DOI：10.7652/xjtuxb201604004

一种采用云模型的同驻虚拟机侧通道攻击威胁度量方法

边根庆[1,2]，翟红[1]，邵必林[2]
（1.西安建筑科技大学信息与控制工程学院，710055，西安；2.西安建筑科技大学管理学院，710055，西安）

摘要：针对云平台中同驻虚拟机间共享物理资源，一些恶意用户通过探测、分析共享资源的信息来隐蔽获取其他用户的私密信息，进而可能引发侧通道攻击潜在威胁的问题，提出了一种基于云模型的同驻虚拟机侧通道攻击威胁度量方法。该方法在分析同驻虚拟机侧通道攻击特征的基础上，利用云模型在多属性决策不确定性转换及模糊性与随机性评估上的强大优势，对云用户的潜在侧通道攻击威胁进行了多指标综合度量评价。实验结果表明，利用该方法对云用户进行威胁度量得出的最大相似度为58.42%、36.47%、46.96%的评价结果符合假定的威胁等级，验证了该方法的可行性。该方法综合考虑了侧通道攻击威胁指标，充分发挥了云模型的度量优势，为云环境中同驻虚拟机间的侧通道攻击检测和防御研究与应用提供了重要依据。

关键词：侧通道攻击；同驻虚拟机；云模型；威胁度量方法
中图分类号：TP301.4 **文献标志码**：A **文章编号**：0253-987X(2016)04-0021-07

A Measurement Method of Side-Channel-Attacks Threat for Co-Residency Virtual Machines Based on Cloud Model

BIAN Genqing[1,2], ZHAI Hong[1], SHAO Bilin[2]
(1. School of Information and Control Engineering, Xi'an University of Architecture and Technology, Xi'an 710055, China;
2. School of Management, Xi'an University of Architecture and Technology, Xi'an 710055, China)

Abstract: A cloud model-based method for measuring the side-channel-attacks threat of the co-residency virtual machines is proposed to solve the potential threat problem of the side-channel-attacks, which is caused by the fact that some malicious users stealthily obtain other users' private information through detecting and analyzing the physical resources shared among the co-residency virtual machines in the cloud platform. Based on the analysis of the side-channel-attacks features, the method makes a comprehensive evaluation for users' potential threat from side-channel-attacks by using the cloud model, which has great advantages in the uncertainty conversion of multi-attribute decision making and the evaluation of fuzziness and randomness. Experimental results show that the maximum similarities 58.42%, 36.47% and 46.96% of the cloud users in the evaluation of the proposed method comply with the assumed threat level, proving the feasibility of the method. The method comprehensively considers the indexes of the side-channel-attacks threat, takes full advantage of the cloud model in metrics, and provides an

收稿日期：2015-12-14。 作者简介：边根庆(1968—)，男，博士生，副教授；翟红(通信作者)，女，硕士生。 基金项目：国家自然科学基金资助项目(61272458)；陕西省自然科学基础研究计划资助项目(2014JM2-6119)；榆林市科技计划资助项目(2014CXY-12)。
网络出版时间：2016-03-02 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20160302.1259.004.html

important basis for the research and application of the side-channel-attacks threat detection and defense for co-residency virtual machines in cloud environment.

Keywords: side-channel-attacks; co-residency virtual machines; cloud model; threat metrics method

云安全问题早已成为学术界、工业界关注的焦点,伴随着云环境中资源虚拟化、计算任务和服务外包、跨域使用等特点,不同用户的虚拟资源很可能会被映射到相同的物理资源上[1]。若非法用户通过探测、分析共享物理资源信息的方式来隐蔽地获取其他用户的相关信息,必使云环境中同驻虚拟机[2](virtual machine, VM)间的隔离性受到破坏,用户的虚拟环境信息泄露从而受到侧通道攻击(side-hannel-attacks,SCA)的威胁。SCA 威胁必将是云平台的极大安全挑战[3-4]。

目前,对于云平台中侧通道攻击的防御主要围绕两方面进行:一方面是对侧通道攻击实施环境进行破坏,加大非法用户 SCA 攻击的难度系数,通过加密侧通道信息[5-6]或对物理的共享资源进行隔离[7]等方式,来达到阻断侧通道攻击的目的,然而这类方法会在一定程度上增加系统开销,应用到实际环境有一定的困难;另一方面则是对异常行为进行检测[8-9],通过监视虚拟机行为,对侧通道及隐蔽信道进行识别,发现系统中可能存在的侧通道攻击威胁,从而减小侧通道攻击的危害,为用户提供一个相对安全的云环境[10],然而这些检测方法能够检测的范围相对来说还不够全面。

