·计算机工程与应用·

基于云模型的风险评估方法研究

张仕斌[1,2]，许春香[1]，安宇俊[2]

(1. 电子科技大学计算机科学与工程学院 成都 611731；2. 成都信息工程学院网络工程学院 成都 610225)

【摘要】以复杂网络环境中的网络交易为研究背景，引入云模型理论，通过对复杂网络环境中的信任、信任影响因素及信任评价机制等问题的研究，提出了基于云模型的信任评估模型，实现了信任的定性与定量的转换，客观地反映了信任的随机性、模糊性和不可预测性；为了有效地对复杂网络中交易风险进行评估，研究并提出了基于云模型的风险评估方法。仿真实验表明，提出的信任评估模型能对复杂的网络环境中实体的信任做出合理的评价；基于云模型的风险评估方法能对电子商务中的交易风险进行合理可行的预测。设计并实现了一个基于云模型的风险评估系统，进一步验证了基于云模型的风险评估方法的可行性和合理性，也为复杂的网络环境中风险评估的研究提供了有价值的新思路。

关 键 词 云模型； 风险评估； 风险等级； 信任云； 信任评估； 信任等级

中图分类号 TP393.08 文献标志码 A doi:10.3969/j.issn.1001-0548.2013.01.020

Study on the Risk Evaluation Approach Based on Cloud Model

ZHANG Shi-bin[1,2], XU Chun-xiang[1], and AN Yu-jun[2]

(1. School of Computer Science & Engineering, University of Electronic Science and Technology of China Chengdu 611731;

2. College of Network Engineering, Chengdu University of Information Technology of China Chengdu 610225)

Abstract In order to achieve a secure network transactions, the main problem we are facing to is the trust, risk and other issues. In this paper, taking the network transactions of complex network environment as the researching background, we proposed the trust evaluation model based on cloud model. This trust evaluation model can implement the conversion between qualitative and quantitative of trusts, and it can objectively reflect the randomness, fuzziness, and unpredictability of the trusts. In order to effectively evaluate transaction risk in complex networks, the risk evaluation approach based on cloud model is researched and proposed. The simulation results confirm that this trust evaluation model can make a reasonable evaluation of the entities' trust in the complex network environment, and that the risk evaluation approach researched in this paper can reasonably predict the risk of network transactions. Finally, we design and realize a risk evaluation system based on cloud model, further also confirm the feasibility and rationality of the proposed risk evaluation approach.

Key words cloud model; risk evaluation; risk level; trust cloud; trust evaluation; trust level

由于复杂网络环境中存在随机性、模糊性和不可预测性等特性[1]，以及网络交易的虚拟性、非面对面、网上支付等，使网络交易面临诸多安全隐患，这些问题统称为网络交易风险。但由于网络交易的前提和基础是信任，因此要做到安全的交易，目前面临的主要是信任、风险等问题[2]。但目前信任、风险评估方法及模型仍存在许多问题需要解决。如如何合理地对信任与风险进行形式化描述、制定信任与风险评估机制、信任及风险评估方法的研究、使用什么样的信任和风险策略、信任与风险之间的关系等[3]。

近些年来，关于风险与评估问题的研究吸引了国内外众多学者。风险评估方法及模型的研究都是研究的热点[4]。在风险评估方法方面，目前主要有基于知识的、基于概率的、基于模型的、基于模糊逻辑的、基于图论的、基于符号验证的和基于层次分析法(AHP)的风险评估方法等[5-7]，但这些评估方法通常都局限于评估技巧的改进，很少从风险的本质属性(风险具有客观性和随机性等)方面进行研究。事实上，风险评估主观性很强，具有随机性、模糊

收稿日期：2012－07－21； 修回日期：2012－08－24

基金项目：四川省科技支撑计划(13ZC2138)

作者简介：张仕斌(1971－)，男，博士，教授，主要从事网络与信息安全、应用密码学方面的研究.

