·热点与综述· 文章编号：1000-3428(2022)02-0010-15 文献标志码：A 中图分类号：TP393

基于机器学习的用户与实体行为分析技术综述

崔景洋[1,2]，陈振国[3]，田立勤[3]，张光华[1]
（1.河北科技大学 信息科学与工程学院，石家庄 050018；2.北京天融信网络安全技术有限公司，北京 100085；
3.华北科技学院 河北省物联网监控工程技术研究中心，河北 廊坊 065201）

摘 要：随着网络安全技术的更新迭代，新型攻击手段日益增加，企业面临未知威胁难以识别的问题。用户与实体行为分析是识别用户和实体行为中潜在威胁事件的一种异常检测技术，广泛应用于企业内部威胁分析和外部入侵检测等任务。基于机器学习方法对用户和实体的行为进行模型建立与风险点识别，可以有效解决未知威胁难以检测的问题，增强企业网络安全防护能力。回顾用户与实体行为分析的发展历程，重点讨论用户与实体行为分析技术在统计学习、深度学习、强化学习等3个方面的应用情况，研究具有代表性的用户与实体行为分析算法并对算法性能进行对比分析。介绍4种常用的公共数据集及特征工程方法，总结两种增强行为表述准确性的特征处理方式。在此基础上，阐述归纳典型异常检测算法的优劣势，指出内部威胁分析与外部入侵检测的局限性，并对用户与实体行为分析技术未来的发展方向进行展望。

关键词：网络安全；用户与实体行为分析；异常检测；统计学习；深度学习；强化学习

开放科学（资源服务）标志码（OSID）：

中文引用格式：崔景洋，陈振国，田立勤，等.基于机器学习的用户与实体行为分析技术综述[J].计算机工程，2022，48(2)：10-24.

英文引用格式：CUI J Y，CHEN Z G，TIAN L Q，et al.Overview of user and entity behavior analytics technology based on machine learning[J].Computer Engineering，2022，48(2)：10-24.

Overview of User and Entity Behavior Analytics Technology Based on Machine Learning

CUI Jingyang[1,2]，CHEN Zhenguo[3]，TIAN Liqin[3]，ZHANG Guanghua[1]
（1.School of Information Science and Engineering，Hebei University of Science and Technology，Shijiazhuang 050018，China；
2.Topsec Network Technology Ltd.，Beijing 100085，China；3.Hebei IoT Monitoring Engineering Technology Research Center，
North China Institute of Science and Technology，Langfang，Hebei 065201，China）

【Abstract】With the continuous development of network security technology，new attacking methods are becoming increasingly numerous，exposing enterprises to unknown threats that are difficult to identify. User Entity Behavior Analytics（UEBA）is an anomaly detection technology to identify potential threat events in user and entity behavior. It has been widely used in external intrusion detection and internal threat analysis of enterprises. By using machine learning methods to model user and entity behavior and identify risk points，UEBA can address unknown threats that are difficult to detect，and enhance the defense of enterprise networks. This paper introduces the development history of UEBA，and discusses its applications in statistical learning，deep learning and reinforcement learning. Then the paper presents the studies of typical UEBA algorithms，and gives comparative analysis of their performance. The paper also describes several commonly used public datasets，feature engineering methods，and two feature processing methods that enhance the accuracy of behavior representation. On this basis，this paper summarizes the advantages and disadvantages of typical anomaly detection algorithms，and the limitations of internal threat analysis and external intrusion detection. Finally，the future research directions in this field are discussed.

【Key words】network security；User and Entity Behavior Analytics（UEBA）；anomaly detection；statistical learning；deep learning；reinforcement learning

DOI：10. 19678/j. issn. 1000-3428. 0062623

基金项目：国家重点研发计划项目（2018YFB0804701）；国家自然科学基金（62072239）；河北省科技厅科技计划项目（20377725D）。

作者简介：崔景洋（1992—），男，硕士，主研方向为机器学习、信息安全；陈振国、田立勤、张光华（通信作者），教授、博士。

收稿日期：2021-09-08 **修回日期：**2021-10-29 **E-mail：**xian_software@163.com

0　概述

随着计算机与网络的快速发展，机器学习技术在人们的生活与工作中起着越来越重要的作用，并在兴趣推荐[1-2]、人脸识别[3]、路径规划[4]等领域得到广泛应用。然而，机器学习技术在给人们生活带来便利的同时也产生了一系列风险问题，例如，信息的过度分析使得人们的生活日益透明化，计算机视觉技术的广泛应用使得图片验证码防御作用下降等[5]。一方面，计算机性能的增强以及技术的不断发展使得网络攻击者的攻击方式更加成熟、趋于隐蔽，难以通过传统威胁检测系统进行检测与防御[6]。另一方面，网络流量数据、设备日志数据量快速增长也提高了对检测性能的要求[7]。

