

引用格式:胡悦,林果园,蔚国莹. 基于 LSTM-GRBM 的云虚拟机异常检测[J]. 微电子学与计算机, 2021, 38(4): 46-51. [HU Y, LIN G Y, WEI G Y. Anomaly detection of cloud virtual machine based on LSTM-GRBM[J]. Microelectronics & Computer, 2021, 38(4): 46-51.]

基于 LSTM-GRBM 的云虚拟机异常检测

胡悦^{1,2}, 林果园^{1,2,3}, 蔚国莹^{1,2}

(1 中国矿业大学 计算机科学与技术学院, 江苏 徐州 221116; 2 矿山数字化教育部工程研究中心, 江苏 徐州 221116; 3 南京大学 新软件技术国家重点实验室, 江苏 南京 210093)

摘 要: 本文提出了一种对云虚拟机进行异常检测的模型 LsGrbmAd. 该模型首先通过长短期记忆网络(LSTM)捕获云虚拟机性能指标的时序特征, 同时利用 Dropout 以防止数据过拟合; 其次利用高斯玻尔兹曼机(GBRM)得出自由能; 最后利用得出的自由能与训练阶段得到的参数基准模型进行对比, 判断云虚拟机是否出现异常. 实验表明该模型能够对云虚拟机进行异常检测, 且准确率有较大的提升.

关键词: 异常检测; 云虚拟机; 长短期记忆网络; 高斯玻尔兹曼机; 云服务

中图分类号: TP306+.3 **文献标识码:** A **文章编号:** 1000-7180(2021)04-0046-06

Anomaly detection of cloud virtual machine based on LSTM-GRBM

HU Yue^{1,2}, LIN Guo-yuan^{1,2,3}, Wei Guo-ying^{1,2}

(1 School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, Jiangsu China; 2 Digitization of Mine, Engineering Research Center of Ministry of Education of China, Xuzhou 221116, Jiangsu China; 3 State Key Laboratory for Novel Software Technology hosted at Nanjing University, Nanjing 210093, Jiangsu China)

Abstract: A model of Long Short Term Memory and Gaussian Boltzmann Machine Anomaly Detection(LsGrbmAd) is proposed in this paper. Firstly, the model captures the timing characteristics of cloud virtual machine performance indicators through long short term memory LSTM), and uses Dropout to prevent data overfitting. Secondly, the free energy is obtained by using The Gaussian Boltzmann machine (GBRM). Finally, the free energy obtained is compared with the parameter benchmark model obtained in the training stage to judge whether there are abnormalities in the cloud virtual machine. The experiment shows that the model can detect the abnormality of the cloud virtual machine, and the accuracy is improved greatly.

Key words: anomaly detection; virtual machine; long short term memory; Gaussian restricted Boltzmann machine; cloud service

1 引言

虚拟机共用云平台上的硬件资源, 配置不当会引发资源竞争等问题, 使虚拟机在运行过程中出现

异常, 导致性能下降甚至宕机, 影响云服务的正常运行, 造成各种损失. 针对上述情况, 需要对云虚拟机进行异常检测, 实现对云平台的监控, 提升云服务可靠性. 本文提出了一种组合学习模型, 将 LSTM、

Dropout 和 GRBM 整合到一个端到端的深度学习网络 LsGrbmAd. 该模型是数据驱动的,通过不断调整网络中的参数,可以有效地捕获到异常信息,克服传统无监督学习方法的局限性,且在处理云虚拟机性能指标数据时,比标准的无监督算法高效得多.

2 LsGrbmAd 模型架构

针对云虚拟机的性能指标,提出云虚拟机异常

检测模型 LsGrbmAd,其模型架构如图 1 所示. LSTM 和 GRBM 是 LsGrbmAd 的两大核心组件. 通过描述 LsGrbmAd 如何训练 LSTM 以及 GRBM,计算云虚拟机正常行为时的自由能,获得相关的参数基准模型,分析 LsGrbmAd 如何选择最佳的基准模型,通过比较云虚拟机性能指标数据的自由能和参数基准模型来展示 LsGrbmAd 如何检测异常.