由于云模型在不确定性转换上具有强大的优势,能很大程度地保留评估过程中固有的不确定性,提升评估结果的可信度,因此本文将云环境中同驻虚拟机侧通道攻击的一些特征和云模型在模糊性与随机性度量方面的优势相结合,研究并设计了一种基于云模型的同驻虚拟机侧通道攻击威胁度量方法(side-channel-attacks threat metrics in co-residency VM based on cloud model)。该方法对检测和防御云环境中侧通道攻击行为,降低侧通道攻击风险具有重要的参考价值。

1 云模型与侧通道攻击

1.1 云模型

云模型[11]是当前非常优秀的度量评价方法之一,它将模糊与随机的特性相结合,为定性定量相结合的信息决策处理提供了有效的评估度量方法。

云定义:设 U 为精确数值表示的定量论域且 $U=\{x\}$,S 是 U 空间上的定性概念,若定量值 $x\in U$,并且 x 是定性概念 S 的一次随机实现,x 对 S 的隶属度 $S_\mu(x)\in[0,1]$ 是有稳定倾向的随机数,$S_\mu:U\to[0,1]$,$\forall x\in U$,$x\to S_\mu(x)$,则 x 在论域 $U=\{x\}$ 上的分布称作云(Cloud),记为 $S(x)$,其中一组 $(x,S_\mu(x))$ 称作一个云滴(Cloud Droplet)。

云的三元组定义:设 $N^3(E_x,E_n,H_e)$ 表示云的数字特征,其中 E_x、E_n、H_e 分别称为云的期望(Expect value)、熵(Entropy)和超熵(Hyper entropy)。E_x 代表 S 的信息中心值,被作为定性概念最具代表性的点。E_n 表示定性概念的可度量粒度,熵越大粒度越大,模糊性也越大。H_e 为熵的熵,是不确定性状态变化的度量,表示定性概念值的样本出现的随机性,揭示了模糊性与随机性的关联。

所有在论域 U 中定量值的元素 x 对定性概念 S 的隶属值基本落在 $[E_x-3E_n,E_x+3E_n]$ 之中,而其落在 $[E_x-3E_n,E_x+3E_n]$ 之外的定量值是极小概率发生事件,故可忽略不计[12]。

1.2 侧通道攻击

最早的侧通道攻击概念[13]是由 Kocher 提出的,侧通道攻击指的是攻击者能够根据电磁辐射、功耗等方式泄露出能量信息的数据以及物理磁盘、内存和 CPU 的利用率等信息与已知的内部物理机中运算操作数之间的相关联系来进行理论分析,隐蔽获取系统的某些关键信息,从而制定出可行的攻击方案。SCA 以低代价高效率而著称,常见的有简单能耗分析攻击、差分功耗分析攻击、故障注入攻击等[14],这些侧通道攻击方法主要针对的是单机环境中的加密设备与加密算法。非法用户在云环境中进行侧通道攻击时,通过将其控制运行的 VM 实例部署到攻击目标 VM 所在的物理机,分析所在物理机的网络队列、CPU 缓存及其他缓冲器等状态信息,获取其他用户的私密信息。

云平台中恶意用户能够实施侧通道攻击的必要条件之一就是需要与攻击目标 VM 同驻。在 Amazon 的 EC2 中,Ristenpart 等通过研究发现,恶意用户以较低代价就能实现 40%的 VM 同驻率,并成功地通过同驻的物理机盗取其他用户虚拟机私密信息[15]。Alabdulhafez 等利用内置的模拟器作为测

试床，将攻击者 VM 部署到与被攻击者 VM 相同的物理机上，通过恶意侧通道攻击方式有效获取同驻虚拟机中的关键敏感信息[16]，例如服务窃取、提取解密密钥、利用 VMware 泄漏的源代码及一些公开披露的 CVE（common vulnerabilities and exposure）漏洞等。桂小林等在实际的云计算系统（青云实验平台）中对 CPU cache 的侧通道攻击进行了大量实验，发现恶意用户实施同驻虚拟机侧通道攻击的成功率与恶意用户拥有和控制的 VM 数量有很大关系[17]，绝大部分恶意用户在发动侧通道攻击前会进行同驻检测，同时为降低攻击成本，会在同驻探测完成后就撤销探测 VM。在此基础上，桂小林等通过对 SCA 的行为分析，得出了 7 种可能发生侧通道攻击威胁的指标。