性和不可预测性等[8]。因此，如何设计风险评估方法，识别各种关键风险要素并判断其重要程度，从而准确地计算风险值成为研究的关键。因此，本文借鉴已有的研究工作，并结合文献[1, 9-10]中的研究成果，以复杂网络环境中的网络交易为研究背景，提出了基于云模型的信任评估模型；并以此为基础，研究并提出了基于云模型的风险评估方法。

1　相关问题的研究

1.1　信任及影响信任的因素

在网络交易中，信任是一方认为另一方是可靠的且能履行自己的承诺，所以信任是进行交易活动的前提和关键[9]。在复杂网络中有许多不确定因素都会对信任产生一定的影响[10]，主要有：1) 用户反馈评价。由于交易后对对方信用的反馈评价(如商品质量、服务等)具有主观性，本文在计算信任值时将用户反馈评价作为参考指标之一。2) 历史信任值。为了抵制“积累了一定的信用后”而实施的欺骗行为，本文计算信任值时将历史信任值也作为参考指标之一。3) 评价人信任值。为了防止不法用户采取信用炒作、周期行骗等行为，本文将评价人信任值作为计算信任值的参考指标之一。4) 商品价值。为了有效地防范信用炒作，本文在信任评估中考虑了商品价值对计算信任值的影响。5) 评价时间权重。由于信任是随着时间变化而不断积累的过程，近期评价比早期评价更具说服力和参考价值，所以本文在计算信任值时考虑了评价时间权重。

1.2　风险及影响风险的因素

风险是指为了达到预期结果，实体可能会遭受到损失的期望[8]。在现实的网络交易中，网络化的交易场所、电子化的交易手段、无纸化的交易信息、交易实体间存在着信任的不对称、交易前的信息不全、交易过程中的价值损失以及道德风险等都会使网上交易存在大量的风险。

事实上，风险具有客观性(风险是客观存在的)、随机性(风险具有不确定性和偶然性)、可测性(风险有时可以用概率进行评测)、普遍性(风险无处不在，无时不有)和可变性(在一定条件下风险具有可转化的特性)[11]。本文通过对C2C模式下交易过程的分析，得出目前影响网上交易风险的主要因素有：1) 商品价格。由于买家看不到交易的实物，商家可能以次充好标高价；2) 卖家信用。卖家信用的高低反映了买家对卖家的信任程度；3) 其他因素。如买家需求、网上支付风险、操作失误、恶意攻击等都会对交易带来风险。因此，本文将这3个因素作为风险评估的指标之一。

2　基于云模型的风险评估方法

基于云模型的风险评估方法主要包括信任评估和风险评估两部分，如图1所示。风险评估是在信任评估的基础上，结合影响风险的其他因素，综合评判出最终的风险等级，得出风险综合评估结果。

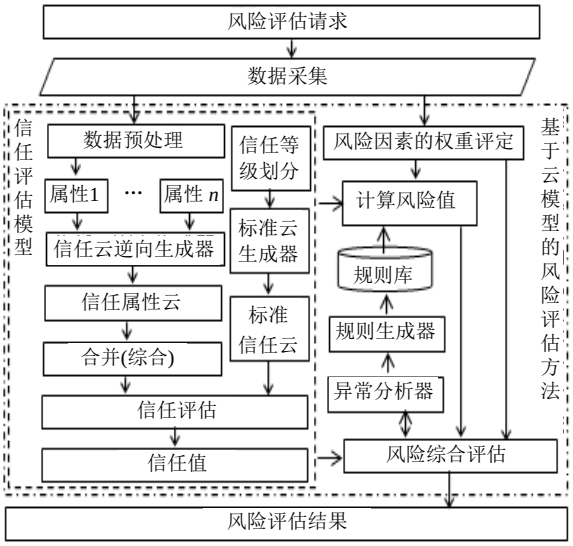

图1　基于云模型风险评估的评估过程

2.1　基于云模型的信任评估模型

2.1.1　基于云模型的信任评估思路

定义 1　设 $U=\{(x_1,x_2,\cdots,x_m)\}$是所研究的论域，$T$ 是与 U 相关联的信任描述值，其中 $x_1,x_2,\cdots,x_m$ 为各对象的信任评价属性，对于 T 所描述的信任隶属度 $C_T(x_1,x_2,\cdots,x_m)$在论域上的分布称为信任隶属云(简称信任云)；每一个元素与其隶属度的序对$(x_i,C_T(x_i))$称为信任云滴，$i=1,2,\cdots,m$。

针对复杂网络环境中信任域的实际情况，本文借助于云模型理论[12]，通过对各实体的属性评价获得实体的信任度，客观地反映了信任的随机性、模糊性和不可确定性。具体过程如下(图1的信任评估模型部分)：1) 划分信任等级，利用标准信任云生成器生成信任云；2) 根据信任评估需求，采集实体有关信息，并对采集到的数据进行预处理；3) 将描述各属性的信息通过信任属性云逆向生成器生成数学信任云；4) 对属性信任云进行综合得到综合云；5) 根据相似度计算与评价得到信任等级；6) 由历史信任值与当前信任值综合评价出最终信任值。

