文章编号:1671-4598(2024)06-0139-06 DOI:10.16526/j.cnki.11-4762/tp.2024.06.021 中图分类号:TP393 文献标识码:A

基于演化博弈的大数据信息泄漏风险访问控制模型设计

周海徽
(武警上海总队,上海 201620)

摘要:大数据信息泄漏会导致网络主机所承担的运行风险增加,严重时下级网络终端会出现无法访问大数据信息服务器的情况;针对上述问题,设计了基于演化博弈的大数据信息泄漏风险访问控制模型;以演化博弈模型为基础,完成对大数据信息均衡点的演化处理,求解信息博弈概率,推导演化博弈模型表达式,从而完善基于演化博弈的大数据信息模糊化处理流程;计算大数据信息泄漏行为的信任度标准,参考信息监控器设置条件,实现对大数据信息泄漏风险的评估;针对风险评估结果,完成大数据信息的访问证据取样,计算访问控制阈值,实现对信息泄漏风险访问的控制,完成基于演化博弈的大数据信息泄漏风险访问控制模型的设计;实验结果表明,所提方法的大数据信息瞬时泄漏量始终小于2.3×10^{11} MB,网络主机所承担的运行风险得到有效控制,下级网络终端不会出现无法访问大数据信息服务器的情况。

关键词:演化博弈;大数据信息;泄漏风险;访问控制模型;均衡点演化;信任度;信任证据

Design of Access Control Model for Big Data Information Leakage Risk Based on Evolutionary Game

ZHOU Haihui
(Shanghai Armed Police Corps, Shanghai 201620, China)

Abstract: The leakage of big data information will increase operational risk borne by network hosts, and in serious cases, lower level network terminals may be unable to access big data information servers. To solve the above problems, a big data information leakage risk access control model based on evolutionary game was designed. Based on the evolutionary game model, complete the evolutionary processing of big data information balance, solve the probability of information game, and derive the expression of the evolutionary game model, so as to improve the big data information fuzzy processing process based on the evolutionary game. Calculate the trust standard of big data information leakage behavior, refer to the information monitor setting conditions, and realize the assessment of big data information leakage risk. Aimed at the risk assessment results, complete the access evidence sampling of big data information, calculate the access control threshold, realize the control of information leakage risk access, and complete the big data information leakage risk access control model design based on the evolutionary game. Experimental results show that the big data information instantaneous leakage of the proposed method is always less than 2.3×10^{11} MB, the operation risk borne by the network host is effectively controlled, and the lower level network terminal will not be unable to access the big data information server.

Keywords: evolutionary game; big data information; leakage risk; access control model; evolution of equant; trust level; evidence of trust

0 引言

大数据信息是指一种规模极大的集合类数据信息参量。大数据信息需要在不同的系统、服务器或节点之间进行传输,以满足数据共享、处理和存储的需求。同时,由于大数据的总量巨大,无法被单个计算机完全处理,因此,需要采用分布式架构体系,以搭建完整的网络平台结构。分布式架构将计算任务和数据分布到多个节点上,通过并行处理和数据分片等技术,提高处理效率和可扩展性,从而优化大数据的管理和处理能力。大数据信息可以同时适应数据挖掘与信息查询指令,且信息参量的传输行为并不会受到网络信道组织运输能力等外界条件的影响,这就表示即使是在网络体系不能保持稳定连接状态的情况下,大数据信息样本也不会出现不完全传输行为[1]。随着物联网存储空间的不断扩大,大数据信息传输速率与终端设备响应速率可能出现不完全匹配的情况,而这也是导致大数据信息出现泄漏的主要原因。在大数据信息泄漏行为的影响下,下级网络终端会因为无法准确分辨所需信息参量,而出现无法访问大数据信息服务器的情况,若非访问行为的表现过于严重,则会使整个物联网平台表现出瘫痪状态。因此,对大数据信息泄漏风险访问控制进行研究具

收稿日期:2023-06-30; **修回日期**:2023-08-03。
作者简介:周海徽(1983-),男,研究生,工程师。
引用格式:周海徽.基于演化博弈的大数据信息泄漏风险访问控制模型设计[J].计算机测量与控制,2024,32(6):139-144,151.

