云计算环境下服务信任评估方法研究

王晋东 卫 波 张恒巍 何嘉婧
(解放军信息工程大学三院 郑州 450001)

摘 要 云计算环境中,服务资源广域分布、复杂多变,服务实体之间的信任关系因不确定性强而难以有效建立与维护。传统的服务信任评估方法无法全面反映信任的随机性和模糊性特征。在研究云模型理论的基础上,提出一种基于加权多属性云的服务信任评估方法。引入时间衰减因子来反映服务信任的时效性,并以多属性信任云来细化信任评估的粒度。计算用户评价相似度,确定推荐实体的推荐可靠性和权重,防止不法分子的合谋欺骗和恶意攻击。通过云相似度计算确定服务的信任等级,为用户的服务选择提供安全决策。仿真结果表明,该方法明显提高了服务交互成功率,并能有效适用于云计算环境下的服务信任评估。

关键词 云服务,云模型,信任评估,信任云,信任等级
中图法分类号 TP391 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.12.009

Research on Service Trust Evaluation Approach under Cloud Computing Environment

WANG Jin-dong WEI Bo ZHANG Heng-wei He Jia-jing
(The Third Institute, PLA Information Engineering University, Zhenzhou 450001, China)

Abstract In cloud computing, the resources of service are widely distributed, complex and fickle. The trust relationship among service entities is hard to establish and maintain with high uncertainty. The characteristics of randomness and fuzziness of services cannot be responded by traditional trust evaluation approach comprehensively, so a service trust evaluation method based on weighted multi-attribute cloud was proposed. Time decay factor was introduced to reflect the timeliness of trust, and multi-attribute trust cloud was used to refine the evaluation granularity. In order to prevent conspiracy to defraud and malicious attacks, the reliability and weight of recommender were confirmed by similarity of evaluation, and the trust rating was confirmed by cloud similarity calculation to provide security decisions for the user's services selection. Simulation results show that this method can improve the success rate of services interaction obviously, and it can be applied to service trust evaluation under cloud computing environment.

Keywords Cloud service, Cloud model, Trust evaluation, Trust cloud, Trust rating

1 引言

云计算[1-3]是继网格计算、并行计算和P2P计算之后迅速发展起来的一种新兴计算模型,它利用抽象、虚拟化、瞬时部署、宽带网络等关键技术,通过网络实现计算、存储和软件等可扩展资源的互联、互通和互操作,以统一服务的形式,向用户提供按需分配、动态配置、价格低廉、高可用性和高可靠性的IT服务[1-3]。其应用系统表现为由多个软件服务组成动态协作系统,系统形态正从面向封闭的、熟识用户群体和相对静态的形式向开放的、虚拟抽象的和动态协作的服务模式转变,这大大增加了实体交互过程中的安全风险,因此需要建立一种信任机制用以在交互之前评估服务提供者的可信程度,确保用户可以获得安全可靠的云服务。

当前国内外学者针对服务的信任评估做了大量的研究工作。文献[4]提出了一个基于经验和概率统计的信任评估模型;文献[5]提出一套基于主观逻辑来推导和计算信任度的方法;文献[6]采用隐马尔可夫链针对信任的随机性特点进行度量;文献[7]应用模糊理论给出了信任评估模型;文献[8]构建了基于第三方认证的服务信任博弈模型和信任评价模型;文献[9]提出一种基于集对分析理论中联系数概念的服务信任表示方法。但信任是一个很难度量的定性概念,其源于人的主观信念,信任度的确定很大程度上依赖于观察者,因此它具有很大的随机性和模糊性,无法精确地加以描述和验证[10]。而以上方法均没有综合考虑信任的模糊性与随机性,无法客观全面地反应服务信任不确定性特征。文献[11]引入了云模型理论对信任进行建模,通过隶属云模型把信任的随机性和模糊性有机地综合在一起;文献[12]提出一种基于云模型的主观信任度量方法,它通过信任变化云刻画信任客体的信

到稿日期:2013-12-19 返修日期:2014-01-28 本文受国家自然科学基金项目(61303074),河南省科技攻关计划项目(12210231003)资助。
王晋东(1966—),男,教授,主要研究领域为信息安全、装备建设与发展;卫 波(1990—),男,硕士生,主要研究领域为信息系统集成、云安全,E-mail:weibo7516@sina.com;张恒巍(1978—),男,博士,讲师,主要研究领域为信息安全、需求工程;何嘉婧(1991—),女,硕士生,主要研究领域为云安全、云资源管理。