2.1.2　标准风险云生成算法的设计

按照本文的信任评估思路，确定各实体的信任

等级是本信任评估模型的关键。

定义 2 假设系统已预先设定一系列信任云(供参考)，则每个信任云称为一个标准信任子云，信任子云都有确定的概念，表示相应的信任等级。

假设信任值的取值范围为[0,10]，将该区间分为 n 个子区间，其中第 i 个子区间为[$R_i^{\min}$, $R_i^{\max}$]。

算法 1(标准信任云生成器) 输入n个子区间；输出标准信任云$\mathrm{STC}_i(\mathrm{Ex}_i,\mathrm{En}_i,\mathrm{He}_i)$，其中$I$=1,2,⋯,$n$，$\mathrm{Ex}_i$、$\mathrm{En}_i$、$\mathrm{He}_i$分别是$\mathrm{STC}_i$的期望、熵和超熵[12]，步骤如下：

1) 根据各区间的上下限值，计算可得：

$$\mathrm{Ex}_i=\begin{cases}R_i^{\min} & i=1\\ \dfrac{R_i^{\min}+R_i^{\max}}{2} & 1<i<n\\ R_i^{\max} & i=n\end{cases} \tag{1}$$

2) 根据上一步的计算结果，计算：

$$\mathrm{En}_i=\frac{R_i^{\min}+R_i^{\max}}{3} \tag{2}$$

3) 计算 $\mathrm{He}_i=\eta$ 。 η 反映了实体信任值的随机性，取值不宜过大，因为He越大Ex的误差越大，信任度的随机性增大，信任结果难以确定。

2.1.3 信任(属性)云逆向生成器的设计

定义 3 设被评价实体共有n个评价，对应m个属性；若将每个评价看作一云滴，由逆向云生成算法生成m个信任云，则将其称为信任云逆向生成器。

由于需重点考查被评价实体的可信性，本文引入加权百分比概念反应评价实体的可信性。

定义 4 某种评价的加权百分比等于每个评价的系数之和除以总评价数，称为加权百分比 θ ，即：

$$\theta=\sum_{i=1}^{M}\lambda_i/N \tag{3}$$

式中，N 为总评价数；λ_i 为每个评价的权重。由于对各属性的评价是定性分等级，而每个等级对应一个区间。为了解决这个问题，本文引入评价得分值的概念确定某个等级所对应的具体数据。

定义 5 设某个属性有W个评价等级，第i个等级得分区间为$[R_i^{\min},R_i^{\max}]$，则该区间的评价值为：

$$\alpha=R_i^{\min}+\theta\times(R_i^{\max}-R_i^{\min}) \tag{4}$$

式中，当 $i\geqslant W/2$ 时， θ 为实体获得的高于或等于i级的加权百分比；当 $i<W/2$ 时， θ 为实体获得的小于i级的加权百分比。如某个属性分为差、中和好等3个等级，分别对应区间[0,4]、[4,6]和[6,10]。若共获得100个评价(“差”30个、“中”40个、“好”30个)，假设所有评价的权值均为1，则根据式(4)计算得到评“差”的得分值为2.8，评“中”的得分值为5.4，评“好”的得分值为7.2，从而实现了评价等级从定性到定量的转换。

算法 2(信任云逆向生成) 输入样本点$X_i(x_{i1},x_{i2},\cdots,x_{im})$, $i=1,2,\cdots,n$ ； 输出m个信任云(TPC$_1$, TPC$_2$, ⋯ ,TPC$_m$)的数字特征为(Ex$_1$,Ex$_2$, ⋯ ,Ex$_m$,En$_1$, En$_2$, ⋯ ,En$_m$,He$_1$,He$_2$, ⋯ ,He$_m$)，具体步骤如下：

1) 计算信任隶属度为：

$$\mu_i=\mathrm{e}^{-\frac{2\ln(1/2)}{n}\times i}$$

2) 计算样本均值为：

$$\overline{x_1}=\frac{1}{n}\sum_{i=1}^{n}\left(x_{1i}\left(\frac{1}{2}+\mu_i\right)\right)$$

$$\vdots$$

$$\overline{x_m}=\frac{1}{n}\sum_{i=1}^{n}\left(x_{mi}\left(\frac{1}{2}+\mu_i\right)\right)$$