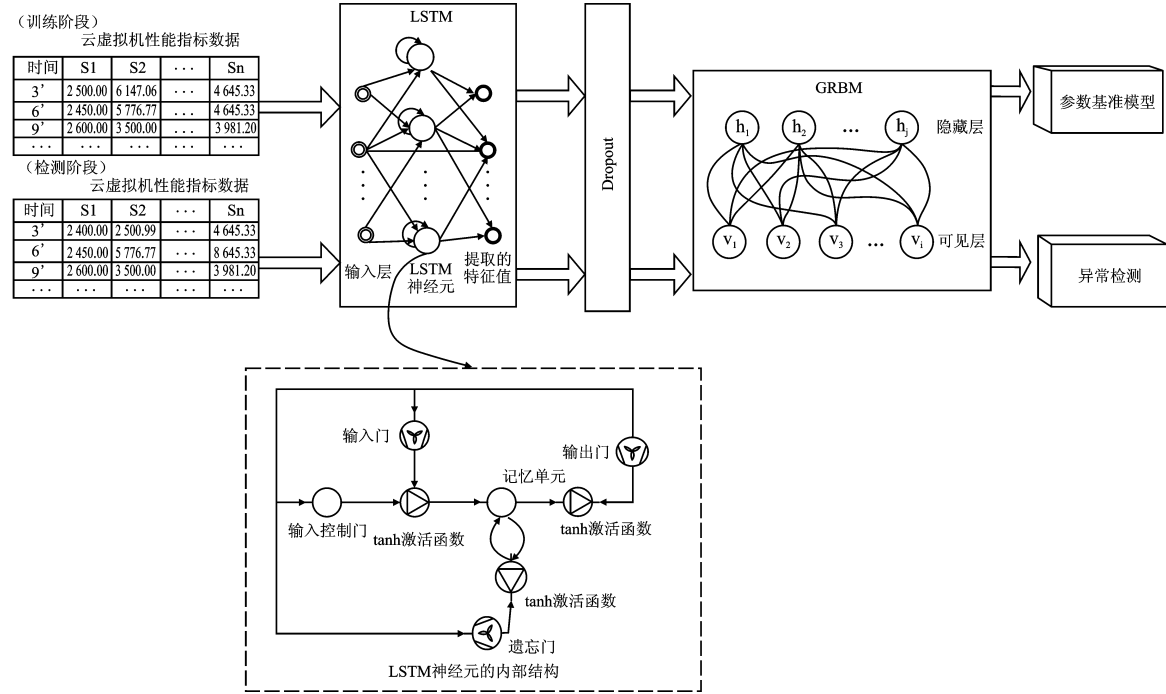


图 1 LsGrbmAd 模型架构图

2.1 核心组件

LSTM 能够处理长时间依赖性的云虚拟机性能指标数据,学习性能指标数据的特征向量,不仅能较好地处理时序数据集,还能缓解梯度消失等问题. 重复的 LSTM 单元可以记录每一个时间点采样的云虚拟机性能指标向量,代表了当前云虚拟机的状态. 输入门控制云虚拟机性能指标信息的流入程度,遗忘门控制云虚拟机性能指标信息的保留程度,输出门控制哪些性能指标信息可以激活 LSTM 单元. LSTM 计算得到细胞信息和隐藏状态向量,通过线性变换与非线性变换,将云虚拟机性能指标映射到更有效的特征空间,得到表示异常检测的关键特征. 下述公式在数学上抽象了该过程,相关公式符号解释如表 1 所示.

$$f_t = \sigma_a(\omega_f x_t + v_f h_{t-1} + b_f)$$
$$i_t = \sigma_a(\omega_i \chi_t + v_i h_{t-1} + b_i)$$
$$o_t = \sigma_a(\omega_o \chi_t + v_o h_{t-1} + b_o)$$

(1)

(2)

(3)

$$\tilde{c}_t = \sigma_b(\omega_c \chi_t + v_c h_{t-1} + b_c)$$
$$c_t = f_t \circ c_{t-1} + i_t \circ \tilde{c}_t$$
$$h_t = o_t \circ \sigma_b(c_t)$$

(4)

(5)

(6)

表 1 符号定义

符号	定义
χ_t	将云虚拟机性能指标向量输入至 LSTM 单元
f_t	遗忘门激活向量
i_t	输入门激活向量
o_t	输出门激活向量
$\tilde{c}_t$	候选细胞信息
c_t	新的细胞信息
h_t	隐藏状态向量或 LSTM 单元的输出向量
ω, v, b	训练阶段需学习的权重矩阵和偏倚向量参数
$\circ$	两个同样维度的向量每个元素分别相乘
$\sigma_a(*)$	标准 sigmoid 函数
$\sigma_b(*)$	tanh 激活函数