有重要意义。

文献［2］提出了基于 MyBatis 和 CBAC 的访问控制方法。使用 MyBatis 插件开发独立的访问控制器组件，联合 SDBatis 机制，测试大数据信息泄漏行为的表现强度，从而在应对多变性访问行为的同时，为下级网络终端提供更多的平台端口组织。文献［3］提出了基于向量表征与计算的动态访问控制方法。在开放式环境中，定义多种不同的优化匹配规则，通过遍历匹配，完成对大数据信息参量的过滤处理，在信息样本的单位传输周期内，可以提供更多的访问终端节点。然而上述两种方法在控制信息样本瞬时泄漏量方面的应用能力有限，无法降低网络主机所承担的数据运行风险。

演化博弈是指不再将个体对象模型化为理想的博弈方式，而是认为个体对象只有通过不断试错，才能使数据信息达到一种博弈均衡的状态，且在整个过程中，物联网体系对于数据信息均衡性的考量遵循唯一的审核函数[4]。相较于其他类型的数据处理模型，演化博弈更适应物联网体系多变性的特征，能够在调节信息参量传输行为的同时，更改网络主机对数据样本的读写与存储作用机制，从而有效控制大数据信息泄漏行为的表现强度。为此，在物联网平台中，设计基于演化博弈的新型大数据信息泄漏风险访问控制模型。

1 基于演化博弈的大数据信息模糊化处理

对于大数据信息的模糊化处理，是设计大数据信息泄漏风险访问控制模型的基础环节，本章节在演化博弈模型的配合下，完善模糊化处理的具体实施流程。

1.1 演化博弈模型构建

构建演化博弈模型是根据大数据信息的均衡点演化结果，求解博弈概率，并以此推导完整的模型表达式。

1.1.1 大数据信息的均衡点演化

大数据信息均衡点演化是针对泄漏风险等级较高的大数据对象所进行的均衡性处置节点重排处理。由于物联网主机对于大数据样本的需求会随着传输任务的改变而发生变化，所以不一样的信息样本输入量，必然对应不一样的均衡点演化结果。

假设 α_1、α_2、…、α_n 为 n 个不同的大数据信息取样对象，属于 $[1,+\infty)$ 的数值区间，利用上述物理量，推导大数据信息输入阈值为：

$$\begin{cases} O_1 = p_1\alpha_1 \\ O_2 = p_2\alpha_2 \\ \quad\vdots \\ O_n = p_n\alpha_n \end{cases} \tag{1}$$

式中，$O_1,O_2,\cdots,O_n$ 表示 n 个不同的阈值参数，$p_1,p_2,\cdots,p_n$ 分别表示与大数据信息取样对象匹配的均衡性取样系数。

演化博弈模型规定，均衡点演化处理过程中，大数据信息输入阈值并不会发生变化，对于网络主机而言，这种稳定性的取样特征保证了演化处理结果的唯一性[5]。

利用公式（1），可将大数据信息均衡点演化条件表示为：

$$I = \frac{\frac{\vec{i}}{\chi}|\Delta U|}{\beta(O_1^{\,2}+O_2^{\,2}+\cdots+O_n^{\,2})} \tag{2}$$

式中，ΔU 表示待处理大数据信息样本的单位累积量，$\vec{i}$ 表示大数据信息样本的均衡点处置向量，χ 表示物联网环境中的数据样本演化处理系数，β 表示满足演化博弈模型的大数据信息取样参数。

均衡点演化的处理结果服务于大数据信息泄漏风险访问控制模型，且整个处置流程受到演化博弈模型的直接影响[6]。因此，为保证大数据信息取样、均衡点演化操作行为之间的相关性，演化博弈模型要求数据样本对象的取值属于同一信息传输周期，若同周期内信息样本数量不满足计算需求，可以适当延长取样周期。

1.1.2 演化后的大数据信息博弈概率求解

大数据信息博弈概率是指均衡点演化处理后，信息样本发生泄露传输行为的概率，考虑有效控制信息泄露风险，演化博弈模型规定求解大数据信息博弈概率时，应尽量取得其极小值结果。均衡点演化处理后，大数据信息样本的泄露风险虽然并不会出现无限扩张的能力，但由于下级网络终端在访问连接方面的需求等级相对较高，所以对于大数据信息博弈概率求解，也可以理解为对大数据信息样本泄露风险行为的进一步抑制处理[7-8]。