3) $(\mathrm{Ex}_1,\mathrm{Ex}_2,\cdots,\mathrm{Ex}_m)=(\overline{x_1},\overline{x_2},\cdots,\overline{x_m})$;

4) 计算熵为：

$$\mathrm{En}_1=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_{1i}-\mathrm{Ex}_1)^2}$$

$$\vdots$$

$$\mathrm{En}_m=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_{mi}-\mathrm{Ex}_m)^2}$$

5) 计算熵的标准差为：

$$\mathrm{En}'_{i1}=\sqrt{\frac{-(x_{i1}-\mathrm{Ex})^2}{2\ln\mu_i}}$$

$$\vdots$$

$$\mathrm{En}'_{im}=\sqrt{\frac{-(x_{im}-\mathrm{Ex})^2}{2\ln\mu_i}}$$

6) 计算超熵为：

$$\mathrm{He}_1=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(\mathrm{En}'_{1i}-\overline{\mathrm{En}'_1})^2}$$

$$\vdots$$

$$\mathrm{He}_m=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(\mathrm{En}'_{mi}-\overline{\mathrm{En}'_m})^2}$$

2.1.4 信任的综合评判

由于对各属性的侧重点不同，所以在对各实体进行评价时，根据各信任属性云的数字特征值以及对应的权重计算出新的综合信任云为：

$$\begin{cases} \mathrm{Ex}=\sum_{i=1}^{m}(\mathrm{Ex}_i\lambda_i) \\ \mathrm{En}=\sqrt{\sum_{i=1}^{m}(\mathrm{En}_i^2\lambda_i)} \\ \mathrm{He}=\sum_{i=1}^{m}(\mathrm{He}_i\lambda_i) \end{cases} \tag{5}$$

式中，m 为属性个数；λ_i 为属性对应的权重。由式(5)计算得到的数字特征(Ex,En,He)是实体信任的综合反映；然后计算出相似度，找出与该实体综合信任云最接近的标准信任子云，该标准信任子云对应的信任等级则为实体的信任等级。

定义 6　设 $\mathrm{TC}_1(\mathrm{Ex}_1,\mathrm{En}_1,\mathrm{He}_1)$、$\mathrm{TC}_2(\mathrm{Ex}_2,\mathrm{En}_2,\mathrm{He}_2)$ 为两个信任云，将 TC_1 经过信任云逆向生成器生成云滴 (x_i,μ_i)，若 x_i 在云 TC_2 中的隶属度为 μ_i'，则称 $\frac{1}{n}\sum_{i=1}^{n}\mu_i'$ 为 TC_1 与 TC_2 的相似度，记为 δ。

算法 3(信任云相似度计算)　输入信任云 $\mathrm{TC}_1(\mathrm{Ex}_1,\mathrm{En}_1,\mathrm{He}_1)$, $\mathrm{TC}_2(\mathrm{Ex}_2,\mathrm{En}_2,\mathrm{He}_2)$；输出 δ。具体步骤为：

1) 在 TC_1 中生成以 En_1 为期望和 He_1^2 为方差的正态随机数 $\mathrm{En}_i'=\mathrm{NORM}(\mathrm{En},\mathrm{He}^2)$；

2) 在信任云 TC_1 中生成以 Ex_1 为期望和 $\mathrm{En}_i'^2$ 为方差的正态随机数 $x_i=\mathrm{NORM}(\mathrm{Ex},\mathrm{En}_i'^2)$；

3) 计算 $\mu_i'=\mathrm{e}^{-\frac{(x-\mathrm{Ex}_2)^2}{2(\mathrm{En}_2)^2}}$；

4) 重复步骤 2)和 3)，直到生成 n 个 μ_i'；

5) 计算 $\delta=\frac{1}{n}\sum_{i=1}^{n}\mu_i'$。

综上所述，最终评定的信任值包括两部分：历史信任值(前一次的信任值)和评估得到的信任值，两部分综合到一起得出最终的信任值。

2.2　基于云模型的风险评估方法

从图 1 可知，风险评估包含以下几个过程：

1) 接收风险评估请求后进行数据采集，对数据进行预处理(数据格式化)。

2) 计算信任值。

3) 读取规则库(包含风险因素系数设置规则、风险等级评定规则、风险报警机制等)中的信息，确定风险因素权重系数(风险因素权重评定模块根据规则库里的规则对各风险因素的权重进行评定)，计算风险值：

$$R=(P_f,C_f)=\sum_{i=1}^{n}F_i\times\lambda_i \tag{6}$$

式中，P_f 为不利事件发生的概率；C_f 为不利事件一旦发生所导致的后果；F_i 为第 i 个风险因素等级评估值；λ_i 为其权重，$\sum_{i=1}^{n}\lambda_i=1$。