用度变化情况，但仅针对一维信任云，无法提供精确的信任信息；文献[13]利用综合信任云重心评价法来计算服务的信任度，但仅通过云重心来确定服务的信任等级，准确度不高，且没有考虑信任的时效性和推荐权重，无法有效抑制合谋欺骗和不实反馈对服务信任评估造成的影响。

因此本文针对现有基于云模型的服务信任评估方法存在对时效性和推荐信任考虑不足的问题，提出基于加权多属性云的服务信任评估方法，引入时间衰减因子为每次服务评价赋权重，从服务的多个属性细化信任评估的粒度，并通过加权属性信任云逆向生成算法计算得到直接信任云，然后根据评价相似度来确定推荐权重并合成得到推荐信任云，最后综合直接信任云和推荐信任云，利用云相似度计算确定信任等级，以有效反应云计算环境中服务实体的信任关系。

2 云模型理论

云模型[14]是20世纪90年代初李德毅院士在传统模糊数学和概率统计的基础上提出的定性与定量之间互换的理论，实现了从定性的概念中获定量数据的范围及分布规律，也可以将定量数据有效转换为恰当的定性概念。

2.1 云的基本概念

设U是一个用精确数值表示的定量论域，C是与U相关的定性概念，论域中的任意一个元素x是定性概念C的一次随机实现，x对C的确定度$\mu(x)\in[0,1]$是有稳定倾向的随机数，$\mu:U\to[0,1]$，$\forall x\in U$，$x\to\mu(x)$，则x在论域U上的分布称为云，每一个x称为一个云滴[14]。

由于正态分布广泛存在于自然现象、社会现象中，因此与正态分布相关的云模型可以广泛用于处理实际中的普遍存在的不确定现象[15]。

2.2 云的数字特征

云模型通过期望Ex、熵En和超熵He来描述概念的不确定性，它们反映了定性概念的定量特征，其数字特征如图1所示。

期望Ex：其是论域空间中最能代表这个定性概念的点，即最典型的样本点；

熵En：其代表定性概念的可度量粒度，表示论域中可被定性概念接受的云滴范围，熵越大则概念越宏范，模糊性越大，反映了定性概念的不确定性。

超熵He：其是熵的不确定性的度量，即熵的熵，代表定性概念样本出现的随机性，是由熵的模糊性和随机性共同决定的，反应了模糊性和随机性之间的关联性。

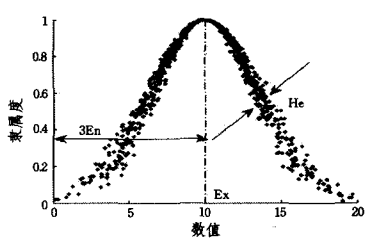

图1 云的数字特征

2.3 云的3En规则

论域中有99.7%的云滴元素落在区间$[Ex-3En,Ex+3En]$内，因此，对于一个定性语言值概念，在其相应的云对象中，落在$[Ex-3En,Ex+3En]$之外的云滴是小概率事件，一般可忽略不计。

3 基于信任扩展的SOA模型

云计算建立在面向服务的体系(SOA)这种新型的分布式计算技术基础上。SOA主要由3种角色组成，其分别为：服务请求者、服务提供者和服务注册中心，并通过发布、查找和绑定操作实现3种角色实体之间的交互。在此基础上，通过增加可信任的第三方代理来扩展SOA模型，如图2所示。实际应用中，用户使用完某个服务后会对其进行评价，信任代理可以根据服务历史评价记录来计算服务当前的信任度，并为下次用户的服务选择提供决策支持。

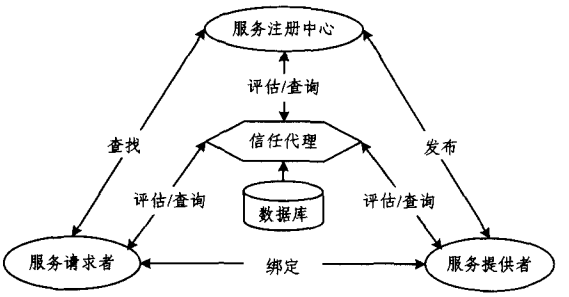

图2 扩展SOA模型

根据云计算环境中服务请求的多样性和信任评估的客观合理性要求，本文选择响应时间、执行成本、可靠性、可用性作为服务信任评价指标。其中，响应时间、执行成本可以通过系统监测得到，可靠性和可用性通过用户反馈得到，可用性用某段时间内服务成功运行时间与该段时间比值来衡量；可靠性用某段时间内服务成功执行的次数与服务执行总次数的比值来表示。由于各属性值大小不同，单位不一，本文根据文献[16]中的方法对各属性值进行归一化处理，由于篇幅限制，在此不再累述。