假设大数据信息演化指数取样集合为：

$$u = \{u_1,u_2,\cdots,u_\delta,u_{\delta+1}\} \tag{3}$$

其中：u_1、u_2、…、u_δ、$u_{\delta+1}$ 表示 $\delta+1$ 个不等于零的演化指数。δ 表示指数参量演化次数标记值，若以 u_δ 作为最后一个演化指数，在大数据信息样本总量无穷大的情况下，有可能导致取样结果无法与博弈概率指标保持正相关映射关系，所以在完成针对 u_δ 指数的取样后，还要针对 $u_{\delta+1}$ 指数继续取样。

关联大数据信息均衡点演化条件、大数据信息演化指数，在博弈系数 γ 的配合下，求解基于演化博弈模型的大数据信息博弈概率求解结果为：

$$Y = (\gamma-1)\left[\frac{I}{\dot{\boldsymbol{y}}}\times\frac{\sum_{e=1}\varphi_e\times|\ t\ |^2}{u}\right] \tag{4}$$

$\dot{\boldsymbol{y}}$ 表示大数据样本在均衡点演化条件下的信息特征，e 表示基于演化博弈模型的大数据信息传输配比参数，t 表示大数据信息博弈周期，φ_e 表示数据样本实时访问概率。如果博弈概率求解结果过大，会导致物联网主机对大数据信息泄漏风险的访问控制能力下降。

1.1.3 大数据信息的演化博弈模型推导

定义大数据信息演化博弈模型是按照演化博弈模型的应用需求，完成对具有泄漏风险的大数据信息进行取样。从本质层面来讲，演化博弈模型的推导既要求数据取样结果的唯一性，也要求信息取样结果之间的相关性。

1）演化博弈模型的唯一性：大数据信息泄漏风险访问

控制模型对于演化博弈模型唯一性的要求是指在建立控制模型过程中，不能按照演化博弈模型，取得两个或两个以上完全相同的信息样本，唯一性保证了所设计模型能够控制不同类型的大数据信息泄漏风险访问行为[9]。

2）演化博弈模型的相关性：控制模型对大数据信息泄漏风险访问行为提出了相关性要求，是指演化博弈模型对于大数据信息样本的取样，应关注关联信息参量之间的数值映射关系[10]。

唯一性针对部分大数据信息对象、相关性针对取样所得的所有大数据信息对象，在演化博弈模型中二者并不矛盾。

利用式（4），推导大数据信息的演化博弈模型表达式为：

$$E=\prod_{\varepsilon=1}\tilde{q}_{\varepsilon}+\varphi Y+(1-r)R' \tag{5}$$

式中，ε 为大数据信息核准系数，$\tilde{q}_{\varepsilon}$ 为单一信息样本的唯一性度量值，R' 为关联信息样本的相关性度量值，r 为演化博弈模型中的数据风险评估参数，φ 为基于演化博弈模型的数据样本置信度参数。演化博弈模型是设计大数据信息泄漏风险访问控制模型的核心参考条件，因此对于计算所需数据样本对象的取样，要求所涉及信息参量必须具有较高的泄漏风险。

1.2　基于演化博弈的大数据信息模糊化处理流程完善

大数据信息模糊化处理是在演化博弈模型的配合下，将具有泄漏风险的大数据信息整合成模糊化状态。风险项是评价已获取大数据信息泄露风险等级的关键指标，其定义值的求解参考演化博弈模型，且为保证模糊化处理结果的有效性，在下级网络终端的单位访问周期内，不能以两个完全相同的大数据信息参量作为处理对象[11]。

对于风险项指标的求解满足如下表达式：

$$W=\frac{\sum_{-\infty}^{+\infty}Q}{\frac{E(1-\eta)}{2}} \tag{6}$$

其中：Q 表示基于演化博弈的大数据信息泄露风险核定参数，且 $Q\neq 0$ 的不等式取值条件恒成立，η 表示具有泄露风险的大数据信息样本在互联网主机中的传输效率。

$Q>0$ 成立时，表示大数据信息传输方向与互联网主机中风险性访问行为的连接方向相同，当前情况下，大数据信息样本的传输效率相对较高，演化博弈模型在单位控制周期内，所需模糊化处理的大数据信息总量也就相对较多；反之，若 $Q<0$ 成立，则表示大数据信息传输方向与互联网主机中风险性访问行为的连接方向相反，此时大数据信息样本的传输效率较低，演化博弈模型在单位控制周期内，所需模糊化处理的大数据信息总量也就相对较少。