2　基于云模型的同驻虚拟机侧通道攻击威胁度量方法

同驻虚拟机侧通道攻击威胁度量是一种多属性决策问题，而云模型可以集成定性概念的模糊性和随机性，能很好地对多属性评价的定量与定性进行转换，让整个评估度量的结果更加可信[18]。本文在分析同驻虚拟机侧通道攻击指标基础上，利用云模型的度量优势，设计了一种基于云模型的同驻虚拟机侧通道攻击度量方法。该方法主要分为两步：确定侧通道攻击威胁的各度量指标；采用云模型的度量方法对各指标进行综合度量。

基于云模型的同驻虚拟机侧通道攻击威胁度量方法的具体流程如图 1 所示。

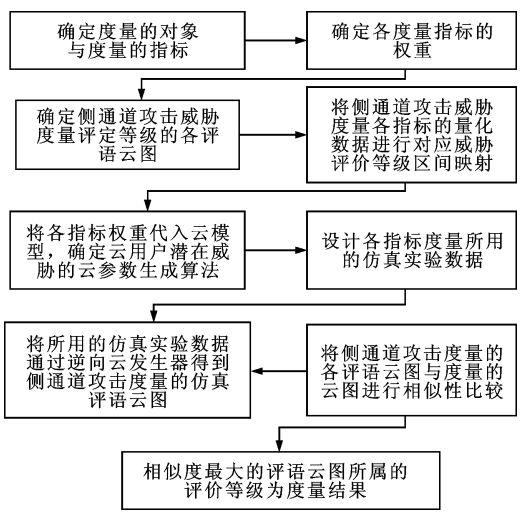

图 1　基于云模型的同驻虚拟机侧通道攻击威胁度量方法流程图

2.1　确定侧通道攻击威胁度量指标集

确定度量的对象为同驻虚拟机侧通道攻击威胁。设度量的指标集为 S_{td}，且 $S_{td}=\{S_{td1},S_{td2},S_{td3},S_{td4},S_{td5},S_{td6},S_{td7}\}$，如图 2 所示，此处的度量指标采用文献[17]中提出的 7 个侧通道攻击指标，可根据实际评估环境情况对评估指标进行调整。

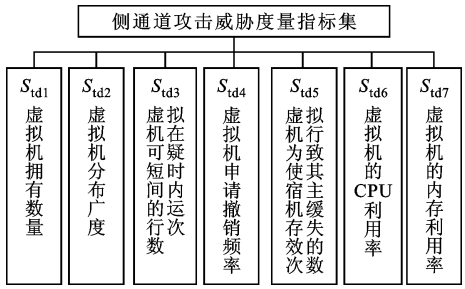

图 2　侧通道攻击威胁度量指标集

确定各度量指标的权重：设度量指标的权重集为 W（指标 S_{tdi} 对应于其相应权重 W_i），且满足 $W_1+W_2+W_3+W_4+W_5+W_6+W_7=1$。

2.2　采用云模型的度量方法对各指标进行综合度量

本文将侧通道攻击威胁度量的评定分为 7 个等级并组成一组定性度量概念，记为 V，其中 $V=\{V_1$ 威胁极低，V_2 威胁低，V_3 威胁较低，V_4 威胁中，V_5 威胁较高，V_6 威胁高，V_7 威胁极高$\}$。由云模型的概念可知，V 的映射区间为$[0,1]$，通过区间划分来反映评定的等级，接着将侧通道攻击威胁度量各指标量化数据进行区间映射。

2.2.1　*确定侧通道攻击威胁度量评定等级的各评语云图*　利用双边约束法将其定量变量云化为正向云模型。假设某一度量等级的双边约束为$[P_{min},P_{max}]$，采用约束条件的中值来代表期望值，用主要作用区域来作为双边约束区域的云，从而近似表示各等级评语的定性度量概念。某一度量等级的云参数为

$$E_x=(P_{max}+P_{min})/2 \tag{1}$$

$$E_n=(P_{max}-P_{min})/6 \tag{2}$$

$$H_e=K \tag{3}$$

式中：K 为常数，它可随变量本身的模糊程度来具体地调整。对于单边约束，可先根据最大的上限或下限来确定一个缺省边界参数/期望值[12]。

本文将定性度量概念 V 中的每一等级度量概念划分为如表 1 所示的度量区间，并给出了各评语云的参数，由式(1)～式(3)求得。

将表 1 中侧通道攻击威胁度量评定的 7 个等级评语在连续的语言值标尺上，采用正向云发生器算法生成如图 3 所示的侧通道攻击威胁度量的各等级评语云图。

表 1 各等级评语云的参数表

评语	度量区间	E_x	E_n	H_e
V_1	[0.0,0.1]	0.00	0.016 67	0.02
V_2	[0.1,0.2]	0.15	0.016 67	0.02
V_3	[0.2,0.4]	0.30	0.033 33	0.02
V_4	[0.4,0.6]	0.50	0.033 33	0.02
V_5	[0.6,0.8]	0.70	0.033 33	0.02
V_6	[0.8,0.9]	0.85	0.016 67	0.02
V_7	[0.9,1.0]	1.00	0.016 67	0.02