4 基于云模型的服务信任评估方法

4.1 基于云模型的服务信任评估思路

针对云计算环境的复杂情况，在扩展SOA模型的基础上，深入分析传统基于云模型的信任评估方法，结合服务实体间信任关系的特点，提出基于加权多属性云的服务信任评估方法，该方法能够对云服务的信任值进行全面度量，客观反应云计算环境中服务信任的模糊性和随机性。具体过程如图3所示。

(1)根据信任评价的需求，信任代理收集被评估服务各属性的信任评价值，然后对收集到的数据进行预处理。

(2)将处理过的数据通过加权属性信任云逆向生成器生成多个信任属性云。

(3)将多个属性信任云合成得到直接信任云。

(4)通过信任代理查找到该服务的推荐者，将推荐者评估

服务的直接信任云合成得到推荐信任云。

(5)综合直接信任云和推荐信任云得到服务的综合信任云。

(6)根据专家意见及实际情况,划分信任等级,并通过标准信任云生成器生成标准信任云。

(7)根据云相似度计算综合信任云与各标准信任云的相似度,并依此得到该服务信任等级。

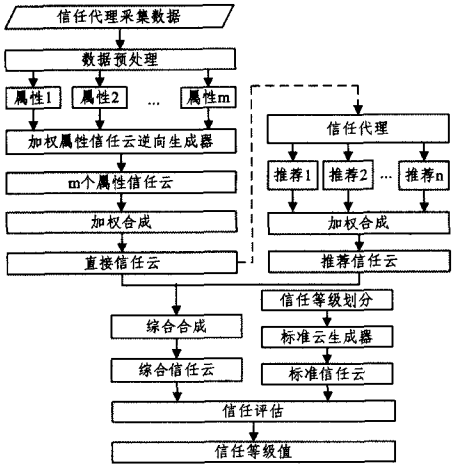

图 3　基于云模型的服务信任评估流程

4.2　标准信任云计算

定义 1　定量数域 $T=[0,1]$是一个信任度的集合,称为信任度空间,C 表示与 T 相关联的信任描述值,对于任意元素 x_i 都存在一个有稳定倾向的随机数 $y=\mu(x)$,称为 x 对 T 的信任度,信任度在 T 上的分布称为信任云,每个元素与其信任度的序对$(x,\mu(x))$称为信任云滴。

完成对服务信任的评估,需要将定量的评价数据转换为定性的评价,信任等级是建立用户对服务信任评估的依据。根据传统的信任等级划分情况,将信任分为如表 1 所列的 6 个等级,并综合多位专家的意见以及现实生活中的实际情况,将论域[0,1]进行划分并与信任等级一一映射,其情况如表 2 所列,并依此生成 6 个信任等级云。

表 1　信任云等级

信任等级	可信度
1	完全不可信
2	不太可信
3	基本可信
4	比较可信
5	可信
6	非常可信

表 2　信任等级范围

信任等级	论域中的取值范围
1	[0,0.2]
2	[0.2,0.4]
3	[0.4,0.6]
4	[0.6,0.8]
5	[0.8,0.9]
6	[0.9,1]

定义 2　系统预先设定好一个系列的信任云供参考,每个信任云称为一个标准信任云,每个标准信任云对应一个确定的概念,表示相应的信任等级,记作 $TC=\{TC_i(Ex_i,En_i,He_i)|(i=1,2,\cdots,6)\}$。

由表 2 可知信任空间被分为 6 个子空间,其中第 i 个子空间为$[t_i^{\min},t_i^{\max}]$,其中 $t^{\min}$ 和 $t^{\max}$ 分别为该子空间的下限和上限,通过采用标准信任云生成算法生成各个标准信任云。

算法 1　标准信任云生成算法

输入:n 个信任子空间

输出:n 个标准信任云 $TC_i(Ex_i,En_i,He_i)$

1. 根据各子空间的上下限,计算期望:

$$Ex_i=\begin{cases}t_i^{\min}, & i=1\\ \dfrac{t_i^{\min}+t_i^{\max}}{2}, & 1<i<n\\ t_i^{\max}, & i=n\end{cases}\tag{1}$$