为更好地检测潜在威胁并及时准确地发现安全问题，用户与实体行为分析（User and Entity Behavior Analytics，UEBA）技术应运而生，在用户行为分析（User and Behavior Analytics，UBA）以及安全信息和事件管理（Security Information and Event Management，SIEM）的基础上发展而来[8]，是一种针对内外网威胁进行分析并通过多维度对系统所面临的风险进行综合评价的威胁检测方法[9]，其中增加的实体（Entity）概念强调了设备行为在网络攻击与威胁检测中的作用。与传统检测方法相比，UEBA进一步提高了威胁检测的精度与效率，增加了风险判断的表述功能，有利于系统发现未知风险，增强系统安全性[10]。

根据用户和实体行为建立基线，找出用户以及实体的异常行为，不仅可以实现企业内部行为检测，还可以解决外部网络安全问题[11]。因此，用户与实体行为分析技术已被广泛应用于企业内部行为分析[12]、主机入侵检测[10,13]、用户画像研究[14-15]、复杂行为建模[16]、推荐系统[17-18]等任务。本文从统计学习、深度学习、强化学习等3个角度出发对机器学习在用户与实体行为分析技术中的研究与应用进行介绍，并讨论相关分析方法的局限性与发展趋势。

1　用户与实体行为分析

用户与实体行为分析由Gartner公司[19]于2015年在《Market Guide for User and Entity Behavior Analytics》调查报告中提出，该报告详细介绍了UEBA的定义、使用范围、应用意义等。UEBA是一类用来追踪监视用户、IP地址、主机等异常行为的模型，可以通过行为的上下文关联进行潜在恶意活动分析[9]。与SIEM和UBA相比，UEBA覆盖的分析范围更广，利用的数据种类更多，三者在不同角度的对比情况如表1所示。

表1　SIEM、UBA和UEBA的对比

Table 1　Comparison of SIEM，UBA and UEBA

检测技术	数据源	分析对象	检测方式	检测结果
SIEM	告警信息	安全信息、安全事件	基于规则	异常点
UBA	用户操作日志	用户行为	基于学习	异常行为序列
UEBA	用户操作日志、应用日志、系统日志	用户与实体行为	基于学习	异常行为序列

自20世纪90年代以来，学者们就开始分析用户的网络行为[20]，由于当时攻击手段单一、检测能力有限，因此威胁检测的目标多以实时防御为主[21]、手段多以专家经验所转换的识别逻辑检测为主[22]、结果多以“正常”和“异常”两种状态为主。之后，新的攻击方式不断增加、新的威胁类型不断出现，传统方法在面对新威胁时的检测效果有限，学者们开始使用进化算法识别未知威胁[23]。21世纪初期，支持向量机（Support Vector Machine，SVM）得到了快速发展与广泛流行，作为传统机器学习算法的里程碑，该算法衍化出一系列变种形式[24]，在威胁检测方面也有不错的效果。目前，行为分析与入侵检测方法多数属于人工智能范畴，以传统统计学习方法为主。随着设备算力的提高与深度学习的发展，学者们开始广泛采用神经网络算法进行检测，以深度学习为主的检测方法在未来的研究中可能会成为主流。此外，知识图谱等复杂数据类型在攻击路径方面有较强的表述能力，因此也有一部分学者使用知识图谱进行入侵检测研究[25]。整个UEBA技术的发展历程呈现由简单到复杂的趋势，各个发展阶段中具有一定代表性的研究成果如图1所示。