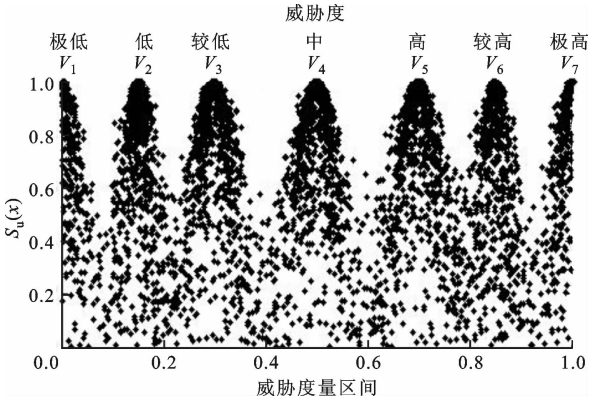

图 3 侧通道攻击威胁度量的各等级评语云图

2.2.2 确定侧通道攻击威胁度量各指标的等级映射区间方法 由于侧通道攻击威胁度量各指标的定性概念量化数据并不是在[0,1]区间,为了更好的将其反映到威胁等级度量的云模型上,需将其映射到相应的等级度量区间。

假设用户在某物理机上拥有超过一半多的 VM 实例则本文设定该用户的潜在威胁性为高,若 S_{td1} 具体映射区间为 $S_{td1}\geqslant 50\%$,将其映射到威胁极高[0.9,1];$30\%\leqslant S_{td1}<50\%$ 映射到威胁高[0.8,0.9];$15\%\leqslant S_{td1}<30\%$ 映射到威胁较高[0.6,0.8];$10\%\leqslant S_{td1}<15\%$ 映射到威胁中[0.4,0.6];$5\%\leqslant S_{td1}<10\%$ 映射到威胁较低[0.2,0.4];$2\%\leqslant S_{td1}<5\%$ 映射到威胁低[0.1,0.2];$S_{td1}<2\%$ 或 $S_{td1}=100\%$ 映射到威胁极低[0,0.1]。

本文假设云平台中的服务器数量为 S,若用户在云平台上的虚拟机占用的服务器数量超过一半以上,则认定其威胁可能性大,S_{td2} 的具体映射区间为:$(S_{td2}\geqslant 0.6S)\sim[0.9,1.0]$;$(0.5S\leqslant S_{td2}<0.6S)\sim[0.8,0.9]$;$(0.4S\leqslant S_{td2}<0.5S)\sim[0.6,0.8]$;$(0.3S\leqslant S_{td2}<0.4S)\sim[0.4,0.6]$;$(0.2S\leqslant S_{td2}<0.3S)\sim[0.2,0.4]$;$(0.1S\leqslant S_{td2}<0.2S)\sim[0.1,0.2]$;$(S_{td2}<0.1S)\sim[0.0,0.1]$。

假设用户虚拟机在可疑短时间 T 内的运行次数威胁阈值为 N,则 S_{td3} 的具体映射区间为:$(S_{td3}\geqslant 2N)\sim[0.9,1.0]$;$(1.5N\leqslant S_{td3}<2N)\sim[0.8,0.9]$;$(1N\leqslant S_{td3}<1.5N)\sim[0.6,0.8]$;$(0.5N\leqslant S_{td3}<1N)\sim[0.4,0.6]$;$(0.3N\leqslant S_{td3}<0.5N)\sim[0.2,0.4]$;$(0.1N\leqslant S_{td3}<0.3N)\sim[0.1,0.2]$;$(0.1N\leqslant S_{td3})\sim[0.0,0.1]$。

S_{td4}、S_{td5} 指标与 S_{td3} 的映射类似,首先设定威胁阈值,再根据阈值映射到相应区间。S_{td6} 和 S_{td7} 指标的映射与 S_{td1} 的威胁假设类似,故映射区间可参照 S_{td1},考虑到篇幅有限这里不再赘述。