4) 异常分析(分析评估结果是否准确，若与实际情况不相符合，则将分析结果提交给规则生成器)，有异常转至步骤 5)，无异常转至步骤 6)。

5) 规则生成器生成新规则(根据异常分析器提供的结果对规则库中相应规则进行更新，或者创建新的规则)，写入规则库。

6) 风险的综合评估：根据计算得到的风险值、信任值和风险因数，进行风险的综合评估，然后与规则库里的规则判断当前交易的风险等级，最后给出可以交易或因风险过大而建议终止交易的参考结论，即风险综合评估结果。

3　仿真实验与分析

仿真实验所用PC机的基本配置如下：Intel® Core™ i3 CPU，3G内存，操作系统为Microsoft Windows XP，在Matlab环境下进行实验；仿真实验数据来自淘宝网某商家的交易记录(共400条)。

3.1　基于云模型的信任评估模型的仿真实验与分析

1) 对数据进行预处理。

① 确定信任评价属性(因淘宝网交易评价有商品描述相符度、卖家服务态度、卖家发货速度等 3 项，本文增加了商品价格作为对信任评价属性)。

② 将买家对商品描述相符度、卖家服务态度、卖家发货速度的评价分为 5 个等级，由式(4)分别计算得到评价属性区间的分值，如表 1 所示。

表1　评价属性区间的分值

等级区间	非常差	差	一般	好	非常好
区间得分值	[0,2]	[2,4]	[4,6]	[6,8]	[8,10]
商品与所描述相符程度	1.9	3.6	5.6	6.6	8.2
服务态度	1.8	3.5	5.5	6.6	8.2
发货速度	1.9	3.8	5.8	6.8	8.3

③ 将商品价格分成 5 个区间，由式(4)计算出的得分值，如表 2 所示。

表2　商品价格属性区间的分值

商品价格区间	等级区间	价格区间得分值
[10,150] [4 930,5 070]	[0,2]	1.9
[150,350] [4 730,4 930]	[2,4]	3.6
[350,800] [4 280,4 730]	[4,6]	5.6
[800,1 500] [3 580,4 280]	[6,8]	6.4
[1 500,2 540]	[8,10]	8.1

[2 540,3 580]

④ 信任区间的定义。

根据经验将[0,10]区间划分为：[0,1.5](极不可信)，[1.5,3.5](不可信)，[3.5,6.5](低可信)，[6.5,8.5](一般可信)，[8.5,10](高可信)。

2) 信任值的计算。

① 将标准信任子云分为极不、不、低、一般和高可信云(对应STC_1(0,0.5,0.2)、STC_2(2.5,0.67,0.2)、STC_3(5,1.33,0.2)、STC_4(7.5,0.67,0.2)和STC_5(10,0.5,0.2)，根据算法1生成信任云，如图2所示。

