

基于深度学习和信任度量的云平台 自适应恶意攻击检测与响应算法

王东岳,刘浩[†]

(黑龙江省气象数据中心,黑龙江 哈尔滨 150000)

摘要:由于提取的云平台数据特征与异常行为相关性不高,云平台自适应恶意攻击检测效果不佳。因此,设计了基于深度学习和信任度量的云平台自适应恶意攻击检测与响应算法。利用传感器采集云平台数据,并对其进行平滑计算和规范化处理,再对其进行聚类分析,在深度学习网络的作用下,提取出云平台运行数据的多个特征,并计算其信任度值,通过计算自适应控制函数,构建恶意攻击检测模型,将检测结果作为基础,计算恶意攻击带来的风险值,由此设计恶意攻击响应机制。以某云平台为实验对象的测试结果表明该算法在实际应用中检出率较高,检测效果较好。

关键词:深度学习;信任度量;云平台;恶意攻击;攻击响应;攻击检测算法;算法设计

中图分类号:G642

文献标识码:A

Adaptive Malicious Attack Detection and Response Algorithm for Cloud Platform Based on Deep Learning and Trust Measurement

WANG Dongyue, LIU Hao[†]

(The Meteorology Data Center of Heilongjiang, Haerbin, Heilongjiang 150000, China)

Abstract: Due to the low correlation between the extracted cloud platform data features and abnormal behavior, the adaptive malicious attack detection effect of the cloud platform is poor. Therefore, a cloud platform adaptive malicious attack detection and response algorithm based on deep learning and trust measurement was designed. Utilizing sensors to collect cloud platform data, smoothing and normalizing it, and then performing cluster analysis on it. Under the influence of deep learning networks, multiple features of cloud platform operation data are extracted, and their trust values are calculated. By calculating adaptive control functions, a malicious attack detection model is constructed, and the detection results are used as the basis to calculate the risk value brought by malicious attacks, design a malicious attack response mechanism based on this. The test results show that, taking a certain cloud platform as the experimental object, the algorithm has a high detection rate and good detection effect in practical applications.

Key words: deep learning; trust measurement; cloud platform; malicious attacks; attack response; attack detection algorithm; algorithm design

随着云计算技术的快速发展,云平台在各个领域得到了广泛应用,成为数据存储和处理的重要载体。然而,云平台的安全问题也日益突出,恶意攻击事件频发,对用户的数据安全和隐私带来了严重威胁。传统的基于规则和签名的检测方法在面对复杂多变的恶意攻击时,往往存在误报率高、漏报严重等

问题。因此,研究一种自适应的恶意攻击检测与响应算法,对于提高云平台的安全性和可靠性具有重要的实际意义。因此,在上述背景下,不少研究学者针对攻击检测方法展开了研究,并提出了自己的想法。

文献[1]对物联网中收集的大量原始数据进

行清洗、去噪和特征提取,在聚类分析的作用下,将相似的数据点归为一类,并识别出其中的异常数据点,再对异常数据点进行分类,计算对应的特征阈值,判断该异常数据特征是否为恶意攻击特征,由此实现对恶意攻击的检测。该方法通过特征提取和异常检测,能够准确地识别出异常数据,降低误报率,但其对大规模数据的处理能力有限,检测效率较低。文献[2]利用传感网络中的传感器节点采集网络中的能耗数据,并计算每个节点的信任值,由此识别出其中异常数据节点,再利用分类器对其进行进一步分类,检测出其中的克隆攻击。该方法能够在大数据集上快速地进行克隆攻击检测,提高了检测效率,但其在检测过程中需要大量的计算资源,检测成本较高。文献[3]对收集的网络流量数据进行清洗,在混合深度神经网络的作用下,提取出网络流量数据的空间特征和时间序列特征,由此构建对应的攻击检测模型,对网络流量数据中的 DoS 攻击进行检测。该方法可以实时地检测 DoS 攻击,有效应对对低速率的 DoS 攻击,但其在检测过程中,由于对用户隐私保护性不够,导致出现用户隐私泄露的可能。文献[4]利用监控系统实时采集电池储能系统的运行数据,并消除采集数据中的异常值和荣誉值,利用机器学习算法,构建正常行为模型,并将正常行为模型和实时数据进行对比,检测出其中的异常行为,再利用分类器进行对其进行分类,确定异常行为的类别。该方法能够实时监测电池储能系统的运行状态,及时发现并响应网络攻击,有效降低损失,但其在检测过程中,无法实时更新正常行为模型,导致检测结果存在一定误差。