受限玻尔兹曼机 (restricted Boltzmann machines, RBM) 是由跨层对称连接且同一层内节点之间没有连接的随机神经网络^[1]. Montufar 等人^[2]和 Le Roux 等人^[3]表明 RBM 计算一个随机变量概率分布近似值. 因此, 适合对云虚拟机性能指标以时间序列形式进行建模. 传统的 RBM 处理二值化数据集, 若对云虚拟机性能指标数据集进行二值化处理, 数据中包含的一些重要的信息将会丢失. 对实值云虚拟机关键性能指标的建模, RBM 表现的不够理想. GRBM 是 RBM 的直接扩展, 它可以用来处理实值数据. 因此, 使用 GRBM 来处理实值云虚拟机关键性能指标集合.

2.2 工作原理与分析

从云虚拟机中获取的性能指标数据, 存在数据噪声. 因此, 需要找出对云虚拟机异常状态贡献度较高的指标, 获得更为准确的模型. 首先, 将获取到的性能指标数据输入至 LSTM 中, LSTM 可以在 5 分钟时间窗口内多次采样云虚拟机性能指标数据, 用 LSTM 提取的时序数据特征来代替直接向 GRBM 中每隔 5 分钟取一个数据点, 这样采集到的数据特征更密集且具备时序特征, 使得在一个时间窗口内的数据包含了更多的时间点的信息. 相比于直接使用一个时间点的信息特征更加丰富. 如果不使用 LSTM, 在 5 分钟采样 10 次云虚拟机性能指标数据, GRBM 的计算量会大幅度增加且训练代价较高. 因此, 使用 LSTM 来处理一个时间窗口内的数据得出一组时序特征向量.

同时, 为了对云虚拟机性能指标数据进行高度智能化, 防止训练数据过拟合现象, 引入 Dropout. Dropout 每个隐藏单元 h_i 以概率为 ρ 被保留, 以概率为 $q=1-\rho$ 被丢弃出网络, 充分利用 LSTM 所获得的关于输入的云虚拟机性能指标数据分布的所有知识, 模型的泛化性更强.

最后, 由 LSTM 对云虚拟机进行特征提取的性能指标数据直接输入至 GRBM. LSTM 提取的性能指标特征初始化 GRBM 的可见层, 之后进行吉布斯采样, 包含三个步骤. 首先, 根据式(7)计算隐藏层节点的概率分布, 每个隐藏层节点的概率若大于阈值则激活该节点, 取值为 1, 否则为 0. 其次, 更新可见层节点的值. 可见层使用式(8)计算, 可得到可见层的概率分布, 可见层节点是高斯单元, 其值通过一个高斯分布生成, 均值为激活单元的均值, 方差需要手动设定. 最后, 再根据式(7)更新隐藏层节点概率分布, 并依此概率对节点值进行激活. 设置隐藏层单元

数量等于可见层单元数量, 进一步学习检测异常的关键特征, 通过可见层与隐藏层的节点值可计算得到云虚拟机性能指标的能量. GRBM 的能量函数为式(9)所示, GRBM 通过对能量函数进行变化得到自由能 $G(v)$, 更为有效的近似于对数似然函数, 在训练过程中最小化输入的自由能来构建较好的模型, 如式(10)所示.

$$P(h_j = 1 | v) = \text{sigmoid}(\sum_i \frac{v_i}{\sigma_i} \omega_{ij} + c_j) \quad (7)$$

$$P(v_i | h) = \frac{1}{\sigma_i \sqrt{2\pi}} \exp(-\frac{1}{2\sigma_i^2}(v_i - b_i - \sigma_i \sum_j \omega_{ij} h_j))^2 \quad (8)$$

$$E(v, h; \tau) = -\sum_{i=1}^F \sum_{j=1}^H \frac{v_i}{\sigma_i} \omega_{ij} h_j - \sum_{j=1}^H c_j h_j + \sum_{i=1}^F \frac{(v_i - b_i)^2}{2\sigma_i^2} \quad (9)$$

$$G(v) = \log e^{-E(v, h; \tau)} \quad (10)$$

式中, F 个可见节点 $v \in R^F$ 表示获取到的云虚拟机关键性能指标值; H 个隐藏节点 $h \in R^H$ 表示随机变量; $\tau = \{\omega, b, c\}$ 是 GRBM 模型中的网络权值; ω, b, c 分别为边的权值矩阵, 可见层的偏倚系数和隐藏层的偏倚系数; σ_i^2 表示第 i 个可见层单元的方差项; σ_i 为协方差.