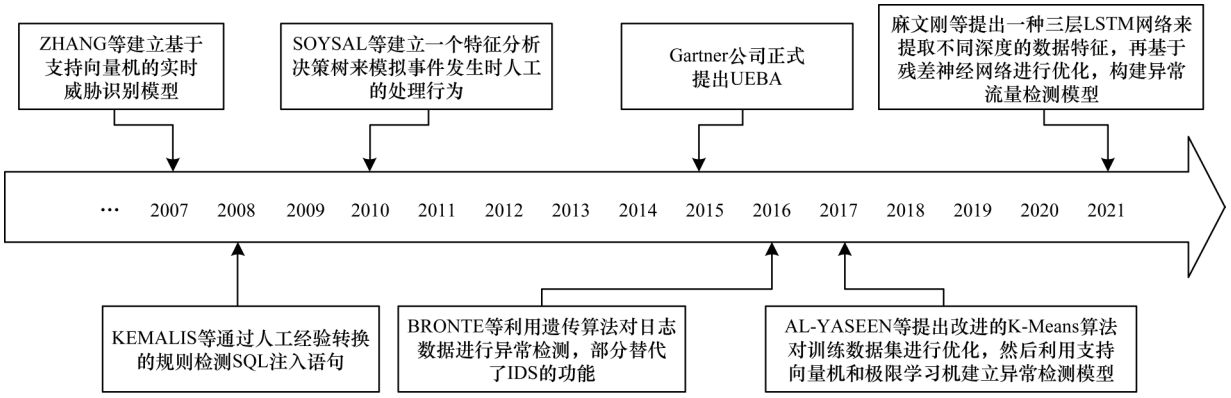

图1　UEBA发展趋势图

Fig.1　Development trend chart of UEBA

UEBA的分析对象包括用户行为与实体行为。用户行为指的是用户在终端设备的操作[26],例如使用应用程序、与数据的交互、点击行为、鼠标移动、执行命令行语句等。实体行为主要指无法与真实用户产生直接关联的行为[27],例如某些APP自身的运行日志、病毒木马的动作记录以及一些高级持续性威胁(Advanced Persistent Threat, APT)[28]的行为轨迹等。

根据行为产生路径与方向的不同,UEBA的研究内容主要包含内部威胁分析及外部入侵检测两个方面。内部威胁分析主要解决企业内部违规操作所引起的安全问题,从内向外所延展出的异常事件复杂多变的形式是内部行为分析中的研究难点,对于员工行为进行分析、发现其中的异常点,可以降低企业风险,提高企业管理效率,避免从内部产生攻击。外部入侵检测同样也是UEBA技术中不可或缺的一环,例如防火墙(Firewall)、入侵检测系统(Intrusion Detection System, IDS)、入侵防御系统(Intrusion Prevention System, IPS)以及Web应用防火墙(Web Application Firewall, WAF)等[29],这几种外部检测方法是目前各研究领域的热点,在实际应用中均有不错效果。

2 基于统计学习的UEBA技术

本节将讨论统计学习方法在UEBA技术中的应用。统计学习是基于统计方法对数据规律进行总结的一种关键技术,根据类别标签的使用方式不同,统计学习由监督学习、无监督学习、半监督学习等研究类别组成[30],其中:监督学习指的是使用带有类别标签的数据进行模型建立的过程,主要用于解决分类、回归等问题[31];无监督学习是指有数据但没有标签的情况,主要应用于聚类分析、异常值检测等任务[32];半监督学习是指训练数据中只含有小部分标签,根据实际情况在医疗诊断、物联网设备分析、工业故障分析、流量异常检测等领域中[33]有广泛应用。

2.1 基于有监督统计学习的UEBA技术

监督学习的建模过程一般是构建预测器的过程。监督学习使用带有已知的类别标签训练数据进行模型训练,模型建立完成后再对待检测样本进行预测,无论是对于离散变量的分类还是对于连续变量的回归,都需要模型给出一个预测值。监督学习的代表算法有KNN、SVM、逻辑斯谛回归、线性回归、决策树等[34],在UEBA中,基于监督学习的算法可以根据先验数据构建预测模型,并对新样本进行预测,从而判断新样本的异常程度或者对新样本按照不同的攻击类型进行多分类和二分类。

基于规则的检测方法在入侵检测系统中具有广泛应用。文献[35]根据经验设计检测逻辑对SQL注入行为进行检测,模型利用SQL语句规范来定义Web应用程序生成和执行SQL查询时预期的语法结构,建立SQL语句有效性检测模块,并使用事件监控模块检测违反规范的查询行为,符合预期结构的语句才能正常在数据库内执行,实时检测SQL注入攻击。之后将检测的结果记录到日志中以便后续检测过程中检测结构的建立,其中准确率(Accuracy)和召回率(Recall)达到100%,具体的检测过程如图2所示。