2.2.3 将各指标权重代入云模型确定云用户威胁云参数生成算法 对同驻虚拟机侧通道攻击威胁,本文给定了 7 个度量指标(后期可自由增加指标),将 7 个指标的数据通过逆向云发生器[18]得到威胁性云参数$(E_{x_i},E_{n_i},H_{e_i})$。在逆向云发生器中,威胁性云参数 E_{x_i}、E_{n_i}、H_{e_i} 为

$$E_{x_i}=\overline{X} \tag{4}$$

$$E_{n_i}=(\pi/2)^{1/2}\times\frac{1}{n}\sum_{j=1}^{n}|x_j-\overline{X}| \tag{5}$$

$$H_{e_i}=(S^2-E_{n_i}^2)^{1/2} \tag{6}$$

式中:$i=7$;$\overline{X}$ 为 j 组数据的样本均值;S^2 为样本方差;$\frac{1}{n}\sum_{j=1}^{n}|x_j-\overline{X}|$ 为一阶样本绝对中心距。

将各指标的威胁性云参数结合各指标所占权重通过下式求出威胁度量的综合云参数 $S_\mu=(E_x,E_n,H_e)$

$$E_x=\frac{E_{x1}E_{n1}W_1+\cdots+E_{x7}E_{n7}W_7}{E_{n1}W_1+\cdots+E_{n7}W_7} \tag{7}$$

$$E_n=E_{n1}W_1+\cdots+E_{n7}W_7 \tag{8}$$

$$H_e=H_{e1}W_1+\cdots+H_{e7}W_7 \tag{9}$$

2.2.4 利用云相似性比较算法确定威胁度量等级 对确定的威胁度量综合云参数 $S_\mu=(E_x,E_n,H_e)$ 与各等级 V_i 的评语云参数(E_{xi},E_{ni},H_{ei})进行相似性计算,本文中使用的相似性判断方法为带权重的欧式距离法,其中与威胁评语云相似度最大的值则为用户威胁度量评估结果[19]。

输入为仿真用户威胁度量综合云参数 $S_\mu=(E_x,E_n,H_e)$和表 1 中的侧通道攻击威胁度量的各等级 V_i 的评语云(E_{xi},E_{ni},H_{ei}),以及确定的 3 个向量参数所占权重值 W_{E_x}、W_{E_n}、W_{H_e},且 $W_{E_x}+W_{E_n}+W_{H_e}=1$。输出为威胁度量等级 V_i。

具体算法流程如下:

步骤 1 $D_i=(W_{E_x}(E_x-E_{x_i})^2+W_{E_n}(E_n-E_{n_i})^2+$

$W_{H_e}(H_e-H_{e_i})^2)^{1/2}$；

步骤 2　$\delta_i=1/D_i$；

步骤 3　$O_i=(\delta_i/\sum_{i=1}^{n}\delta_i)$，其中 δ_i 为带权重的欧氏距离，O_i 为相似度；

步骤 4　重复步骤 1 至步骤 3，算出所有的 O_i；

步骤 5　$\max(O_i)$对应 V_i 为云用户威胁度量等级。

3　实验与分析

为验证基于云模型的同驻虚拟机侧通道攻击威胁度量方法的可行性，本文设计了 3 种类型的云用户 U_1、U_2、U_3，假定其分别为低、中、高威胁用户。利用第 2 节提出的度量方法对云用户进行侧通道攻击威胁等级度量。采用随机数生成器给出了如表 2 所示的测试数据(可根据实际情况自由选择所用的数据规模，本文中每个指标分别给出了 5 组数据)。