在以往研究的基础上,本文设计了基于深度和信任度量的云平台自适应恶意攻击检测与响应算法。利用传感器采集大量的云平台运行数据,并对数据进行聚类分析,在深度学习和信任度量的支持下,构建云平台恶意攻击检测模型,并设计相应的云平台恶意攻击响应机制。本算法弥补了传统检测算法的不足,提高了云平台对未知恶意攻击的检测准确率和响应速度,还结合深度学习和信任度量技术,实现了对云平台中数据流量的实时监测和分析。同时,通过对数据的来源、行为和属性进行综合分析,提高了数据信任度量结果的准确性和可靠性,为云平台的安全防护提供了一种新的思路和方法,有助于推动云计算技术的安全应用和发展。

1 云平台自适应恶意攻击检测与响应算法设计

1.1 云平台运行数据聚类分析

云平台运行数据种类繁多,包括但不限于云平

台上各种软件资源的运行状态、硬件资源的资源占用情况、网络流量数据等。利用传感器采集云平台数据,并将采集的数据汇总到计算机中^[5-6]。为提高云平台运行数据的质量,对其进行平滑计算,剔除运行数据中的干扰因素。其平滑计算的具体过程如下所示:

$$y(n) = \begin{cases} \sum_{k=-\infty}^{+\infty} x[k]h[n-k] \\ \int_{-\infty}^{+\infty} x(k)h(t-k)dk \end{cases} \quad (1)$$

式中, $y(n)$ 表示云平台运行数据平滑计算的结果, $x[k]$ 表示采集的云平台运行数据中的离散数据, $h[n-k]$ 表示数据的平滑响应值, $x(k)$ 表示采集的云平台运行数据中的连续型数据^[7], $h(t-k)$ 表示连续型数据的平滑响应值。通过上述公式,完成对云平台运行数据的处理,提高数据的质量,对数据进行规范化处理,减小后续计算过程中的计算压力。其数据规范化处理的具体过程如下所示^[8]:

$$y'(n) = \frac{y(n) - y_{\min}(n)}{y_{\max}(n) - y_{\min}(n)} \quad (2)$$

式中, $y'(n)$ 表示云平台运行数据的规范化处理结果, $y_{\min}(n)$ 表示采集的云平台运行数据最小值, $y_{\max}(n)$ 表示采集的云平台运行数据最大值。通过上述公式,完成对云平台运行数据的规范化处理。对云平台运行数据进行聚类分析。在聚类分析的过程中,需要先计算不同数据点之间的距离,确定对应的聚类中心,再将所有的数据点进行分配,并计算分配结果与实际聚类中心之间的距离,如此循环往复,直到最终的聚类中心和预设的聚类中心重合^[9-11]。在上述过程中,云平台运行数据的聚类结果如下所示:

$$\begin{cases} d(x,y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \dots + (x_i - y_i)^2} \\ c = \arg \min \sum_{i=1}^N d(x_k, y_i) \end{cases} \quad (3)$$

式中, $d(x,y)$ 表示不同数据点 x 和 y 之间的距离度量, c 表示云平台运行数据的聚类结果, $d(x_k, y_i)$ 表示云平台运行数据点与聚类中心之间的距离。通过上述公式,完成对云平台运行数据的聚类分析,为后续构建攻击检测模型奠定基础。