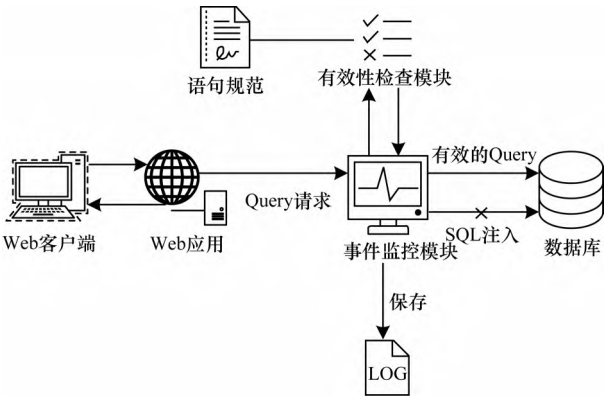

图2 通过人工经验转换的规则检测SRL注入语句的流程

Fig.2 Procedure of detecting SRL injection sentences through the rules of human experience conversion

文献[36]研究无人机(Unmanned Aerial Vehicles, UAV)的安全问题,根据无线数据攻击的链路特征以及其他影响因素建立攻击检测规则,增强了无人机系统的安全性,其准确率为97.4%。文献[37]建立基于预定义事件签名的Web应用入侵检测系统,通过签名知识库进行行为分析与异常检测。但上述基于规则的检测方法难以应对未知威胁,不能够对相应的系统进行动态防护[38]。

回归方法在检测过程中多应用于连续异常值的检测,大部分带有时序性特征。文献[39]对用户的登录时间、登录间隔、在线时长、会话时长等行为特征进行回归分析,建立用户习惯画像进行异常识别并及时调整网络负载。学者们还使用3σ准则、自回归(Autoregressive, AR)模型、自回归移动平均(Autoregressive Moving Average, ARMA)模型等[40]将历史行为基线与预测值进行比较,如果预测值与行为基线相差较大,则会被标注为异常值。

针对有类别标记的行为数据,可以直接使用算法构建模型。文献[41]使用KNN算法对用户行为数据进行分析,建立针对“伪装者”数据的分类模型。监督学习算法的性能瓶颈在于训练数据集中类别标签的正确率,由于很多数据集样本的标签都已经固定,因此一些学者也采用多算法结合的方式提升异常检测的正确率。文献[42]基于KNN构建一种云环境下的入侵检测系统,该系统参考了智能体(Agent)与聚类算法的特性提高了入侵检测的效率,系统的准确率与召回率分别为92.23%与88.07%,在实际应用中取得了不错的效果。此外,决策树算法的检测方式简单、逻辑清晰、可解释性强,也大范围应用于异常检测领域[43]。为减少建模时间,提升模

型检测效果，文献[44]使用SMOTE（Synthetic Minority Oversampling Technique）采样方法对高度不平衡的数据进行预处理，之后分别使用Hellinger距离以及K-L散度对构造过程进行改进，建立了惰性决策树（LazyDT）提高算法性能。

基于监督学习的行为分析与异常检测的优势在于可以使用先验知识进行建模，在从一定程度上提高了检测精度，但检测流程过于依赖样本标签。在实际应用中：一方面，样本标签的质量会对检测模型的构建起到非常大的影响；另一方面，对数据样本进行标注同样也会消耗大量人力成本与时间成本。因此，在使用监督学习算法建立异常识别模型时，还需要注意在建模过程中训练成本与检测效率之间的平衡问题。

2.2　基于无监督统计学习的UEBA技术

在实际入侵检测与行为分析中，数据在产生时往往并不带有标签，而采用一些方式对数据进行标注会耗费一定的资源。无监督学习可以从无标签数据中学习一定的规律，并使用这些规律对新数据进行分析。无监督学习的代表算法有K均值（K-Means）、基于密度的聚类算法（Density-Based Spatial Clustering of Applications with Noise，DBSCAN）、主成分分析（Principal Component Analysis，PCA）等[45]。在UEBA中使用聚类等无监督学习方法进行威胁识别时，一般会对大部分数据样本的代表性特征进行学习，并根据数据自身的特性进行分类，最终针对偏离群体的数据样本进行分析，判断其是否为异常点。近年来，各种类型的网络设备与数量均呈现增长趋势，所产生的海量数据难以标记，因此无监督威胁检测算法的研究是未来的重点之一。