表 2　云用户度量指标测试数据表

用户	指标	指标所用测试数据
U_1	S_{td1}	0.215 76,0.134 64,0.216 59,0.225 84,0.185 60
	S_{td2}	0.103 88,0.291 02,0.047 39,0.198 44,0.178 40
	S_{td3}	0.252 17,0.352 34,0.261 93,0.118 86,0.188 91
	S_{td4}	0.292 52,0.193 70,0.147 31,0.214 32,0.133 78
	S_{td5}	0.159 60,0.078 21,0.114 96,0.068 75,0.017 96
	S_{td6}	0.208 66,0.016 51,0.053 13,0.198 07,0.180 86
	S_{td7}	0.199 98,0.111 21,0.088 71,0.272 14,0.321 23
U_2	S_{td1}	0.452 17,0.557 24,0.543 51,0.550 82,0.455 12
	S_{td2}	0.555 46,0.601 46,0.511 93,0.615 11,0.536 31
	S_{td3}	0.297 13,0.440 73,0.160 73,0.332 79,0.359 04
	S_{td4}	0.554 21,0.466 18,0.349 18,0.486 86,0.500 35
	S_{td5}	0.518 15,0.459 78,0.638 51,0.478 80,0.414 66
	S_{td6}	0.333 02,0.431 23,0.528 30,0.416 39,0.302 61
	S_{td7}	0.361 71,0.246 90,0.454 72,0.489 14,0.361 17
U_3	S_{td1}	0.742 61,0.784 10,0.739 75,0.813 46,0.812 51
	S_{td2}	0.764 28,0.759 13,0.837 91,0.789 19,0.833 05
	S_{td3}	0.835 04,0.720 47,0.777 63,0.889 26,0.808 62
	S_{td4}	0.782 67,0.867 32,0.984 59,0.782 64,0.870 63
	S_{td5}	0.822 37,0.652 40,0.793 41,0.821 01,0.720 04
	S_{td6}	0.760 79,0.900 86,0.872 87,0.736 99,0.859 62
	S_{td7}	0.827 03,0.883 62,0.873 99,0.798 88,0.779 83

将上面 3 个用户的各指标所用的仿真实验测试数据通过逆向云算法得到各指标的威胁性云数字特征见表 3～表 5，然后将各指标权重(本文仿真实验中的权重数据来源于文献[17])通过式(7)～式(9)求出威胁度量综合云参数 $S_\mu=(E_x,E_n,H_e)$的侧通道攻击度量的仿真云图，如图 4 所示。

表 3　U_1 的各指标威胁性云数字特征(对 H_e 为负情况取 0)

指标	E_x	E_n	H_e
S_{td1}	0.195 69	0.035 660	0.011 08
S_{td2}	0.163 83	0.088 425	0.029 43
S_{td3}	0.234 84	0.081 172	0.031 80
S_{td4}	0.196 33	0.057 245	0.026 41
S_{td5}	0.087 90	0.049 515	0.018 83
S_{td6}	0.131 45	0.096 882	0.000 00
S_{td7}	0.198 65	0.098 956	0.015 75

通过式(7)～式(9)求出的 U_1 仿真云参数为(0.158 06,0.079 65,0.014 21)。

表 4　U_2 的各指标威胁性云数字特征(对 H_e 为负情况取 0)

指标	E_x	E_n	H_e
S_{td1}	0.511 77	0.058 281	0.000 00
S_{td2}	0.564 05	0.044 348	0.000 00
S_{td3}	0.318 08	0.089 390	0.050 43
S_{td4}	0.471 36	0.063 845	0.040 60
S_{td5}	0.501 98	0.076 552	0.036 76
S_{td6}	0.402 31	0.084 719	0.027 11
S_{td7}	0.382 73	0.089 438	0.031 09

通过式(7)～式(9)求出的 U_2 仿真云参数为(0.423 54,0.081 26,0.032 06)。

表 5　U_3 的各指标威胁性云数字特征(对 H_e 为负情况取 0)

指标	E_x	E_n	H_e
S_{td1}	0.778 49	0.037 405	0.000 00
S_{td2}	0.796 71	0.038 871	0.000 00
S_{td3}	0.806 20	0.057 306	0.026 30
S_{td4}	0.857 57	0.075 114	0.035 55
S_{td5}	0.761 85	0.075 826	0.000 00
S_{td6}	0.826 23	0.077 541	0.000 00
S_{td7}	0.832 67	0.046 257	0.000 00

通过式(7)～式(9)求出的 U_3 仿真云参数为(0.807 03,0.065 31,0.003 98)。

分别将 U_1、U_2、U_3 的仿真云参数通过云相似性比较算法与表 1 中侧通道攻击威胁度量的各等级评语云参数进行相似度比较，设 W_{E_x}、W_{E_n}、W_{H_e} 3 个向量参数占的权重值分别为(0.7,0.2,0.1)。表 6 为

各用户仿真云与表 1 中各等级评语云的相似度表。

表 6 各用户仿真云与各等级评语云的相似度表

评语	相似度/%		
	U_1	U_2	U_3
V_1	12.54	6.93	2.94
V_2	58.42	10.68	3.61
V_3	14.06	23.33	4.68
V_4	5.91	36.47	7.72
V_5	3.74	10.61	21.88
V_6	2.93	6.88	46.96
V_7	2.40	5.10	12.19