2. 根据各子空间上下限和 3En 规则,计算熵:

$$En_i=\begin{cases}\dfrac{t_i^{\max}-t_i^{\min}}{3}, & i=1\text{ 或 }n\\ \dfrac{t_i^{\max}-t_i^{\min}}{6}, & 1<i<n\end{cases}\tag{2}$$

3. 计算 $He_i=\eta$

其中 η 为常数,反应实体信任值的随机性,需要根据属性值的不确定性和模糊性的程度具体设定,本文参考文献[17]将超熵设为 $\eta=0.01$,从而得到标准信任云(TC)的分布情况,如图 4 所示。

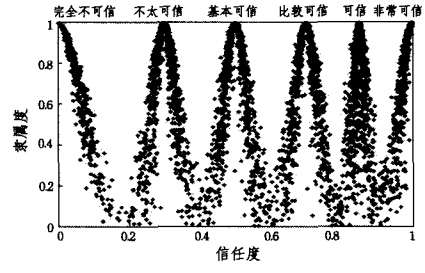

图 4　标准信任云图

4.3　直接信任云计算

4.3.1　属性信任云计算

为了提高对服务信任评估的准确性,从服务的多个属性细化信任评估的粒度。在云计算环境中,服务的信任度随着时间不断变化和积累,距离当前决策时刻越近的评价越有说明力和参考价值,对信任评估的影响越大,因此为了有效反应服务信任评估的时效性,引入时间衰减因子为每次信任评价赋权重,设计一个加权属性信任云逆向生成算法。

假设有时间窗口$[t_b,t_c]$,其中 t_c 为信任决策时刻,t_b 为信任评价时间阈值,在 t_b 之前的评价离决策时刻太远,不能正确反映当前服务的信任情况而不予考虑。$TD(A,B,t_d)$表示时间窗口内用户 A 对服务 B 在 t_d 时刻的信任评价。为用户评价赋权重的基本原则是,时间越早的评价权重越小;反之则权重越大,为了准确反应信任的时效性,将用户评价按评价时间倒序排列,结合时间衰减因子 λ,得到权重 $w(i)$,如下所示:

$$w(i)=\lambda^i\left(\frac{1}{2}<\lambda\leqslant 1,i=1,2,\cdots n\right)\tag{3}$$

式中,i 表示某次评价在序列中的次序。权重 $w(i)$表示该次信任评价对服务整体信任评价的影响程度,需要满足如下约束条件:

$$\sum_{i=1}^{n} w(i)=1 \tag{4}$$

当前大部分信任评估方法在引入时间衰减因子时存在很大的主观因素和盲目性，而本文根据式(4)可推导出 λ 满足等式(5)，并根据时间窗口内评价次数 n 求出衰减因子 λ 的值，这就避免了 λ 由人为主观设定带来的不确定性。

$$\lambda=\sqrt[n]{\frac{2\lambda-1}{\lambda}} \tag{5}$$

通过为信任评价值赋权重，能够有效抑制较长时间前的评价对信任评估的影响。根据当前时间窗口内的信任评价值及其权重，设计加权属性信任云逆向生成算法如下：

算法 2 加权属性信任云逆向生成器

输入：用户 A 对服务 B 在该属性上的评价值($x_{1j}, x_{2j}, \cdots, x_{nj}$)，评价值按评价时间倒序排列；评价值的权重集合($w_j(1), w_j(2), \cdots, w_j(n)$)。

输出：用户 A 对服务 B 在第 j 个评价指标上的属性信任云 $TC_j(Ex_j, En_j, He_j)$

1. 计算样本均值 $\bar{x}_j=\frac{1}{n}\sum_{i=1}^{n} w(i)x_{ij}$，一阶样本绝对中心矩 $d_j=\frac{1}{n}\sum_{i=1}^{n} w(i)|x_{ij}-\bar{x}_j|$，样本方差为 $S_j^2=\frac{1}{n-1}\sum_{i=1}^{n} w(i)(x_{ij}-\bar{x}_j)^2$