对于互联网主机而言，其在按照模糊化标准处理大数据信息时，既可以根据风险等级判定条件，定义风险性向量，也能够使其有效控制下级网络终端的访问接入行为。大数据信息模糊化处理流程如图 1 所示。

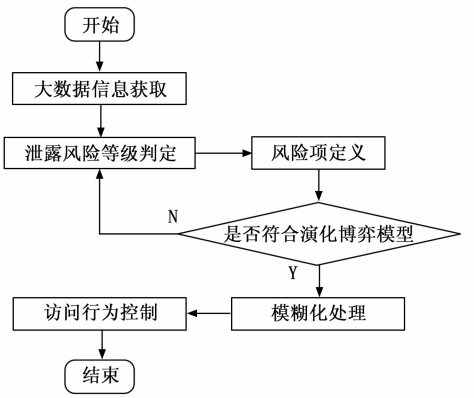

图 1　大数据信息模糊化处理流程图

如果具有泄露风险的大数据信息样本的单位累积量过大，那么互联网主机对于信息参量的模糊化处理能力可能会出现一定程度的下降[12]。当前情况下，为充分发挥演化博弈模型的处理能力，可以适当缩短下级网络终端的单位访问周期，从而达到控制数据样本累积量的目的。

2　针对模糊化处理条件的大数据信息泄漏风险评估

访问控制模型的实现，还需根据演化博弈的模糊化处理条件，完成对大数据信息泄漏风险的评估，本章节针对具体评估步骤展开研究。

2.1　大数据信息泄漏行为的信任度计算

大数据信息泄漏行为信任度是基于演化博弈模型所提出的数据样本信任性考量理念。互联网主机在控制大数据信息泄漏风险访问行为时，所选取的默认对象不是任何一个信息样本，而是以演化博弈模型为标准定义的大数据样本集合体[13]。由于大数据集合体的传输受到模糊化处理条件的直接影响，所以互联网主机在计算大数据信息泄漏行为信任度时，要保证核心访问节点与具有泄露风险的大数据信息样本之间的对应关系[14]。

对于大数据信息泄漏行为信任度的计算，要求数据样本集合体定义式的取值必须属于 $[1,+\infty)$ 的数值区间。大数据样本集合体定义式为：

$$A=1+\frac{2\times W\times \iota}{\overline{\tilde{S}}\times\hat{a}-d\times\tilde{a}} \tag{7}$$

式中，ι 为基于演化博弈的大数据信息泄露风险参量取样系数，$\hat{a}$ 为大数据信息样本的风险性评级参数，$\tilde{a}$ 为大数据信息样本的泄露行为评级参数，$\overline{\tilde{S}}$ 为互联网主机对已泄露大数据信息的取样均值，d 为互联网空间中基于演化博弈的大数据信息控制阈值。

利用公式（7），可将大数据信息泄漏行为的信任度计算结果表示为：

$$D=\sum_{\kappa_1=1}^{+\infty}\sum_{\kappa_2=1}^{+\infty}f_{\kappa_1}\times\lambda_{\kappa_2}\times A^2 \tag{8}$$

式中，κ_1、κ_2 表示两个不同的互联网风险区域划定参数，且演化博弈模型规定，$\kappa_1\neq\kappa_2$ 不等式取样条件恒成立，f_{κ_1} 表示

大数据信息泄漏风险的可信任性度量值，λ_{e_0} 表示持续性信任向量。在互联网环境中，信任度取值越接近“0”，就表示大数据信息泄漏行为的风险性访问等级越高。

2.2 基于信任度的大数据信息监控器设置

设置大数据信息监控器是根据信任度条件，完成对具有泄露风险的大数据信息样本的筛选，由于控制模型对风险性访问行为的处理遵循以演化博弈原则为基础所制定的模糊化条件，所以对于监控器结构的设置也必须参考演化博弈模型。完整的大数据信息监控器部件由 zabbix 服务器、agent 客户端、访问控制节点、互联网信息终端四部分组成。其中，agent 客户端可以深入互联网信息终端内部，并在其中提取具有泄露风险的大数据信息。互联网信息终端中包含大量的信息节点，且这些节点对于大数据对象的辨识能力并不相同，所以 agent 客户端提取所得的大数据信息样本类别也并不固定[15]。agent 客户端向外输出的大数据信息样本会在 zabbix 服务器中不断累积，当其实时累积量达到既定数值标准后，访问控制节点进入连接状态，并根据演化博弈模型，完成对泄漏风险信息的模糊化注册处理。大数据信息监控器设置模型如图 2 所示。