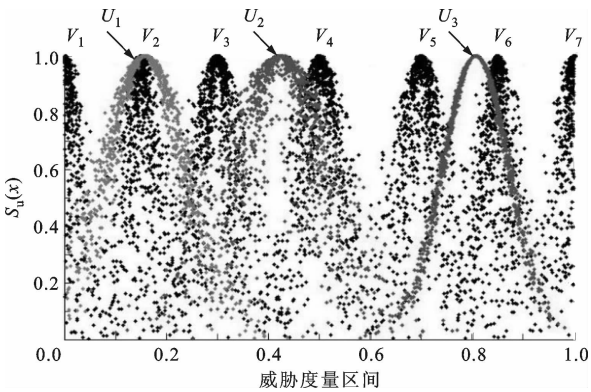

图 4 各等级评语云与 3 个用户仿真云比较图

由表 6 可知，用户 U_1 的最大相似度为 58.42%，落在 V_2 评语上为威胁度低，用户 U_2 的最大相似度为 36.47%，落在 V_4 评语上为威胁度中，用户 U_3 的最大相似度为 46.96%，落在 V_6 评语上为威胁度高。从图 4 中也可以清晰地看到，3 个用户的威胁度量范围依次落在了威胁低、中、高云图附近，满足假定的 3 个用户的威胁属性，从而验证了本文提出的基于云模型的同驻虚拟机侧通道攻击威胁等级度量方法具有的可行性。

4 结 语

本文以桂小林等提出的侧通道攻击威胁指标为基础，结合云模型在多属性决策度量上的优势，提出了一种基于云模型的同驻虚拟机侧通道攻击威胁等级度量方法，并通过该方法对云平台中的同驻虚拟机侧通道攻击的威胁性进行了多指标综合评价。实验表明，该方法能综合考虑侧通道攻击威胁各指标的影响，实现对威胁等级的度量。本文方法是对云模型理论应用领域的一种新探索，同时对云环境中同驻虚拟机间的侧通道攻击检测和防御研究及其应用具有重要参考价值。

参考文献：

[1] 丁滟，王怀民，史佩昌，等. 可信云服务 [J]. 计算机学报，2015，38(1)：133-149.
DING Yan，WANG Huaimin，SHI Peichang，et al. Trusted cloud service [J]. Chinese Journal of Computers，2015，38(1)：133-149.

[2] BATES A，MOOD B，PLETCHER J，et al. On detecting co-resident cloud instances using network flow water-marking techniques [J]. International Journal of Information Security，2014，13(2)：171-189.

[3] GENKIN D，PIPMAN I，TROMER E. Get your hands off my laptop：physical side-channel key-extraction attacks on PCs [J]. Lecture Notes in Computer Science，2014，8731：242-260.

[4] WU Z，XU Z，WANG H. Whispers in the hyper-space：high-bandwidth and reliable covert channel attacks inside the cloud [J]. IEEE/ACM Transactions on Networking，2015，23(2)：603-614.

[5] LING Z，LUO J，ZHANG Y，et al. A novel network delay based side channel attack：modeling and defense [C]// Proceedings of the 2012 IEEE Conference on Computer Communications. Piscataway，NJ，USA：IEEE，2012：2390-2398.

[6] RAJ H，NATHUJI R，SINGH A，et al. Resource management for isolation enhanced cloud services [C]// Proceedings of the 2009 ACM Workshop on Cloud Computing Security. New York，USA：ACM，2009：77-84.

[7] 乔然，胡俊，荣星，等. 云计算客户虚拟机间的安全机制研究与实现 [J]. 计算机工程，2014(12)：26-32.
QIAO Ran，HU Jun，RONG Xing，et al. Research and implementation of security mechanism among guest virtual machine in cloud computing [J]. Computer Engineering，2014(12)：26-32.

[8] DAI W，JIN H，ZOU D，et al. TEE：a virtual DRTM based execution environment for secure cloud-end computing [J]. Future Generation Computer Systems，2010，49(3)：663-665.

[9] SERDAR C，CARLA E B，CLAY S. IP covert channel detection [J]. ACM Trans on Information and System Security，2009，12(4)：1-29.

[10] YU Si，GUI Xiaolin，ZHANG Xuejun，et al. Detecting cache-based side channel attacks in the cloud：an approach with cascade detection mode [J]. Journal of Internet Technology，2014，15(6)：903-915.

[11] LI Deyi，LIU Changyu，LIU Luying，et al. Study on the universality of the normal cloud model [J]. Engineering Sciences，2005(2)：18-24.