2. 云的期望 $Ex_j=\bar{x}_j$；

3. 云的熵 $En_j=\sqrt{\frac{\pi}{2}}\times d_j$；

4. 云的超熵 $He_j=\sqrt{S_j^2-En_j^2}$。

经过以上加权属性信任云逆向生成算法可以求得多个属性信任云 $TC_j(Ex_j, En_j, He_j)$。

4.3.2 多属性信任云合成

求得各属性信任云后，需要将多个属性信任云合成得到直接信任云。由于各属性在信任评价时所占权重不同，因此需要考虑各属性信任云的权重，权重满足 $\alpha=\{\alpha_j \mid \alpha_j>0, \sum_{j=1}^{m}\alpha_j=1\}$。

根据各属性信任云的数字特征值及对应权重可以合成得到直接信任云 $TC_{dir}(Ex_{dir}, En_{dir}, He_{dir})$，它能够有效地反应当前用户对服务的直接信任情况，计算公式如下：

$$\begin{cases} Ex_{dir}=\sum_{j=1}^{m}(Ex_j\times\alpha_j) \\ En_{dir}=\sqrt{\sum_{j=1}^{m}(Ex_j^2\times\alpha_j)} \\ He_{dir}=\sum_{j=1}^{m}(He_j\times\alpha_j) \end{cases} \tag{6}$$

4.4 推荐信任云计算

在用户与服务很少交互的情况下，需要通过信任推荐机制获得更多的信任。当前关于推荐信任的计算，大多是将各推荐者的推荐信任简单相加求均值，没有考虑推荐可靠性对信任评估的影响，这给不法用户进行合谋欺骗、恶意攻击提供了机会。

在实际情况中，用户倾向于相信与自己有相同评价标准的推荐者，因此本文通过用户评价相似度来表示推荐者的推荐可靠性并依此确定推荐权重。采用皮尔森相关系数度量用户 A 和 C 的评价相似度，根据推荐者对服务的信任数据可得到皮尔森相关系数计算公式：

$$\mathrm{sim}(A,C)=\frac{\sum_{i\in\Omega_{AC}}(ZT_{A,i}-\overline{ZT_A})(ZT_{C,i}-\overline{ZT_C})}{\sqrt{\sum_{i\in\Omega_{AC}}(ZT_{A,i}-\overline{ZT_A})^2}\sqrt{\sum_{i\in\Omega_{AC}}(ZT_{C,i}-\overline{ZT_C})^2}} \tag{7}$$

式中，Ω_{AC} 表示与用户 A 和 C 都进行过直接交互的服务集合；$Z_{A,i}$ 和 $ZT_{C,i}$ 表示用户 A 和 C 对服务 i 的直接信任评价，用直接信任云的信任期望 Ex 来表示；$\overline{ZT_A}$ 和 $\overline{ZT_C}$ 表示用户 A 和 C 在评价集合上直接信任评价的平均值。

则用户 A 和 C 的评价相似度可表示如下：

$$r(A,C)=\begin{cases}\mathrm{sim}(A,C), & \mathrm{sim}(A,C)\geqslant 0\\ 0, & \text{else}\end{cases} \tag{8}$$

假设在时间窗口 $[t_b, t_c]$ 内，除了用户 A 外，服务 B 还与其他 m 个用户进行过直接交互，则会产生 m 个推荐信任，各推荐者的推荐权重可表示为：

$$\beta_i=\frac{r(A,i)}{\sum_{j=1}^{m} r(A,j)},(i\in[1,m]) \tag{9}$$

综合考虑其他推荐者的推荐信任及其推荐权重，将推荐者评估服务的直接信任云进行加权合成得到推荐信任云 $TC_{dir}(Ex_{dir}, En_{dir}, He_{dir})$，它能够有效地反应来自其他推荐者的推荐信任，计算公式如下：

$$\begin{cases} Ex_{rec}=\sum_{i=1}^{m}(Ex_i\times\beta_i) \\ En_{rec}=\sqrt{\sum_{i=1}^{m}(Ex_i^2\times\beta_i)} \\ He_{rec}=\sum_{i=1}^{m}(He_i\times\beta_i) \end{cases} \tag{10}$$

4.5 综合信任云计算

用户对服务的信任评估需要通过综合直接信任和推荐信任得到，其计算公式如下：

$$T_{total}=\delta T_{dir}+(1-\delta)T_{rec},\delta\in[0,1] \tag{11}$$

在实际情况中，当用户与服务没有交互或长时间未交互时，用户倾向于依赖推荐信任，随着交互次数增多，用户的直接信任在信任评估中所占的比重将不断增大。本文通过引入交互门限来动态调整直接信任的权重，从而得到权重 δ 计算公式如下：

$$\delta=\begin{cases}\frac{\sqrt{sum}}{2k}, & sum\leqslant k^2\\ 1-\frac{k}{2\sqrt{sum}}, & sum>k^2\end{cases} \tag{12}$$