K均值算法的训练速度快、可解释性强，广泛用于异常识别。文献[46]基于K均值算法构建一种多层次入侵检测模型，通过分批进行小规模训练的方式减少模型的迭代时间，借鉴支持向量机的思想来优化检测流程，准确率为95.75%，FPR为1.87%，取得了不错的效果。文献[47]基于K均值算法按照特征对流量数据进行分组，在调参的同时尽可能地保留分组信息，该方法可以显著降低训练模型所需的特征数从而提高检测效率，其准确率达到了99.73%。与K均值算法相比，DBSCAN算法不仅更适合识别不规则形状的聚类簇，还能在一定程度上减少噪声数据在建模过程中的干扰[48]。文献[49]构建一种自适应DBSCAN算法，该算法首先分析流量数据的特征值，之后对聚类簇内数据与噪声数据分别进行处理，并建立对应的余弦相似性计算过程。该处理方式降低了噪声数据对于模型准确度的影响，增强了模型的鲁棒性。由于采取了对噪声值单独处理的建模思路，因此该模型可以更加细致地检测出隐蔽的DoS攻击，其准确率达到了99.96%，具体建模过程如图3所示。

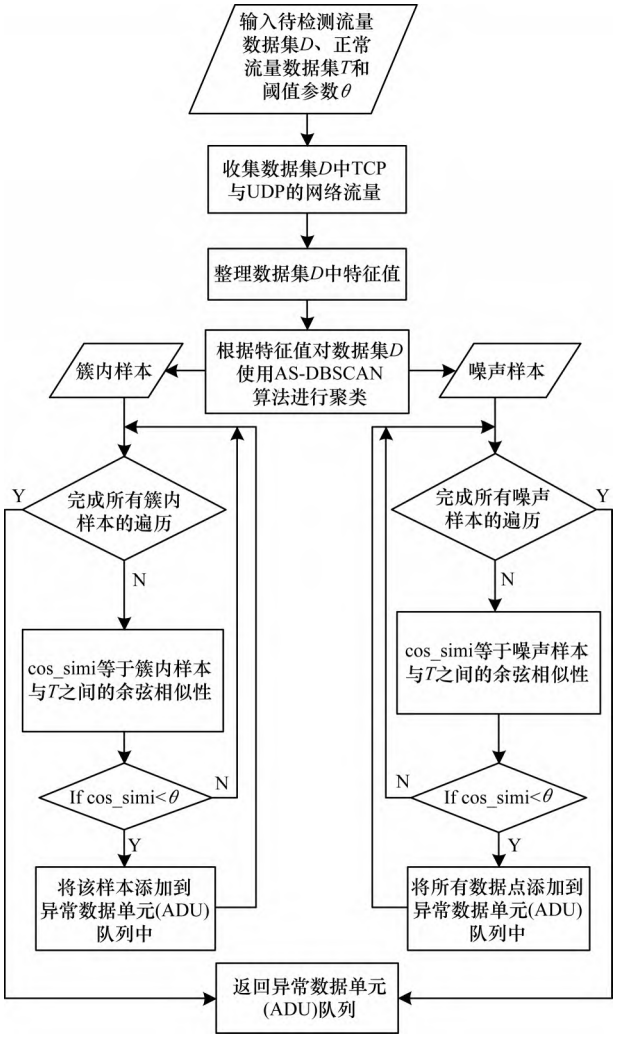

图3　通过对簇内数据与噪声数据分别建模检测异常的流程

Fig.3　Procedure of anomaly detection through modeling for data in cluster and noise data respectively

在实际异常检测过程中，有时不需要获得确定性的聚类结果。对用户及实体行为进行模糊聚类[50]，可以使得一个实体包含在若干聚类簇内，从一定程度上可以避免遗漏异常行为，降低了异常检测算法的漏报率。主成分分析方法主要用于建模前数据的降维处理，文献[51]使用PCA算法处理了数据库操作行为日志，降低了行为数据维度，提高了建模速度。同时，主成分分析也可以直接用于异常检测，文献[52]设计一种基于PCA算法的无监督自动化异常检测方法，通过计算降维后源空间与低维空间映射点的直接距离，检测主机操作日志映射过程失衡的情况，进行异常点的判断。

随着设备数据产出量的不断扩大，样本的标记工作也变得愈发困难，基于无监督的异常检测方法在UEBA研究领域将成为热点方向，无监督算法可以减少数据样本对标签的依赖，一方面可以降低类别标注的成本，另一方面能从未被标签束缚的样本中学到新规则，解决一定的未知风险识别问题。但不足之处在于无监督学习算法往往都需要大量的计算资源，如何降低计算开销解决大规模数据处理问