1.2 基于深度学习和信任度量的恶意攻击检测模型构建

将上述聚类分析的结果作为基础,在深度学习和信任度量的作用下,构建恶意攻击检测模型。在构建攻击检测模型的过程中,先提取聚类后的云平台运行数据特征,在深度学习的作用下,对提取的特征进行分类。深度学习作为一种机器学习算法,能

够自动提取输入数据的层次特征,并将提取的特征进行选择和优化^[12]。其特征提取流程如图 1 所示。

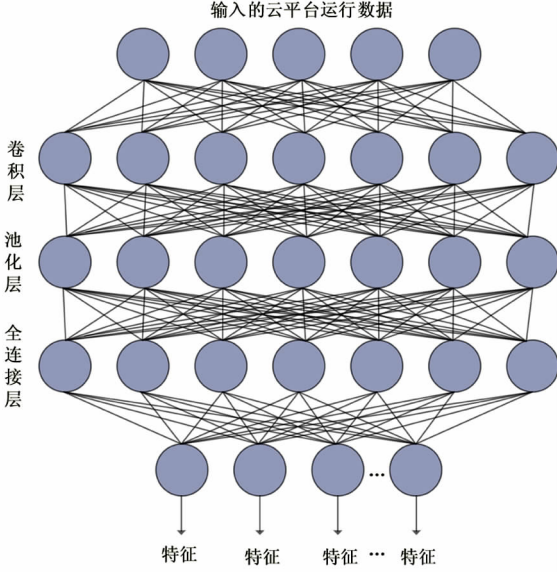


图 1 基于深度学习的云平台运行数据特征提取流程

如图 1 所示,在上述云平台数据特征提取的过程中,利用深度学习网络,先对运行数据进行卷积操作,初步提取云平台运行数据的特征,在池化层中,对提取的数据特征进行降维,将降维结果作为基础,通过全连接层,提取出相关性较高的特征。

通过计算特征的激励函数,提取出与云平台运行异常相关性较高的特征,由此完成对云平台运行数据的多个特征提取^[13]。将上述提取结果作为基础,在信任度量机制的作用下,计算不同运行数据的信任值。其具体计算过程如下所示:

$$\lambda_i = \alpha \times S_i + \beta \times B_i + \gamma \times C_i \quad (4)$$

式中, λ_i 表示计算的不同运行数据的信任值, S_i 表示运行数据特征的稳定性, B_i 表示运行数据的行为特征值, C_i 表示运行数据的贡献值, α 、 β 、 γ 分别表示对应的权重参数。根据上述计算结果,分析云平台运行数据的行为特征和历史表现。

结合上述提取的运行数据特征,通过云平台自适应控制函数,对当前云平台异常行为进行判断,判断其是否为恶意攻击^[14]。在上述过程中,构建的恶意攻击检测模型具体如下所示:

$$\left\{ \begin{array}{l} \xi_i = \frac{\sum_{i=1}^n u_i \cdot \lambda_i}{J(w, b_{ik}, n)} - \frac{1}{2} \sum_{i=1}^n \alpha_i \beta_i \varphi \\ J(w, b_{ik}, n) = \frac{1}{2} w - \sum_{i=1}^n b_{ik} [y_i (w b_{ik} + n) - 1] \\ \varphi = \frac{1}{2} \mathbf{B}^T \mathbf{B} + \tau \sum_{i=1}^n \frac{\alpha_i \beta_i}{u_i} \end{array} \right. \quad (5)$$

式中, ξ_i 表示构建的恶意攻击检测模型, u_i 表示提取的云平台运行数据特征的特征值, $J()$ 表示自适应控制函数, w 表示提取数据特征的特征分量, b_{ik} 表示不同特征之间的差异度, n 表示提取的云平台数据特征数量, α_i 表示恶意攻击特征参数, β_i 表示云平台的模糊特征参数, y_i 表示特征之间的关联系数, φ 表示云平台运行数据的分布算子, $\mathbf{B}$ 表示特征矩阵, τ 表示特征寻优参数。通过上述公式,完成对恶意攻击检测模型的构建。利用该攻击检测模型,对云平台运行过程中出现的恶意攻击进行检测,为后续设计云平台恶意攻击响应机制提供检测结果。