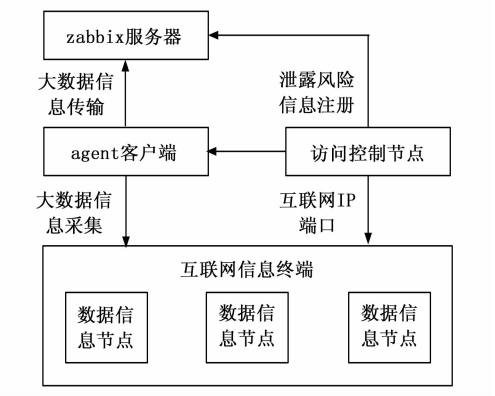

图 2 大数据信息监控器结构模型

监控器访问控制节点与互联网信息终端之间的连接借助互联网组织提供的 IP 端口，在演化博弈模型作用下，信息泄漏行为信任度计算结果始终保持定值状态，所以主机元件控制风险访问行为时，节点对象对大数据信息的提取能力始终保持稳定[16]。互联网信息终端具有完全开放的连接特征，所以主机元件在控制大数据信息泄漏的风险性访问行为时，注册、采集、传输等程序指令的传输都具有双向性。

2.3 利用监控器的信息泄漏风险评估

实现大数据信息泄露风险评估是设计访问控制模型的必要环节，由于评估对象是具有泄露风险的大数据信息对象，因此必须利用大数据信息监控器完成对评估信息参量的提取。对于大数据信息泄漏风险的评估，包含如下两个处理流程。

信任度指标更新：监控器设备只具有瞬时处理能力，评估信息泄漏风险时，为满足设备元件的瞬时处理需求，应保证信任度指标的即时性状态，对信任度指标进行更新处理[17]。

信任度指标的更新表达式为：

$$F=\left(1-\frac{g_{\max}-g_{\min}}{\mu}D\right)\times|\overline{G}| \tag{9}$$

式中，μ 为大数据信息泄露风险项的信任度更新阈值，$g_{\max}$ 为即时性访问向量的最大取值，$g_{\min}$ 为即时性访问向量的最小取值，$\overline{G}$ 为单位访问周期内的大数据信息泄露风险项取样均值。

大数据信息监控器对泄漏风险项的筛选：并不是所有大数据信息泄漏风险项都满足演化博弈模型对于信息参量访问行为的控制需求，而该项处理是按照演化博弈模型，完成对符合控制条件的大数据信息泄漏风险项的筛选[18]。

风险性筛选表达式为：

$$H=F\times\left(\frac{\tilde{\nu}}{\dot{h}+1}\right)^2 \tag{10}$$

式中，$\tilde{\nu}$ 为基于演化博弈模型的信息参量访问行为控制阈值，$\dot{h}$ 为大数据信息样本筛选特征。

大数据信息泄漏风险评估公式：

$$J=\vec{j}\left[\sqrt{\frac{1}{\bar{\omega}}}(F\times H)^2\right] \tag{11}$$

式中，$\vec{j}$ 为评估标准值，$\bar{\omega}$ 为大数据信息泄漏风险行为的访问授权参数。监控器作为大数据信息泄露风险的评估容器，因此设备元件对信息参量的承载能力，影响互联网主机对访问行为的控制作用效果。

3 面向风险评估结果的访问控制模型设计

参考上述章节推导所得大数据信息泄漏风险评估条件设计访问控制模型，需要在取样访问证据的基础上，求解访问控制阈值，并针对既定大数据信息对象，完成对信息泄漏风险访问的控制。