题,是无监督异常检测算法一个重要的研究方向。

2.3 基于半监督统计学习的UEBA技术

半监督学习因其所使用的训练数据只含有部分标签,所以名为半监督学习[53]。尽管对每条网络数据进行标注需要付出一定的代价,但在各网络设备、网络探针或者监测系统中获得少部分带有标签的数据相对比较容易。半监督学习能够将少量带标签与大量无标签数据相结合构成训练集完成建模过程,通常半监督学习可以获得比无监督聚类更好的检测效果[54]。半监督学习算法包括半监督聚类、半监督分类、半监督降维、半监督集成等算法[55]。在UEBA中半监督算法可以在一定程度上解决实际流量数据、行为数据异常样本与正常样本的不平衡分布问题,比较适合应用于当前形势下的工业安全防御体系。

聚类作为异常检测的主要手段在现阶段研究中占有较大比重,半监督聚类是无监督聚类的升级版本,结合有监督与无监督学习过程的优势,优化异常检测与行为分析的效果。文献[56]提出一种基于协同聚类的半监督DDoS检测算法,该算法中无监督的部分可以剔除与DDoS检测无关的流量数据,从而减少误报率,提高准确性,最终准确率为98.23%、FPR为0.33%。文献[57]提出一种基于K-Means的半监督算法,该算法能够通过改进聚类初始中心的选择解决孤立点和局部最优的问题,优化DDoS检测的结果,其准确率为99.68%,效果优于文献[56]的检测模型。半监督分类同样也有不少研究成果,文献[58]设计一种半监督支持向量机,可以充分利用未标记样本数据的潜在信息,优化分类过程,最终构建在线分类器。在实际威胁检测与行为分析中,由于数据样本的维度过高,通常需要将特征降维后再进行建模,针对不平衡样本分布情况,可以使用文献[59]提出的降维算法,专门应对稀疏样本问题,该算法通过保留矩阵局部投影的方式处理未标记信息,之后再对其他未标记信息进行处理,分析其K近邻的几何结果,适合异常检测问题的数据处理。除此之外,半监督集成也是当前的一个研究热点[60],可以先将未标记的样本通过自我训练的方式组成若干小的分类器,之后将这些小分类器集成为一个整体进行预测,解决了标记样本数据过少的问题。

无论是对于企业内部用户行为分析还是外部入侵检测,最大的问题仍然是数据样本难以标注。与监督学习相比,半监督学习对数据标注比例没有特定要求;与同一算法的无监督学习相比,半监督学习往往能取得更好的检测效果。但由于样本标签的特殊性,半监督学习需要更复杂的处理流程与更长的训练时间。此外,在半监督算法的设计过程中,一般都只针对一种类型的问题进行优化,同一个半监督算法难以推广到其他应用场景。例如,文献[56-57]均专门针对DDoS场景进行设计,不能检测其他类型的威胁或者异常情况。

2.4 统计学习模型性能对比及分析

基于统计学习方法对内部人员进行行为分析、外部网络异常进行检测的技术手段发展比较成熟,侧重点在于根据样本标注进行各类别数据中的规律学习,在计算效率与计算结果的可解释性方面要优于深度学习方法。由于训练过程较为清晰,因此异常行为链的全过程呈现方面与深度学习相比具有较大的优势。表2给出了部分统计学习算法的对比情况,其中:N/A表示原文献未体现相关指标;性能评价数据来自原文献,可能存在实验环境及参数的不同。基于传统机器学习的异常检测多为二分类算法,即判断一个样本是否为异常样本。相较多分类任务,二分类任务在模型训练成本以及预测准确度评价方面具有一定优势,因此在整体性能表现上要优于深度学习方法。

表2 部分统计学习算法的性能评价对比

Table 2 Comparison of performance evaluation of some statistical learning algorithms

统计学习类型	文献编号	统计学习算法	任务类别	性能评价指标/%		
				Accuracy	Recall	FPR
有监督	文献[35]	特征匹配	二分类	100.00	100.00	N/A
	文献[36]	加权特征计算	二分类	97.40	N/A	N/A
	文献[42]	Agent聚类、K-Means、KNN	二分类	92.23	88.07	N/A
无监督	文献[46]	K-Means、SVM、ELM	多分类	95.75	N/A	1.87
	文献[47]	KBFG-C4.5	多分类	99.73	N/A	0.00
	文献[49]	DBSCAN	二分类	99.96	N/A	0.00
半监督	文献[56]	Co-clustering	二分类	98.23	N/A	0.33
	文献[57]	半监督K-Means	二分类	99.68	N/A	1.40

在实际应用中,样本标注仍然是当前所面临的主要问题之一。对于有监督学习而言,尽管可以通过设置合适的参数、选取恰当的模型等方法得到不错的模型表现,甚至能够达到100%的预测准确率,但只局限于实验环境。在企业应用中由于样本标注成本问题,半监督学习在未来会更具发展前景。