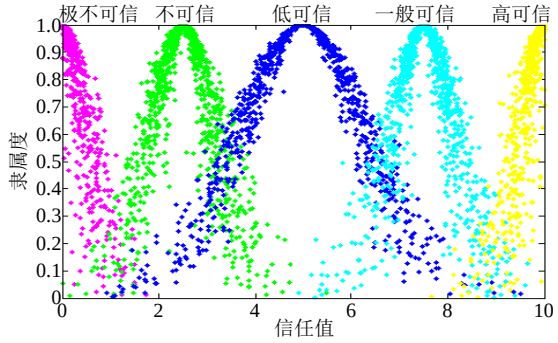

图2 标准信任云生成图

② 将预处理后的数据利用算法 2 生成属性云。

③ 将属性云进行合并得到综合评价云TC(5.5,1,0.4)，综合评价云与标准信任云对比如图3所示。

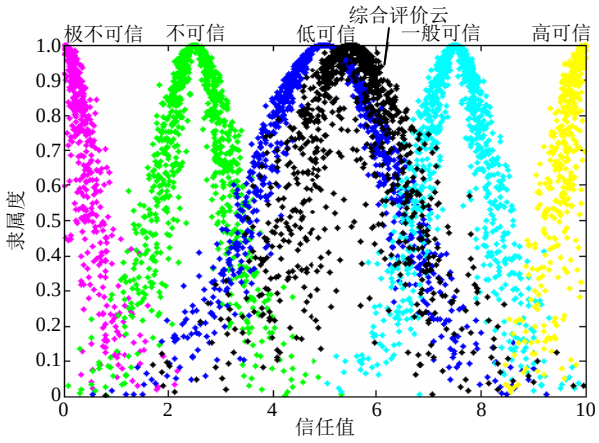

图3 综合后的综合云与标准云对比图

④ 根据算法3计算综合评价云与标准信任子云的相似度，如表3所示。由表3可知综合评价云与低可信云相似度最高，所以该商家信任等级为低可信。

表3 综合评价云与标准信任子云的相似度

标准信任子云	极不可信云	不可信云	低可信云	一般可信云	高可信云
相似度	0.000 1	0.040 3	0.758 2	0.143 4	0.001 4

⑤ 低可信的信任值区间为[3.5,6.5]，根据信任云滴的分布，在低可信及其以上等级的云滴占总云滴的 90%，由式(4)计算出信任值为 6.2。

3) 实验结果分析。

本文的实验采取了历史信任值与当前信任值(本文的评估方法)各占 50%的权重，前一次评定的信任值为 6，所以本次最终的信任值为 6×50%+6.2×50%=6.1。

本文的仿真实验结果与预期结果相同，证明了本文的信任评估模型是合理可行的。

3.2 基于云模型的风险评估方法仿真实验与分析

1) 数据处理及信任值的计算。

本文的仿真实验是在3.1节仿真实验的基础上进行，因此实验中的“确定信任评价属性、评价属性区间的分值、商品价格属性区间的分值、信任区间的定义和信任值的计算”都与3.1节相同。

2) 可由式(6)计算风险值为：

$$R=(1-t)\ \lambda_1+w\lambda_2+d\lambda_3+p\lambda_4+e\lambda_5+m\lambda_6$$

式中，$\sum_{i=1}^{6}\lambda_i=1$；$t$为格式化到区间[0,1]上的信任值；$w$为交易金额格式化到[0,10]区间上的值；$d$为当前交易金额与历史平均值之差所得的价格得分；$p$为网上支付问题产生的可能性得分；$e$为操作失误可能性得分；$m$为恶意行为发生可能性得分。本文设定规则库中初始值为：$\lambda_1=0.4$，$\lambda_2=0.3$，$\lambda_3=0.3$；假设网上支付风险、操作失误、恶意行为发生的可能性很小可以忽略，所以λ_4、λ_5、λ_6均取0。

3) 异常分析器分析前一次交易中风险评估的准确性，若前一次的评估有误，则在该次评估中对规则库进行更新，调整λ_1、λ_2、λ_3、λ_4、λ_5、λ_6的取值(如前一次评估风险预测过大，则调整的原则是使风险值 R 变小)。本文采取遍历法，以 0.01 为步长，在增加某一个权重大小的同时减小另一个权重大小，使总的权重之和为 1 不变；然后找出其中符合规则且产生的风险值变化最小的组合，将这组权重系数作为新的权重分配，更新到规则库中。

4) 实验结果分析。

图 4 显示了某商家 400 次交易的信任与风险的变化曲线，风险预测正确率如表 4 所示。

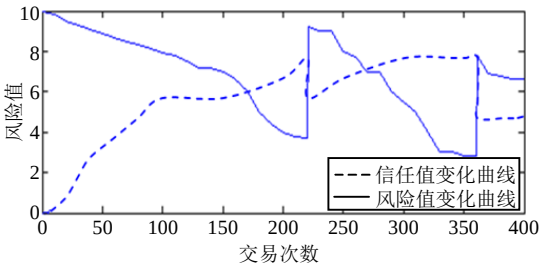

图4　信任与风险变化曲线图

表4　风险预测准确率统计

风险预测项	百分比/(%)
准确率	85.6
风险预测过大	7.8
风险预测过小	6.6

从图4可以看出，在第200次和第250次之间有一次交易的风险突然很大(因为预先设定商家有异常行为)，而对应的信任值也随之减小，说明存在失败交易，买家给出了很差的评价；同样，在第350次和第400次之间也有一次，这两次预测与实际相符合，也验证了本文研究的风险评估方法的可行性。