[12] 王晓峰，洪磊. 基于云的概念空间模型研究 [J]. 计算机工程与应用，2010，46(20)：202-206.
WANG Xiaofeng，HONG Lei. Study on concept space model based on the cloud theory [J]. Computer Engineering and Applications，2010，46(20)：202-206.

[13] KOCHER P，JAFFE J，JUN B. Differential power Analysis [J]. Lecture Notes in Computer Science，1999，1666：388-397.

[14] KIM H，BRUCE N，LEE H J，et al. Side channel attacks on cryptographic module：EM and PA attacks accuracy analysis [J]. Lecture Notes in Electrical Engineering，2015，339：509-516.

[15] RISTENPART T，TROMER E，SHACHAM H，et al. Hey，you，get off of my cloud：exploring information leakage in third-party compute clouds [C]// Proceedings of the 16th ACM Conference on Computer and Communications Security. New York，USA：ACM，2009：199-212.

[16] ALABDULHAFEZ A，EZHILCHELVAN P. Experimenting on virtual machines co-residency in the cloud：a comparative study of available test beds [C]// Proceedings of the 29th Annual ACM Symposium on Applied Computing. New York，USA：ACM，2014：363-365.

[17] 桂小林，余思，黄汝维，等. 一种面向云计算环境侧通道攻击防御的虚拟机部署方法：中国，CN2011 10376037.0 [P]. 2012-07-11.

[18] 杜湘瑜，尹全军，黄柯棣，等. 基于云模型的定性定量转换方法及其应用 [J]. 系统工程与电子技术，2008，30(4)：772-776.
DU Xiangyu，YIN Quanjun，HUANG Keli，et al. Transformation between qualitative variables and quantity based on cloud models and its application [J]. Systems Engineering and Electronics，2008，30(4)：772-776.

[19] 陈思，王曙燕，孙家泽，等. 基于云模型的可信软件可靠性度量模型 [J]. 计算机应用研究，2014，31(9)：2729-2731.
CHEN Si，WANG Shuyan，SUN Jiaze，et al. Trusted software reliability measures based on cloud model [J]. Application Research of Computers，2014，31(9)：2729-2731.

（编辑　武红江）

（上接第 6 页）

[2] AN Ning，JIANG Lili，WANG Jianyong，et al. Toward detection of aliases without string similarity [J]. Information Sciences，2014，261(10)：89-100.

[3] ANWAR T，ABULAISH M. Namesake alias mining on the Web and its role towards suspect tracking [J]. Information Sciences，2014，276(20)：123-145.

[4] LIU Zhaoli，QIN Tao，GUAN Xiaohong，et al. Alias detection across multi-online applications based on user's behavior characteristics [C]// Proceedings of the 2015 IEEE Trustcom. Piscataway，NJ，USA：IEEE Computer Society，2015：1154-1159.

[5] KUMAR S，ZAFARANI R，LIU Huan. Understanding user migration patterns in social media [C]// Proceedings of the 25th AAAI Conference on Artificial Intelligence. New York，USA：ACM，2011：1-6.

[6] BEKKERMAN R，MCCALLUM A. Disambiguating Web appearances of people in a social network [C]// Proceedings of the International Conference on World Wide Web. New York，USA：ACM，2005：463-470.

[7] HIRSCHBERG D S. Algorithms for the longest common subsequence problem [J]. Journal of the ACM，1977，24(4)：664-675.

[8] WANG Chenxu，GUAN Xiaohong，QIN Tao. Who are active? an in-depth measurement on user activity characteristics in Sina Microblog [C]// Proceedings of the 2012 IEEE Global Communications Conference. Piscataway，NJ，USA：IEEE Communication Society，2012：2083-2088.

[9] LEVENSHTEIN V I. Binary codes capable of correcting deletions，insertions and reversals [J]. Soviet Physics Doklady，1965，163(4)：845-848.

[10] AHO A V，HIRSCHBERG D S，ULLMAN J D. Bounds on the complexity of the longest common subsequence problem [J]. Journal of the ACM，1976，23(1)：104-109.

[11] QIN Tao，ZHAO Dan，ZHU Min，et al. Mapping different online behaviors to physical user for comprehensive knowledge-pushing services [C]// Proceedings of the IEEE International Conference on Communications. Piscataway，NJ，USA：IEEE Communication Society，2014：671-675.

[12] WISE M J. String similarity via greedy string tiling and running KarpRabin matching：463 [R]. Sydney，Australia：University of Sydney. Department of Computer Science，1993.

（编辑　武红江）