1.3 云平台自适应恶意攻击响应机制设计

根据恶意攻击检测模型的检测结果,设计云平台自适应恶意攻击响应机制。在设计响应机制的过程中,根据云平台的实际情况,并对已知的恶意攻击行为进行分析,判断恶意攻击对云平台运行的影响程度,计算恶意攻击的风险值。其具体计算过程如下所示:

$$k_f = \kappa \times \mathfrak{R} \times \Gamma \quad (6)$$

式中, k_f 表示恶意攻击的风险值, κ 表示恶意攻击带来的后果, $\mathfrak{R}$ 表示恶意攻击被发现的概率, Γ 表示恶意攻击出现的可能性。通过上述公式,完成对恶意攻击带来的风险的计算。将该计算结果作为基础,实现对恶意攻击的自动响应。其自动响应的部分代码如图 2 所示。

```
import numpy as np
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score
features = [
]
labels = [
    0, 0, 0, 1, 1, 0, 1, 1, 0, 0,
]
X_train, X_test, y_train, y_test = train_test_split(features, labels,
                                                    test_size=0.2, random_state=42)
clf = RandomForestClassifier(n_estimators=100)
clf.fit(X_train, y_train)
y_pred = clf.predict(X_test)
accuracy = accuracy_score(y_test, y_pred)
print("Accuracy:", accuracy)
def respond_to_malicious_activity(data):
    prediction = clf.predict([data])[0]
    if prediction == 1:
        print("Detected malicious activity:", data)
        return False
    else:
        return True
```

图 2 恶意攻击自动响应的部分代码

如图 2 所示,将恶意攻击检测模型的检测结果作为基础,对其进行风险值的计算,由此触发相应的响应机制。在该响应机制中,针对出现的恶意攻击,上述算法能够快速切断恶意攻击的路径,减轻

恶意攻击的影响^[15]。同时,还能将应对恶意攻击中的各种信息传输到云平台,并对这些信息进行不断分析,由此保证防御效果。

2 实验测试

将所提出的方法与现有的算法进行对比,提高实验结果的真实性和可靠性。本文设计的基于深度学习和信任度量的云平台自适应恶意攻击检测与响应算法为算法 1,基于数据挖掘与孤立森林算法的恶意攻击检测算法为算法 2,基于聚类分析与改进蚁群算法的恶意攻击检测与响应算法为算法 3。为对比上述三种算法在实际应用中效果,设计的实验具体如下。

2.1 实验准备

为验证本文设计的基于深度学习和信任度量的云平台自适应恶意攻击检测与响应算法在实际应用中的效果,进行实验测试。以某云平台为实验对象,利用传感器对其进行运行数据采集,由此构建对应的实验环境。其具体的实验环境如图 3 所示。



图 3 实验环境

如图 3 所示,利用数据采集器对云平台的运行数据进行采集,并将采集的运行数据传输到计算机中,对其进行处理和分析。同时,设置相应的实验参数。其具体的实验参数如表 1 所示。

表 1 实验参数

序号	实验参数	参数设置
1	深度学习网络的层数	3 层
2	深度学习网络的节点数	400
3	学习率	0.05
4	正则化参数	1.0
5	信任值阈值	0.7
6	更新周期	20 s
7	采样时间	2 h
8	数据集 A	10000 条
9	数据集 B	523 条
10	数据集 C	6248 条