从表 4 可以看出，本文的基于云模型的风险评估方法所做预测准确率较高，也进一步说明了本文研究的风险评估方法的可行性和合理性。

4　基于云模型的风险评估系统的实现

基于云模型的风险评估系统实现的框架结构如图5所示。通信接口模块负责与应用系统进行通信；信任评估模块是根据获取到的用户相关信息计算出信任值(使用本文研究的信任评估模型)；风险评估模块将计算得到的风险值、信任评估模块计算出来的信任值与交易订单数据进行综合评估，得出风险评估结果(使用本文的风险评估方法)；数据预处理模块将评估所需的数据进行格式化处理；数据库接口模块负责与应用系统数据库建立连接，根据评估需求从数据库中提取相关的数据。

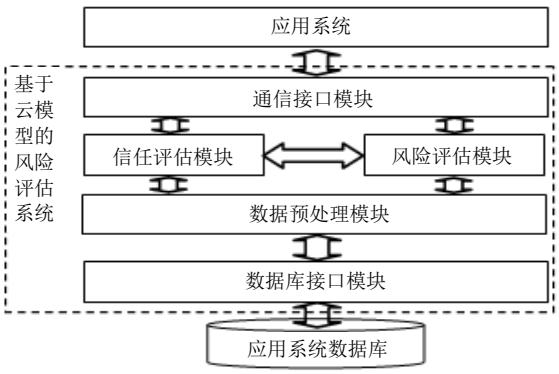

图5　基于云模型的风险评估系统实现的框架结构

本文的系统使用 C 语言编写，分别在 Windows XP SP3 和 Suse Linux 10 环境中进行测试与运行。测试数据均来自淘宝网，图 6 所示为某次风险较低情况下的交易界面，可以看出商家的信任值是 7.5，本次交易的风险值为 3.2，为低风险。

图6　低风险交易

图7所示为某次风险较大时的交易界面，可以看出此次的交易风险值为8.2，为高风险，系统在付款按钮旁给出高风险提示，提醒买家谨慎交易。

图7　高风险交易

5　结 束 语

在复杂网络中，信任是网络交易的前提和基础，但从事网上交易也存在着一定的风险。本文借鉴了已有的研究工作，以网络交易为研究背景，提出了基于云模型的信任评估模型，并以此为基础，研究并提出了基于云模型的风险评估方法。仿真实验表明，使用本文的信任评估模型和风险评估方法可以对网络交易风险进行很好的预测。本文设计并实现了一个风险评估系统，能为买家做交易时提供风险参考，进一步验证了基于云模型的风险评估方法的可行性和合理性。目前有很多技术还停留在实验室中，距离推广还有很多实际问题需要进一步的研究解决。

参　考　文　献

[1] 张仕斌，何大可，远藤誉. 模糊自主信任建立策略的研究[J]. 电子与信息学报, 2006, 28(8): 1492-1496.
ZHANG Shi-bin, HE Da-ke, HOMARE E. Research of fuzzy autonomous trust establishment strategy[J]. Journal of Electronics & Information Technology, 2006, 28(8): 1492-1496.

[2] 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.
WANG Shou-xin, ZHANG Li, LI He-song. Evaluation approach of subjective trust based on cloud model[J].

Journal of Software, 2010, 21(6): 1341-1352.

[3] 刘玉玲, 杜瑞忠, 冯建磊. 基于软件行为的检查点风险评估信任模型[J]. 西安电子科技大学学报, 2012, 39(1): 179-185.
LIU Yu-ling, DU Rui-zhong, FENG Jian-lei, et al. Trust model of software behaviors based on check point risk assessment[J]. Journal of Xidian University, 2012, 39(1): 179-185.

[4] 李晓蓉, 庄毅, 许斌. 基于危险理论的信息安全风险评估模型[J]. 清华大学学报(自然科学版), 2011, 51(10): 1231-1235.
LI Xiao-rong, ZHUANG Yi, XU Bin. Risk assessment model for information security based on danger theory[J]. J Tsinghua University(Sci & Tech), 2011, 51(10): 1231-1235.