式中，sum 是用户与被评估服务近期交互次数，k^2 为交互门限。

综合直接信任云和推荐信任云得到综合信任云 $TC_{total}(Ex_{total}, En_{total}, He_{total})$，它能够有效地反应用户对服务的当前信任情况，计算公式如下：

$$\begin{cases} Ex_{total}=Ex_{dir}\times\delta+Ex_{rec}\times(1-\delta) \\ En_{total}=\sqrt{Ex_{dir}^2\times\delta+Ex_{rec}^2\times(1-\delta)} \\ He_{total}=He_{dir}\times\delta+He_{rec}\times(1-\delta) \end{cases} \tag{13}$$

4.6 信任等级的综合评判

用户对被评估服务的信任等级的确定，需要将综合信任云与各标准信任云进行比较，通过云相似度计算算法求出相

似度，找到与该服务综合信任云最接近的标准信任云，其所对应的信任等级即为对该服务的信任综合评判结果。

定义 3 设有两个信任云 $TC_1(Ex_1, En_1, He_1)$ 和 $TC_2(Ex_2, En_2, He_2)$，将信任云 TC_1 经过正向云发生器生成 TC_1 的 N 个云滴 (x_i, μ_i)，若 x_i 在云 TC_2 中的隶属度为 μ_i'，则 $\frac{1}{N}\sum_{i=1}^{N}\mu_i'$ 称为云 TC_1 和 TC_2 的相似度，记作 φ。

算法 3 云相似度计算算法

输入：$TC_1(Ex_1, En_1, He_1)$，$TC_2(Ex_2, En_2, He_2)$

输出：两信任云之间的信任度 φ

1. 在云 TC_1 中生成以 En_1 为期望和以 He_1 为方差的正态随机数 $En_1' = N(En_1, He_1)$；
2. 在云 TC_1 中生成以 Ex_1 为期望和以 En_1' 为方差的正态随机数 $x_i = N(Ex_1, En_1')$；
3. 将 x_i 代入比较云 TC_2 的隶属度方程中，计算 $u_i' = e^{-\frac{(xi-Ex2)^2}{2(En2)^2}}$；
4. 重复步骤 2 和 3，直到生成 n 个 u_i'；

计算得到两个云的相似度 $\varphi = \frac{1}{N}\sum_{i=1}^{N}u_i'$。

5 仿真实验与分析

为了验证本文提出的基于加权多属性云的服务信任评估方法的可行性和有效性，利用 MATLAB 对云环境下的服务信任评估模型及其实现算法进行仿真验证。

模拟一个拥有 100 个实体的云环境，每个实体进行 200 次交互，随着时间推移共完成的交互次数为 $100 \times 200 = 20000$。每个实体可同时作为服务提供者和服务请求者。根据所提供服务的优良，可以将实体分为诚实的、非诚实的和恶意的。诚实实体的各信任属性的评价值为[0.6,1]，非诚实实体的评价值为[0.2,0.6]，恶意实体各属性评价值为[0,0.2]，实验环境中恶意实体占 20%，非诚实实体占 30%。本文将信任评价的属性权重都设为 0.25。

5.1 信任评估方法正确性验证

本实验对本文方法的正确性进行验证，收集实体 B 的历史评价记录，并利用加权属性信任云逆向生成算法生成 B 的属性信任云，并将多个属性云进行合成得到直接信任云；通过 4.4 节所述方法求得推荐信任云；之后综合直接信任云和推荐信任云生成综合信任云 $T(0.821, 0.053, 0.015)$；最后通过云相似度计算算法，得到综合信任云与 6 个标准信任云的相似度，如表 3 所列，综合信任云与标准云的比较云图如图 5 所示，从表 3 和图 5 中可知综合信任云与可信云的相似度最高，所以实体 B 信任等级被评定为可信，仿真结果与预期结果相同。

表 3 综合信任云与标准信任云的相似度

信任基准云	与 T_B 相似度
完全不可信云	0.0001
不太可信	0.0009
基本可信	0.0392
比较可信	0.2563
可信	0.7836
非常可信	0.0815