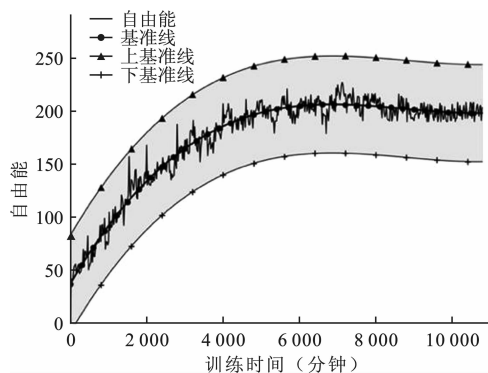
2.3 参数基准模型

参数基准模型是一个关于时间的含有参数的基准模型, 依赖于训练阶段得出的自由能的标准差 $\sigma(G_{Tr})$ 和一个参数 $\gamma \in N$. 首先, 由 LSTM 和 GRBM 计算训练阶段的自由能 G_{Tr} , 由 $Trendline(G_{Tr})$ 拟合随时间变化的自由能的基准线, 再由公式(11) 和公式(12) 分别界定了该参数基准模型的上基准线和下基准线, 云虚拟机正常状态的自由能位于该上下基准线之间.

$$BaseLine_{top} = Trendline(G_{Tr}) + \gamma \sigma(G_{Tr}) \quad (11)$$

$$BaseLine_{bottom} = Trendline(G_{Tr}) - \gamma \sigma(G_{Tr}) \quad (12)$$

$\sigma(G_{Tr})$ 量化了参数基准模型的变化范围, 参数 γ 定义出基准模型上下基准线与基准线之间的距离. γ 越大, 基准模型的自由能的变化范围越大, 这些范围内的值都表明云虚拟机的行为是正常的, 基准模型的容忍度就越高. γ 越小, 基准模型的自由能的变化范围越小, 基准模型的容忍度就越低. 具体 γ 取值情况, 实验阶段加以描述. 通过取一周的云虚拟机性能指标数据集作为训练, 获得参数 $\gamma = 3$ 的基准模型, 如图 2 所示.

图2 参数 $\gamma = 3$ 的基准模型

2.4 异常检测

在检测阶段,通过人工注入异常的方式获得含有异常的云虚拟机的性能指标数据,与训练阶段一样,由 LSTM 和 GRBM 得出自由能 G_{Tx} 。异常的云虚拟机,相应的性能指标会受到影响,结果反映在它们的 G_{Tx} 值上,若该值不在参数基准模型中的上下基准线范围内,判定云虚拟机出现异常。图 3 显示了异常检测阶段,云虚拟机自由能与参数 $\gamma = 3$ 的基准模型的对比。

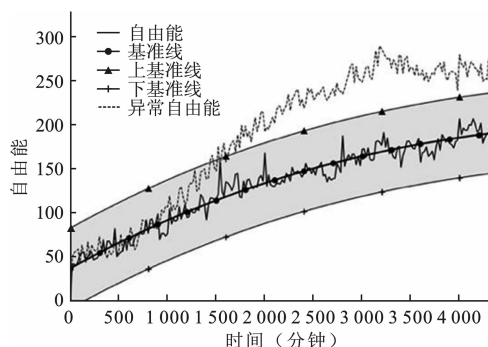


图3 云虚拟机异常检测

3 实验

3.1 实验环境

为了测试 LsGrbmAd 模型在云虚拟机异常检测中的应用效果,利用实验室自主搭建的基于 OpenStack 的弹性云计算平台进行研究和测试,使用戴尔服务器 1 台,联想、宏基和惠普主机各 4 台。戴尔服务器部署 80 台虚拟机,每台联想和惠普主机各配置 4 台虚拟机,每台宏基主机配置 8 台虚拟机,一共可达 144 台虚拟机。其中,虚拟机采用统一配置,CPU 算力 1 GHz,内存 1 GB,存储 20 GB,网络为默认配置,虚拟机部署 Ubuntu18.04 操作系统,具体如图 4 所示。