如表 1 所示,利用先对采集的云平台运行数据进行处理,根据处理结果,提取出云平台运行数据特征,再计算不同数据的信任值。其具体计算结果如图 4 所示。

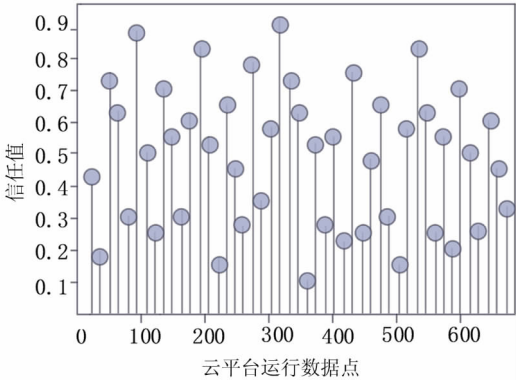


图 4 云平台运行数据信任值的计算结果

如图 4 所示,结合提取的特征,构建对应的恶意攻击检测模型,实现对恶意攻击的检测和处理。

2.2 实验结果讨论

为验证上述三种算法在实际应用中的效果,以算法的检出率为评价指标,对比三种算法的性能。利用三种算法对数据集 A 进行多次恶意攻击检测,统计其检测结果。其具体统计结果如图 5 所示。

如图 5 所示,算法 1 的检出率较高,且在多次实验中数值均在 90% 以上,算法 2 和算法 3 的检出率则相对较低。因此,算法 1 在实际应用中检测效果较好。

为进一步验证上述三种算法在实际应用中的效果,以算法的内存开销为评价指标,进行实验测试。利用三种算法对数据集进行多次检测,统计其检测过程中的内存开销。其具体统计结果如表 2 所示。

表 2 三种算法的检测结果

实验次数	三种算法的内存开销/KB		
	算法 1	算法 2	算法 3
1	52.16	156.48	326.12
2	53.68	142.96	363.36
3	54.36	136.26	345.87
4	62.39	155.26	356.15
5	66.45	174.63	396.78
6	67.13	196.26	400.12
7	68.22	187.26	402.36
8	64.12	188.14	402.56
9	63.69	169.32	413.26
10	61.54	170.26	425.96

如表 2 所示,算法 1 的内存开销均在 70 KB 以下,占用的内存资源较小,算法 2 和算法 3 的内存开销均在 100 KB 以上,占用的内存资源远高于算法 1。因此算法 1 在实际应用中的检测效果较好。

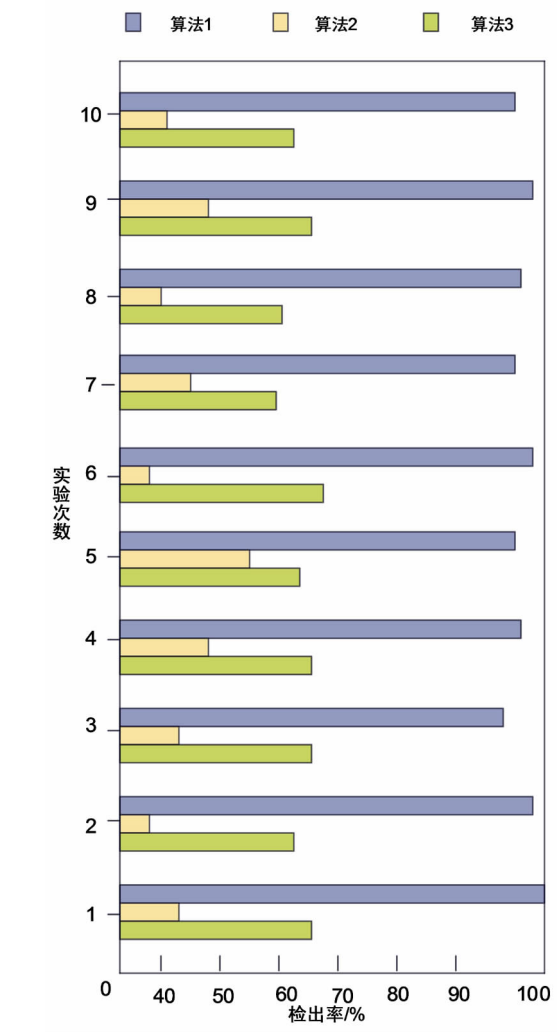


图 5 三种算法的检测结果

综上所述,本文设计的基于深度学习和信任度量的云平台自适应恶意攻击检测与响应算法在实际应用中检出率较高,内存开销较小,检测效果较好,能够准确地检测出云平台在运行过程中出现的恶意攻击,保证云平台的稳定运行。