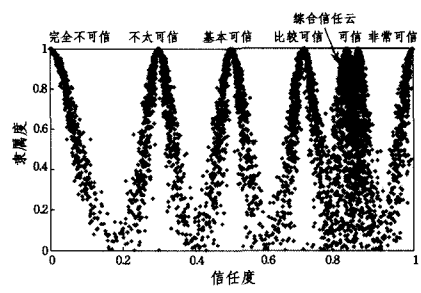

图 5 综合信任云与标准信任云对比图

5.2 信任评估方法有效性验证

本实验对本文方法的有效性进行验证。服务交互成功率是交互过程中成功交互次数所占总交互次数的比例，是信任模型好坏一个重要参考依据。比较在不使用任何信任评估方法（随机选择服务进行交互）、使用传统的不考虑时间衰减、推荐权重的评估方法和使用本文方法情况下，随着交互次数的增长，服务交互成功率的变化情况，如图 6 所示。

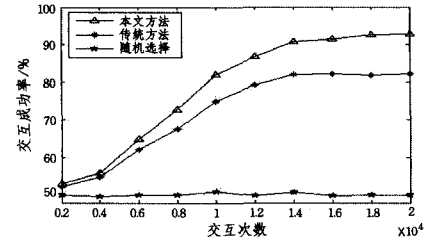

图 6 服务交互成功率比较

从图 6 可知，随机选择服务进行交互时，交互成功率不会随着交互次数的变化而变化，而增加信任评估模型时，交互成功率会随着交互次数增多而增长，但增长越来越缓慢；且采用本文信任评估方法比传统方法有更高的交互成功率，且随着交互次数的增加越来越明显，这说明本文的方法能够有效提高服务交互的成功率。

5.3 抑制恶意推荐实验

该实验进一步验证本文方法对恶意推荐进行控制的有效性。实验分为 5 轮，每轮不断增加服务交互过程中恶意推荐的比例，在实验 2 的 3 种情况下，服务交互成功率变化情况如 7 图所示。

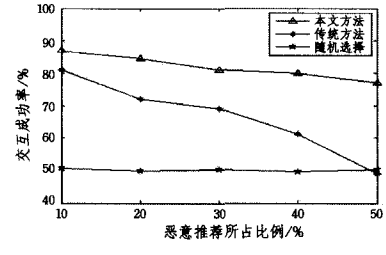

图 7 恶意推荐对交互成功率的影响比较

由图 7 可知，随机选择服务进行交互时，恶意推荐对交互成功没有影响，但在恶意推荐较少时，其交互成功率远远低于其他两种情况。采用传统信任评估方法时，随着恶意推荐的增加，服务交互的成功率速度迅速降低，而采用本文的评估方法，交互成功率变化非常缓慢，这说明本文的方法可以有效地

（下转第 66 页）

Computer Communications (INFOCOM). 2012:549-557

[12] Verdu S. Multiuser Detection [M]. Cambridge University Press,1998

[13] Halperin D, Anderson T E, Wetherall D. Taking the Sting Out of Carrier Sense: Interference Cancellation for Wireless LANs [C]// Proceedings of the ACM Annual International Conference on Mobile Computing and Networking (MOBICOM). 2008:339-350

[14] Sen S, Santhapuri N, Choudhury R R, et al. Successive Interference Cancellation: A Back-of-the-Envelope Perspective [C]// Proceedings of the ACM SIGCOMM Workshop on Hot Topics in Networks (HOTNETS). 2010:1-6

[15] Gollakota S, Katabi D. ZigZag Decoding: Combating Hidden Terminals in Wireless Networks [C]//Proceedings of the ACM Conference on Applications, Technologies, Architectures and Protocols for Computer Communications (SIGCOMM). 2008: 159-170

[16] Qin C, Santhapuri N, Sen S, et al. Known Interference Cancellation: Resolving Collisions due to Repeated Transmissions [C]// Proceedings of the IEEE Workshops on Wireless Mesh Network (WIMESH). 2010

[17] Jiang C, Shi Y, Hou Y T, et al. Squeezing the Most Out of Interference: An Optimization Framework for Joint Interference Exploitation and Avoidance [C]// Proceedings of the IEEE International Conference on Computer Communications (INFOCOM). 2012:424-432

[18] IEEE Std. 802. 11, IEEE Standard for Wireless LAN medium access control (MAC) and physical layer (PHY) specifications [S]. IEEE Computer Society,1999