3.1 大数据信息的访问证据取样

访问证据是影响控制模型对大数据信息泄漏风险访问控制效果的因素。控制模型设计过程中，演化博弈模型对访问证据的取样并不局限于一种或几种数据对象，而是可以将各类相关性信息，都归为访问证据的类别中[19]。相较于其他类型的取样参量，访问证据对于大数据信息泄漏风险参量的包容性更强。在控制信息参量访问行为的过程中，访问证据取样不要求大数据信息的同源性，因此只要在监控器设备保持开放状态的情况下，互联网主机就可以根据泄露风险评估结果，实现对风险访问行为的有效控制[20]。对于大数据信息访问证据取样表达式的求解如公式（12）所示：

$$k=\sum_{-\infty}^{+\infty}\tilde{l}\times\left|\frac{J}{\theta\times L}\right|^2 \tag{12}$$

其中：$\tilde{l}$ 为监控器设备的开放性判别系数，L 为基于演化博弈模型的阈向量取值参数，θ 为大数据信息访问证据标记指征。如果大数据信息泄漏风险项的访问行为并不唯一，那么演化博弈模型在同一控制周期内，可以同时取得多个

访问证据指标。

3.2　针对访问证据的访问控制阈值计算

访问控制阈值决定了控制模型对大数据信息泄漏风险访问行为的作用能力，在访问证据取样结果保持不变的情况下，阈值计算结果越大，就表示控制模型对大数据信息泄漏风险访问行为的作用能力越强。由于访问证据取样结果并不唯一，所以控制阈值指标常表现为区间状态，且在每个数值区间内，一个阈值参数只能对应一种类型的大数据信息泄漏风险访问行为[21-22]。

对于访问控制阈值的计算参考如下表达式：

$$Z=\frac{\sum_{c=1}\vartheta_c\times|\hat{X}|^{-2}}{k} \tag{13}$$

式中，c 为值域区间内的访问证据取样系数，$\hat{X}$ 为访问证据与访问控制阈值之间的映射对应特征，ϑ_c 为阈值指标的数值约束项。阈值指标对大数据信息泄漏风险访问行为的控制作用能力不具有明显的局限性，所以只要在演化博弈模型规定的数据样本区间内完成对信息参量的取值，就可以实现对访问控制阈值指标的准确计算。

3.3　联合阈值指标的信息泄漏风险访问控制

对大数据信息泄漏风险访问的控制是根据阈值指标取值，完成对风险项参数的控制与调节。对于互联网主机而言，其在控制大数据信息泄漏风险访问行为时，参考演化博弈模型，完成对风险项参数的取样，由于阈值指标的数值水平并不会出现明显波动的变化状态，所以针对泄漏风险访问行为的控制是针对定值指标参量的控制[23-24]。

利用式（13），可将大数据信息泄漏风险访问控制表达式定义为：

$$V=\frac{1}{2}[\zeta(\dot{b}+\dot{m})+\sigma Z]^2 \tag{14}$$

其中：σ 为针对阈值指标的大数据信息泄漏风险项调节参数，$\dot{b}$ 为数据信息参量风险访问行为的波动特征，$\dot{m}$ 为数据信息参量风险访问行为的数值取样特征，ζ 为基于演化博弈模型的大数据信息泄漏风险项控制向量。基于演化博弈的大数据信息泄漏风险访问控制模型在调节风险项参数时，除了参考访问控制阈值指标的取样数值，还要求大数据信息样本在互联网空间中的传输规律必须保持一致。

4　实验分析

为了验证设计的基于演化博弈的大数据信息泄漏风险访问控制模型的有效性，采用基于演化博弈的大数据信息泄漏风险访问控制模型（所提方法）、基于 MyBatis 和 CBAC 的访问控制方法（文献［2］方法）和基于向量表征与计算的动态访问控制方法（文献［3］方法）进行对比，设计如下对比实验。