3 结 论

本文提出了基于深度学习和信任度量的自适应恶意攻击检测与响应算法,通过深度学习模型对流量数据进行高效处理,准确识别出恶意流量,同时结合信任度量机制,对云平台中的实体行为进行评估。该算法在实际应用中检出率较高,内存开销较小,检测效果较好,能够准确地检测出云平台在

运行过程中出现的恶意攻击,保证云平台的稳定运行。下一步将不断优化和改进算法,进一步提高云平台的安全性和稳定性,为用户提供更加安全可靠的云服务。

参考文献

[1] 李群,董佳涵,关志涛,等. 一种基于聚类分类的物联网恶意攻击检测方法 [J]. 信息安全, 2021, 21 (8): 82—90.

[2] 毛莉君,王心妍. 基于能耗信任值的无线传感网络克隆攻击检测方法 [J]. 传感技术学报, 2023, 36 (7): 1122—1127.

[3] XU C Y, SHEN J Z, DU X. Low-rate DoS attack detection method based on hybrid deep neural networks[J]. Journal of information security and applications, 2021, 21 (8): 125—136.

[4] KHARLAMOVA N, TRHOLD C, HASHEMI S. Cyberattack detection methods for battery energy storage systems [J]. Journal of Energy Storage, 2023, 44 (15): 1023—1048.

[5] 邢光林,霍红,侯睿. 命名数据网络中基于增强隔离林的 Interest 包洪泛攻击检测方法 [J]. 中南民族大学学报(自然科学版), 2023, 42 (4): 477—481.

[6] 王立敏,卜磊,马乐之,等. 基于指标依赖模型构建与监控的攻击检测方法 [J]. 软件学报, 2023, 34 (6): 2641—2668.

[7] 禹宁,竹瑞博,狄婷,等. 基于 CNN-LSTM 的工控协议同源攻击检测方法 [J]. 计算机应用与软件, 2023, 40 (5): 331—337.

[8] 王海吉,胡健坤,田元. 基于 RNN 的智能电网拓扑变异型 FDI 攻击检测方法 [J]. 沈阳工业大学学报, 2023, 45 (2): 139—144.

[9] 孙锐,冯惠东,孙琦景,等. 纹理和深度特征增强的双流人脸呈现攻击检测方法 [J]. 模式识别与人工智能, 2023, 36 (3): 242—251.

[10] 王博,万良,刘明盛,等. DWT 和 AKD 自动编码器的 DDoS 攻击检测方法研究 [J]. 南京信息工程大学学报(自然科学版), 2023, 15 (4): 419—428

[11] 戚梦逸,刘涅槃,陶晓峰,等. 基于相量测量的状态估计攻击检测方法 [J]. 南京信息工程大学学报(自然科学版), 2023, 15 (4): 460—467.

[12] 梁若舟,高跃,赵曦滨. 基于序列特征提取的溯源图上 APT 攻击检测方法 [J]. 中国科学(信息科学), 2022, 52 (8): 1463—1480.

[13] 赵伟,周颖杰,李政辉,等. 一种基于少量异常标签的 SQL 注入攻击检测方法 [J]. 四川大学学报(自然科学版), 2022, 59 (6): 39—47.

[14] 杨亚红,王海瑞. 基于 Renyi 熵和 BiGRU 算法实现 SDN 环境下的 DDoS 攻击检测方法 [J]. 计算机科学, 2022, 49 (S1): 555—561.

[15] 孙涛,蔡江涛,郭政杰,等. SDN 环境下基于动态阈值的 DDoS 攻击检测方法研究 [J]. 内蒙古大学学报(自然科学版), 2022, 53 (1): 98—104.