(下转第104页)

[4] LAMBROU D. TCPA enabled open source platforms [EB/OL]. [2012-01-11]. http://www.crazylinux.net/downloads/projects /TCPA/TCPA_thesis.html.
[5] Reiner Sailer, ZHANG Xiao-lan, JAEGER T, et al. Design and implementation of a TCG-based integrity measurement architecture[C]//Proceedings of the 13th USENIX Security Symposium. San Diego, CA, USA: [s.n.], 2004.
[6] JAEGER T, SAILER R, SHANKAR U. PRIMA: policy-reduced integrity measurement architecture[C]// Proceedings of the 11th ACM Symposium on Access Control Models and Technologies. California, USA: ACM, 2006.
[7] IBM. vTPM: virtualizing the trusted platform module [EB/OL]. [2012-07-11]. http://domino.research.ibm.com/library/cyberdig.nsf/1e4115aea78b6e7c85256b360066f0d4/a0163fff5b1a61fe85257178004eee39?OpenDocument
[8] DINABURG A, ROYAL P, SHARIF M, et al. Ether: Malware analysis via hardware virtualization extensions [C]//Proceedings of the 15th ACM Conference on Computer and Communications Security(CCS 2008). Alexandria, VA: ACM, 2008.
[9] 程戈, 邹德清, 李敏, 等. 基于可信轻量虚拟机监控器的安全架构[J]. 计算机应用研究, 2010, 27(8): 3045-3049.
CHENG Ge, ZOU De-qing, LI Min, et al. Trusted lightweight VMM bases security architecture[J]. Application Research of Computers, 2010, 27(8): 3045-3049.
[10] AZAB A M, NING Peng, ZHANG Xiao-lan. SICE: A hardware-level strongly isolated computing environment for x86 multi-core platforms[C]//Proceedings of The 18th ACM Conference on Computer and Communications Security (CCS 2011). Chicago, Illinois, USA: ACM, 2011.
[11] 赵波, 张焕国, 李晶, 等. 可信PDA计算平台系统结构与安全[J]. 计算机学报, 2010, 33(1): 82-93.
ZHAO Bo, ZHANG Huan-Guo, LI Jing, et al. The system architecture and security structure of trusted PDA[J]. Chinese Journal of Computers, 2010, 33(1): 82-93.
[12] 李博, 李建欣, 胡春明, 等. 基于VMM层系统调用分析的软件完整性验证[J]. 计算机研究与发展, 2011, 48(8) : 1438-1446.
LI Bo, LI Jian-xin, HU Chun-ming, et al. Software integrity verification base on VMM-Level system call analysis technique[J]. Journal of Computer Research and Development, 2011, 48(8) : 1438-1446.
[13] SAHITA R, WARRIEU R, DEWAN P. Dynamic software application protection[EB/OL]. [2012-08-11]. http:// blogs.intel.com/wp-content/mt-content/com/research/trusted/dynamic/launch-flyer-rls-passool.pdf.
[14] Mccune J M, PARNO B, PERRIG A, et al. Flicker: an execution infrastructure for TCB minimization[C]// Proceedings of the ACM European Conference in ComputerSystems (EuroSys). [S.l.]: ACM, 2008.

编 辑 税 红

(上接第97页)

[5] KARABACAK B, SOGUKPINAR I. ISRAM: Information security risk analysis method[J]. Computer & Security, 2005, 24(2): 147-159.
[6] NGAI T, WAT F. Fuzzy decision support system for risk analysis in e-commerce development[J]. Decision Support Systems, 2005, 40(2): 235-245.
[7] BODIN L, GORDON L, LOEB M. Evaluating information security investments using the analytic hierarchy process[J]. Communications of the ACM, 2005, 48(2): 7-83.
[8] 杨柳, 吕英华. 基于云模型的网络风险评估技术研究[J]. 计算机仿真, 2010, 27(10): 95-98.
YANG Liu, LÜ Ying-hua. An evaluation model for network risk based on cloud theory[J]. Computer Simulation, 2010, 27(10): 95-98.
[9] 张仕斌, 陈麟, 王一川. 一种基于模糊推理的主观信任评价模型[J]. 仪器与仪表学报, 2009, 30(S1): 658-660.
ZHANG Shi-bin, CHEN Lin, WANG Yi-chuan. A subjective trust valuation model based on fuzzy reasoning[J]. Chinese Journal of Scientific Instrument, 2009, 30(S1): 658-660.
[10] ZHANG Shi-bin, HE Da-ke. Fuzzy model for trust evaluation[J]. Journal of Southwest Jiaotong University (English Edition), 2006, 14(1): 23-28.
[11] HOLE K J, NETLAND L H. Toward risk assessment of large-impact and rare events[J]. IEEE Security and Privacy, IEEE Computer Society, 2010, 8(3): 21-27.
[12] 李德毅, 杜鹢. 不确定性人工智能[M]. 北京: 国防工业出版社, 2005.
LI De-yi, DU Yi. Artificial intelligent with uncertainty[M]. Beijing: National Defence Industry Press, 2005.

编 辑 黄 莘