3 基于深度学习的UEBA技术

以往神经网络受限于计算能力不足,应用范围不如统计学习方法广泛,但自从21世纪初设备算力逐步提高,神经网络的研究取得了革命性进展,尤其在最近10年间,对于神经网络的研究与使用成为当下最主流的研究方向之一。深度学习通过神经网络

从连续的神经层中学习参数，构建预测模型。深度学习与传统统计学习方法在特征与权重的处理方式上有着明显不同，尤其神经网络非线性权重模型在特征选择方面表现优异。随着当前安全数据规模的不断扩大，特征的种类也变得越来越多，传统机器学习手段在进行复杂特征选择方面的优势不足，而深度学习方法可以进行自动特征选择，更适合目前的情况。在实际应用中，深度学习模型主要包括自编码器（Auto Encoder，AE）、多层感知神经网络、循环神经网络、卷积神经网络、生成式对抗网络等。

3.1　基于自编码器的UEBA技术

自编码器是一种可以学到输入数据高效表示的神经网络，对监督信息不敏感，一般包含编码器（Encoder）与解码器（Decoder）两个部分。常用的自编码数据异常检测模型有自编码模型和变分自编码（Variational Auto Encoder，VAE）模型两种。

文献[61]基于自编码模型建立一种稀疏数据表示框架，针对大规模高维数据可以起到降维的作用，同时能够提取比手动处理更高级的特征，最终F1值（F1-Score）达到了0.812 0。有些自编码器需要学者们提供不包含异常的干净数据才能正常建模，而有些鲁棒性较强的自编码器[62]可以直接使用包含异常的数据，并从中识别出异常值和噪声，但其准确率与召回率均只有65%。但在无监督特征抽取、复杂任务处理、异常实时检测等方面，自编码器效果有限，因此学者们也会采用与其他方法结合的形式进行异常检测。文献[63]在使用编码器的过程中发现在尝试将输出数据尽量还原成对应输入的过程中，隐藏层的数据流动会产生压缩，基于此原理提出一种基于密度估计的自编码异常检测模型，解决了自编码器在训练集上重建异常数据能力差的问题。在训练阶段，自编码器首先在一个正常的训练集上进行训练，得到初步训练完成的模型，随后使用训练集进行训练并将训练数据压缩至隐藏层，通过设置密度阈值的方式调节压缩尺度，采用质心密度估计和核密度估计（Kernel Density Estimation，KDE）两种方法来建立密度估计模型，从而解决异常点检测问题，建模过程如图4所示。

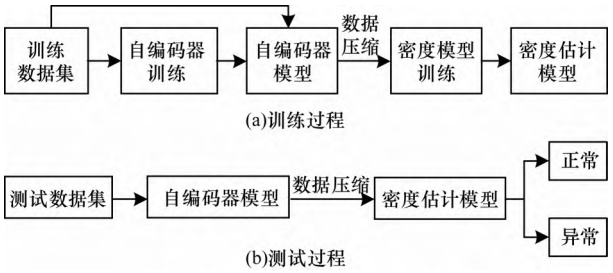

图4　基于密度估计的自编码异常检测流程

Fig.4　Procedure of auto encoding anomaly detection based on density estimation

3.2　基于多层感知神经网络的UEBA技术

多层感知（Multi-Layer Perceptron，MLP）神经网络是一种基础神经网络，由一个输入层、一个输出层和多个隐藏层组成。在多层感知神经网络中，各层网络之间通过全连接的方式构成网络结构，在各神经元中可以设置激活函数实现非线性函数参数的学习，常用的激活函数有tanh、sigmoid、relu等，MLP可以构成最简单的分类器，实现softmax逻辑回归。文献[64]利用MLP进行KDD CUP 99数据的分类处理，在某些类别的攻击上的检测效果优于SVM算法。但由于多层感知神经网络的构造比较简单，因此直接应用于数据中取得的效果往往较有限，其在UEBA中多与其他算法进行联合使用。文献[65]利用Apriori算法进行样本特征的处理，挖掘出样本中关联规则较强的特征后再使用多个MLP进行分类，并使用AdaBoost算法集成得到最终结果，其准确率达到了99.55%。总体而言，尽管多层感知神经网络只有简单的结构形式，但仍然可以学习出数据内的非线性信息，因此在简单数据分类上一般要优于传统统计学习算法。

