-la-Neuve, Belgium: Springer, 1998. 329 – 344.
[16] JØSANG A, Haller J. The Beta reputation system[A]. Proceedings of the 15th Bled Electronic Commerce Conference[C]. Bled, Slovenia: Bled eConference, 2002. 1 – 14.
[17] CUKERF, SMALES. On the mathematical foundations of learning[J]. Bulletin (New Series) of the American Mathematical Society, 2001, 39(1):1 – 49.
[18] PARADESI S, DOSHI P, SWAIKA S. Integrating behavioral trust in web service compositions[A]. IEEE International Conference on Web Services (ICWS'09)[C]. Los Angeles, CA, USA: IEEE, 2009. 453 – 460.
[19] HUANG L, DENG S, LI Y, et al. Trust evaluation mechanism for collaboration of data-intensive services in cloud[J]. Applied Mathematics & Information Sciences, 2003, 7(1L):121 – 129.
[20] HANG Chung-Wei, ZHE Zhang, MUNINDAR S. Shin: Generalized trust propagation with limited evidence[J]. Computer, 2013, 46(3):78 – 85.

作者简介

杨 震 男,1979 年出生,北京工业大学计算机学院教授. 主要研究方向为数据挖掘、内容安全、可信计算技术.
E-mail:yangzhen@bjut.edu.cn

杨甜甜 女,1992 年出生,硕士研究生,主要研究方向为信息安全、信息安全标准、可信计算技术.
E-mail:yangtiantian@emails.bjut.edu.cn

范科峰(通信作者) 男,1978 年出生,中国电子技术标准化研究院高级工程师. 主要研究方向为信号处理、信息安全.
E-mail:fankf@cesi.ac.cn

王 勇 男,1964 年出生,桂林电子科技大学教授. 主要研究方向为云计算、计算机网络技术及应用、信息安全.
E-mail:ywang@guet.edu.cn