4.1　实验准备

本次实验在互联网平台中进行，开始实验前，打开数据寄存器设备，通过调节相关代码程序，完成对大数据信息泄漏风险项参数的取样，互联网数据寄存器调试代码如图 3 所示。

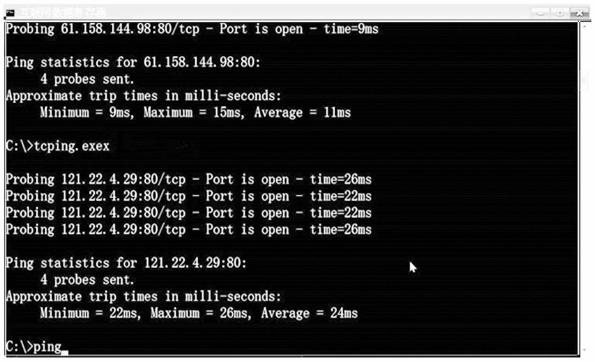

图 3　互联网实验平台设置

在互联网空间中，大数据信息泄漏风险项参数的出现具有偶发性特征，且在数据寄存器设备保持非稳定运行状态的情况下，网络主机取样所得的风险项参数并不能满足实验需求。因此，为保证实验结果的准确性，在完成互联网数据寄存器设置后，还需根据大数据信息泄漏风险项参数的取样结果，完成对信息泄露风险等级的评定。

考虑实验公平性，每完成一次大数据信息泄漏风险项参数取样后，需要将数据元件调试至实验开始前的连接状态，并根据当前情况下的泄露风险评定结果，完成对大数据信息访问连接行为的二次调试。

4.2　原理与流程

大数据信息泄漏行为是导致互联网主机所承担运行风险不断提升的主要原因，在信息泄露风险评定等级相对较高的情况下，下级网络终端可能会表现出无法访问大数据信息服务器的响应行为。本次实验通过大数据信息的瞬时泄漏量水平，来判断下级网络终端是否会出现无法访问大数据信息服务器的情况，从而分析所选用访问控制模型对大数据信息泄露风险访问行为的控制能力。

在互联网访问连接过程中，大数据信息泄漏风险项的分布曲线如图 4 所示。

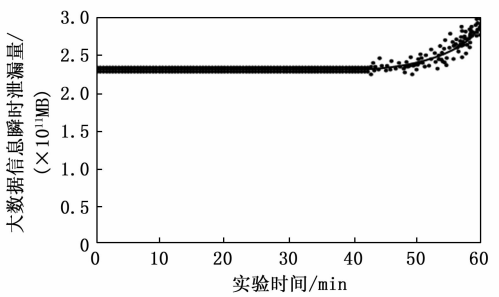

图 4　大数据信息泄漏风险项分布曲线

分析图 4 可知，当大数据信息瞬时泄漏量达到 2.3×10^{11} MB 之前，风险项参数始终保持较为均匀的分布状态，且每一个风险项参数与风险曲线之间的距离水平完全相等；当大数据信息瞬时泄漏量超过 2.3×10^{11} MB 后，风险项参数呈现较为混乱的分布状态，风险项参数与风险曲线之间

的距离水平并没有明显规律性。由此可知，2.3×10^{11} MB 为大数据信息瞬时泄漏量的临界值，当大数据信息泄漏量超过该数值时，下级网络终端会出现无法访问大数据信息服务器的情况，本次实验过程中，所选用控制模型若可将大数据信息泄漏量控制在该数值水平下，则表示该模型对大数据信息泄漏风险访问行为的控制能力较强。

本次实验的具体执行流程如下：首先，完成对大数据信息泄漏风险项参数的取样；将基于演化博弈的大数据信息泄漏风险访问控制模型的执行程序输入互联网主机中，记录该模型作用下，大数据信息瞬时泄漏量的数值水平，所得结果为实验组变量；然后，将基于 MyBatis 和 CBAC 的访问控制方法的执行程序输入互联网主机中，记录该模型作用下，大数据信息瞬时泄漏量的数值水平，所得结果为 A 对照组变量；接着，将基于向量表征与计算的动态访问控制方法的执行程序输入互联网主机中，记录该模型作用下，大数据信息瞬时泄漏量的数值水平，所得结果为 B 对照组变量；最后，统计所得变量数据，总结实验规律。

4.3 数据处理

实验组、A 对照组、B 对照组大数据信息瞬时泄漏量的具体实验数值如表 1 所示。

表 1 大数据信息瞬时泄漏量

实验时间 /min	实验组 /$\times10^{11}$ MB	A 对照组 /$\times10^{11}$ MB	B 对照组 /$\times10^{11}$ MB
10	1.0	1.0	1.0
20	1.2	1.7	1.6
30	1.4	1.9	2.0
40	1.5	2.3	2.4
50	1.8	2.5	2.7
60	2.1	2.8	3.2