3.2 实验设置

本文使用 TensorFlow 和 Keras 深度学习框架

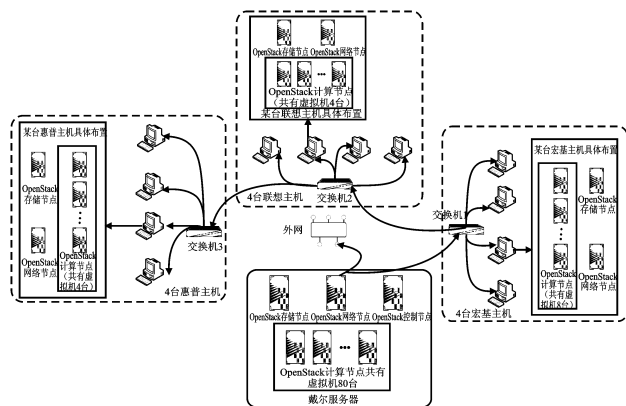


图4 云平台网络拓扑图

进行建模与训练,使用图形处理器(GPU)加快模型学习速率,提高计算机性能。模型将 LSTM 的循环次数设置为时间窗口大小,每一次的批处理数为 128, LSTM 隐藏层维度设置为 64,使用 Dropout 层设置 Dropout 的比例为 0.2。GRBM 的可见层单元数目与隐藏层单元数目一致,设置为 64,模型的学习率为 0.001,目标函数见 GRBM 公式(10)所示。使用 Adam 方法优化目标函数,超参选择如下,学习率为 0.001, $\beta_1 = 0.9$, $\beta_2 = 0.999$, $\epsilon = 10^{-8}$, decay = 0.0。本文共监测 10 天的数据,前 7 天的数据作为训练集数据,后 3 天通过手动异常注入的方式实时获取异常数据作为测试集数据集。

3.3 评价指标

为更准确的评价模型 LsGrbmAd 的性能,本实验采用召回率(真正类率)、精确率、误报率、F1 和正确率来评价检测结果的好坏。召回率 R_{AD} 是当云虚拟机出现异常状态时,能被正确识别出异常的概率,与召回率公式相同的真正类率 TPR_{AD} 表示被检测的所有云虚拟机中,真实状态是正常的云虚拟机的百分比。精确率 P_{AD} 是在所有被检测出是异常状态的云虚拟机中真正的异常状态的百分比。大量实验表示,召回率与精确率是负相关的。因此,使用 F1 来表示召回率与精确率的调和平均值。 FPR_{AD} 表示真实状态是正常的云虚拟机被检测为异常的虚拟机,即误报率。 $Accuracy_{AD}$ 称为正确率,即所有检测的结果与真实状态一致的云虚拟机占有所有被测云虚拟机的比率。

3.4 实验结果

3.4.1 参数基准模型中参数的选择

云虚拟机异常检测的实验中,为了得出更好的参数基准模型,通过 FPR_{AD} 、 TPR_{AD} 和 $Accuracy_{AD}$ 3 种评价指标来获取最佳参数 γ 值,依次取 γ 值为 1、

2、3 和 4,结果如图 5 所示。

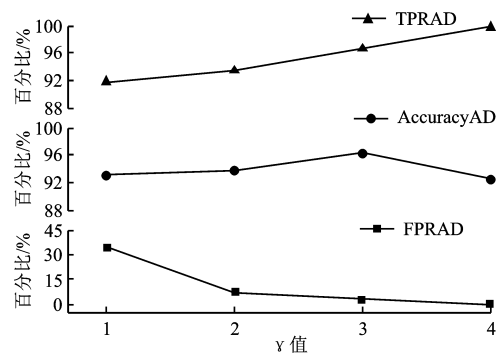


图 5 4 种参数的误报率、正确率和真正类率对比

参数 γ 值越大,表明异常检测阶段中判定结果是正常的虚拟机的概率就越大.因此参数 γ 值越大, FPR_{AD} 越低, TPR_{AD} 越来越大.当参数 γ 值为 4 时,得出 $FPR_{AD} = 0$, $TPR_{AD} = 1$.但是,此时由于 γ 过大,可能在异常检测时测试结果将所有的云虚拟机全都判定为正常,而异常的云虚拟机是小部分事件,所以 γ 取值为 4, $Accuracy_{AD}$ 是四个取值中最低的一个但还是可达 0.925.但是当 γ 为 3 时,正确率最高,可达 0.963, FPR_{AD} 值为 0.026, FPR_{AD} 值为 0.966.综合实验结果分析可以得出,在该云虚拟机异常检测实验中,最终获取参数 γ 为 3 的基准模型.