[19] Jamieson K, Balakrishnan H. PPR: Partial Packet Recovery for Wireless Networks [C]// Proceedings of the ACM Conference on Applications, Technologies, Architectures and Protocols for Computer Communications (SIGCOMM). 2007:409-420

[20] Bianchi G. Performance analysis of the IEEE 802. 11 distributed coordination function [J]. IEEE Journal on Selected Areas in Communications (JSAC),2000,18(3):535-547

[21] Malone D, Duffy K, Leith D. Modeling the 802. 11 Distributed Coordination Function in Nonsaturated Heterogeneous Conditions [J]. IEEE/ACM Transactions on Networking, 2007, 15 (1):159-172

[22] Chatzimisios P, Vitsas V, Boucouvalas A C. Throughput and Delay Analysis of IEEE 802. 11 protocol [C]// Proceedings of the IEEE International Workshop on Network Applicances (IWNA). 2002:168-174

(上接第 42 页)

预防合谋欺骗和不实反馈等恶意推荐行为。

结束语 在复杂开放的云计算环境中,信任是服务交互活动的前提和关键,其直接影响云服务的质量和云计算技术的发展与推广。因此本文针对云计算环境中服务实体间信任关系的不确定性,在云模型理论基础上借鉴现有评估方法的思想,提出基于加权多属性云的服务信任评估方法,该方法以多属性信任云细化信任评估的粒度,通过引入时间衰减因子来反应信任的时效性,考虑了推荐可靠性对信任评估的影响,能够更加客观真实地反应云计算环境中服务实体间的信任特征。实验结果表明,该方法明显地提高了服务交互成功率,并能够有效抑制不法分子的合谋欺骗和恶意推荐,更加真实地反映云计算环境中服务信任情况,为用户的服务选择提供可靠的安全决策。

参 考 文 献

[1] Buyya R, Yeo C S, Venugopal S, et al. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility[J]. Future Generation Computer Systems,2009,25(6):599-616

[2] Armbrust M, Fox A, Griffith R, et al. A view of cloud computing [J]. Communications of the ACM,2010,53(4):50-58

[3] 冯登国,张敏,张妍,等. 云计算安全研究[J]. 软件学报,2011,22 (1):71-82

[4] Vivekananth P. Reputation Based Trust Model for Grid with Enhanced Reliabilty[C]// Junior E R H, et al., eds. INTECH 2011, CCIS. Berlin Heidelberg: Springer-Verlag,2011

[5] Josang A, Presti S. Analyzing the relationship between risk and trust[C]// iTrust04: Proceedings of the Second International Conference on Trust Management. Berlin: Springer-Verlag,2004

[6] Ehab M, ElSalamouny. Probabilistic trust models in network security[D]. University of Southampton,2011

[7] Song Shan-shan, Hwang K, Macwan M. Fuzzy Trust Integration for Security Enforcement in Grid Computing[C]// International Symposium on Network and Parallel Computing (NPC2004). Heidelberg: Spring Verlag,2004:9-21

[8] 王文婧,杜惠英,吕廷杰. 基于第三方认证的云服务信任模型[J]. 系统工程理论与实践,2012,32(12):2774-2780

[9] 黄德才,陈姜倩. 基于集对分析的信任评估模型及其在服务选择中的应用[J]. 计算机科学,2012,39(1):210-214

[10] 唐文,胡建斌,陈钟. 基于模糊逻辑的主观信任模型研究[J]. 计算机研究与发展,2005,42(10):1654-1659

[11] 黄海生,王汝传. 基隶属云理论的主观信任评估模型研究[J]. 通信学报,2008,29(4):13-19

[12] 王守信,张莉,李鹤松. 一种基于云模型的主观信任评价方法[J]. 软件学报,2010,21(6):1341-1352

[13] 谢立军,朱智强,孙磊,等. 基于隶属度理论的云服务行为信任评估模型研究[J]. 计算机应用研究,2013,30(4):1051-1054

[14] 李德毅,杜鹢. 不确定性人工智能[M]. 北京:国防工业出版社,2005

[15] 李德毅,刘常昱. 论正态云模型的普适性[J]. 计算机工程科学,2004,6(8):431-440

[16] Ran S. A model for Web services discovery with QoS[J]. ACM SIGEcom Exchanges,2003,4(1):1-10

[17] 孟祥怡,张光卫,刘常昱,等. 基于云模型的主观信任管理模型研究[J]. 系统仿真学报,2007,19(14):3310-3317