分析表 1 可知，随着实验时间的延长，实验组、A 对照组和 B 对照组大数据信息瞬时泄漏量均呈现不断增大的数值变化态势，且当实验时间为 10 min 时，3 组信息瞬时泄漏量的数值水平完全相等。在整个实验过程中，实验组大数据信息瞬时泄漏量的数值上升幅度相对较慢，最大值仅能达到 2.1×10^{11} MB，并未达到临界值 2.3×10^{11} MB，与 A 对照组和 B 对照组的最大值相比，分别下降了 0.7×10^{11} MB 和 1.1×10^{11} MB。

4.4 实验结论

综合上述实验结果可知，基于演化博弈的大数据信息泄漏风险访问控制模型的应用，可使大数据信息瞬时泄漏量始终低于临界值水平，能够解决由大数据信息泄漏导致的网络主机所承担的运行风险提升的问题，可以避免网络终端出现无法访问大数据信息服务器的情况，符合实际应用需求。

5 结束语

本文设计了基于演化博弈的大数据信息泄漏风险访问控制模型，通过演化博弈的模糊化处理大数据信息参量，完成对信息泄漏风险的准确评估，根据访问证据与控制阈值的取样结果，实现对信息泄漏风险访问行为的有效控制。通过实验验证了该方法可以有效控制大数据信息的瞬时泄漏量，能够解决下级网络终端无法访问大数据信息服务器的问题，由大数据信息泄漏导致的网络主机所承担运行风险提升的行为得到了有效制止。

参考文献：

[1] 赖丹晖，罗伟峰，黄建华，等. 基于业务调用认证登录接口的电网信息防泄漏技术 [J]. 中国电力，2022，55 (8)：184-189.

[2] 叶茂林，余发江. SDBatis：基于 MyBatis 和 CBAC 的数据库应用访问控制 [J]. 武汉大学学报 (理学版)，2022，68 (1)：57-64.

[3] 王清旭，董理君，贾 伟，等. 开放式环境下基于向量表征与计算的动态访问控制 [J]. 计算机科学，2022，49 (s2)：727-733.

[4] 胡 晓，付江伟，吴珊丹. 基于演化博弈的应急物流最优仓库定位 [J]. 计算机仿真，2021，38 (11)：415-419.

[5] 熊 强，杨欣琦，李治文. 网络安全漏洞信息披露中多元参与主体行为策略演化博弈分析 [J]. 运筹与管理，2021，30 (7)：102-109.

[6] 高建杰，王永立，邵毅明. 基于终点需求可变的市域旅游客流运输均衡分配模型 [J]. 重庆交通大学学报 (自然科学版)，2023，42 (1)：99-106.

[7] 魏 娜，刘明雍. 基于贝叶斯纳什均衡的不完全信息博弈目标分配决策 [J]. 西北工业大学学报，2022，40 (4)：755-763.

[8] 雷 鹰，郑万波，魏 嵬，等. 基于概率性能感知演化博弈策略的“云+边”混合环境中任务卸载方法 [J]. 计算机应用，2021，41 (11)：3302-3308.

[9] 王文焕，郭 鹏，詹荣荣，等. 基于最短路径算法的继电保护数据模型结构及搜索优化 [J]. 电机与控制学报，2021，25 (1)：68-78.

[10] 郭 玮，谷宇航，江 南. 面向多粒度时空对象数据模型的网络电子地图生成方法 [J]. 地球信息科学学报，2022，24 (7)：1264-1274.

[11] 项兆坤，陈 婷，苏 仟，等. 面向 OLAP 数据库查询处理功能的模糊测试工具 [J]. 华东师范大学学报 (自然科学版)，2021 (5)：74-83.

[12] 王彦平，刘 航，李 洋，等. 基于栅格投影的地基合成孔径雷达三维地形匹配俯仰角模糊处理方法 [J]. 电波科学学报，2021，36 (4)：571-578.

[13] 翟 峰，冯 云，程 凯，等. 基于信息熵的多源电力物联终端设备信任度评价方法 [J]. 中国电力，2022，55 (5)：158-165.

[14] 宋玉龙，马文明，刘彤彤. 融合用户信任度的概率矩阵分解群组推荐算法 [J]. 计算机工程，2022，48 (1)：105-111.

[15] 周 正，胡 毅，杨 巍，等. 多源异构数控设备监控服务器的研究与实现 [J]. 小型微型计算机系统，2021，42 (11)：2382-2387.

(下转第 151 页)