3.4.2 实验结果及分析

为了验证 LsGrbmAd 模型对云虚拟机异常检测性能的影响,本文采用文献[5]提出的常规 LOF 云虚拟机异常检测机制作为对比模型,同时对比模型还选择 LSTM 与一个全连接层组成的异常检测模型,以及云虚拟机性能指标进行处理的 GRBM 异常检测机制,和本文对性能指标进行特征提取的 LsGrbmAd 4 种异常检测机制进行对比,具体实验结果如表 2 所示.

表 2 4 种异常检测机制对异常检测性能的影响

异常检测机制	FPR_{AD}	R_{AD}	P_{AD}	$F1$	$Accuracy_{AD}$	平均时间(s)
LOF	0.273	0.892	0.931	0.911	0.925	0.230
LSTM	0.102	0.915	0.944	0.928	0.947	0.008
GRBM	0.073	0.931	0.974	0.952	0.954	0.116
LsGrbmAd	0.026	0.966	0.982	0.974	0.963	0.124

本文提出的 LsGrbmAd 充分考虑了云虚拟机的时序特征.与其他三种机制相比,平均时间没有明显优势,但仍在可接受范围内;而对云虚拟机进行异常检测时,明显将误报率降低至 0.026,召回率提升至 0.966,精确率提高至 0.982, $F1$ 为 0.974,正确

率提升至 0.963.

4 结束语

由于云环境具有高动态和高复杂两大特性,对云虚拟机异常检测算法的实时性、非线性分类能力以及高维数据的容忍性提出了更高要求.本文综合运用 LSTM 和 GRBM 提出了 LsGrbmAd 模型对云虚拟机进行异常检测,经过 LSTM 获取的数据点特征信息更加丰富,再通过 GRBM 获取自由能与基准模型进行比较,从而判断云虚拟机是否处于异常状态.通过计算不同的 γ 值,提出了 $\gamma=3$ 的最佳参数基准模型,并与其他三种异常检测机制对比,实验证明本文提出的 LsGrbmAd 模型对提高云虚拟机异常检测的准确率、 $F1$ 以及正确率具有明显优势和应用潜力.

参考文献:

[1] 张健,丁世飞,张楠,等.受限玻尔兹曼机研究综述[J].软件学报,2019,30(7):2073—2090. DOI: 10.13328/j.cnki.jos.005840.
ZHANG J, DING S F, ZHANG N, et al. Restricted Boltzmann machines: a review[J]. Journal of Software, 2019, 30(7): 2073-2090. DOI: 10.13328/j.cnki.jos.005840.

[2] MONTUFAR G, AY N. Refinements of universal approximation results for deep belief networks and restricted Boltzmann machines[J]. Neural Computation, 2011, 23(5): 1306-1319. DOI: 10.1162/NECO_a_00113.

[3] LE ROUX N, BENGIO Y. Representational power of restricted Boltzmann machines and deep belief networks[J]. Neural Computation, 2008, 20(6): 1631-1649. DOI: 10.1162/neco.2008.04-07-510.

[4] 叶青,黄强,聂斌,等.一种自适应的高维离群点识别方法[J].《广西师范大学学报》(自然科学版),2020,38(2):107-114. DOI: 10.16088/j.issn.1001-6600.2020.02.012.
YE Q, HUANG Q, NIE B, et al. An adaptive high-dimensional outlier recognition method[J]. Journal of Guangxi Normal University (Natural Science Edition), 2020, 38(2): 107-114. DOI: 10.16088/j.issn.1001-6600.2020.02.012.

[5] 权鹏宇.基于上下文的虚拟机异常检测研究[D].昆明:昆明理工大学,2018.
QUAN P Y. A research on virtual machine anomaly detection based on context[D]. Kunming: Kunming University of Science and Technology, 2018.

作者简介:

胡悦女,(1996-),硕士研究生.研究方向为云计算安全.
E-mail:hy_2750637032@163.com.

林果园男,(1975-),博士,副教授.研究方向为云计算,信息安全.
蔚国莹女,(1995-),硕士研究生.研究方向为信息安全.

(上接第 45 页)

作者简介:

李众男,(1974-),博士,副教授.研究方向为机器学习、软件工程等.
白瑞君(通讯作者)男,(1992-),硕士.研究方向为深度学习、计算机视觉. E-mail:1066193265@qq.com.

洪军男,(1979-),博士,讲师.研究方向为云计算安全等.
李亚伦男,(1994-),硕士.研究方向为深度学习.
王高男,(1973-),博士,教授.研究方向为图像处理等.
杨剑男,(1979-),博士,讲师.研究方向为计算机视觉及人工智能等.