3.3　基于卷积神经网络的UEBA技术

卷积神经网络（Convolutional Neural Network，CNN）主要基于卷积层和池化层的往复作用实现特征抽取，最终通过全连接层实现分类。在多次卷积和池化的过程中，数据的特征被很好学习。一般在处理数据的过程中，需要将样本数据转换为图像的形式才能进行检测。在流量分析中，可以使用二进制表示的流量数据，将数据串进行分割处理，按照字节进行裁剪，之后将每个字节都转换成二进制值，再转换成像素点。然后通过对多个像素点进行整合，可以将某一串流量数据转换为灰度图片。

文献[66]整理了多个将流量数据转换为相应图像的方式，不需要手工抽取设计特征，减少了主观因素在异常检测过程中的影响，之后使用卷积神经网络对流量数据的图片形式进行处理，识别其中的异常软件流量。针对基础设施的工业控制系统（Industrial Control System，ICS）的异常检测问题，文献[67]结合主成分分析法与卷积神经网络设计一种1D卷积网络，其准确率、召回率与F1值分别为98.02%、98.39%和0.980 5。文献[68]注意到当前ICS数据有限，只使用工业数据进行异常检测的效果不佳，于是采用传统IT数据与ICS数据相结合的形式合成一个新的训练数据集，随后使用CNN进行检测，效果要优于只使用工业数据的情况，其准确率为86.37%，召回率为67.67%。

使用卷积神经网络处理流量进行威胁行为检测问题的主要难点在于如何进行前期数据处理工作使其适用于CNN的网络结构。对于特征处理及抽取的方法将直接影响检测效果。与常见的全连接神经网络相比，卷积神经网络的优势在于可以处理更高维度的数据，而且使用者完全不用关心每一层特征的具体表现形式，其缺点是过程不透明，可解释性较差，只给出了检测结果，很难对检测过程的细节进行分析。

3.4　基于循环神经网络的UEBA技术

循环神经网络（Recurrent Neural Network，RNN）是一类用来处理序列数据的神经网络。基础神经网络只在层与层之间建立连接，而RNN可以在本层处理单元内部之间进行连接。从作用上看，这是一种带有记忆功能的反馈系统，当前神经元状态与上一时刻的神经元状态密切相关。因此，RNN在具有序列属性的数据上表现尤其优异，无论是流量分析还是用户行为检测，均能够挖掘出数据中所包含的时序信息及行为意图。

基于循环神经网络对Linux系统内的实体行为进行分析，利用RNN对特征的敏感性抽取行为特征可以实现对网络日志中的高级网络威胁进行检测[69-70]。文献[71]基于CNN与RNN提出两个有效的载荷分类方法，可以在无需特征工程的情况下，快速完成分类并显著提高分类准确率，该方法在NSL-KDD数据集上的表现尤为突出，其准确率、召回率和F1值分别达到99.36%、99.81%和0.993 8。文献[72]将模糊C均值聚类与循环神经网络相结合，采用先聚类后神经网络分类的方式对流量数据进行处理，解决了云环境中入侵检测系统效率低下的问题。长短期记忆(Long Short-Term Memory，LSTM)网络是一种时间循环神经网络，尤其解决了长序列训练过程中的梯度爆炸或梯度消失问题。文献[73]将三层LSTM堆叠在一起分层抽取流量数据的不同深度特征，每通过一次LSTM层，数据特征增加一阶，最终将一阶、二阶、三阶特征与原始数据进行合并，再基于残差神经网络对其中的异常数据进行识别，模型准确率、召回率与F1值分别为90.78%、94.61%、0.925。

循环神经网络在训练过程中需要计算网络梯度数值，而梯度又与神经元权重密切相关，很容易造成梯度过大过小的问题，这是RNN模型应用中最值得注意的一点，在长序列分析时尤其明显。因此，在使用RNN进行用户或实体的行为序列分析时，应尽量减少序列输入规模或者在结构上进行改进。

3.5 基于生成式对抗网络的UEBA技术

生成式对抗网络(Generative Adversarial Network，GAN)[74]自2014提出以来受到了工业界和学术界的广泛关注，是一种无监督方法，至少包括生成(Generative，G)模型和判别(Discriminative，D)模型两个部分，通过两个模型相互博弈进行模型训练，判别模型根据生成数据判断数据类型，生成模型根据给定数据生成新的数据。在博弈过程中，为了得到更好的结果，这两个模型会不断提高自己的判别效率与生成效率。在进行异常检测时，经常存在数据分布极度不平衡的问题，正常样本远大于异常样本。直接对不平衡数据建模分析容易造成模型有偏，进一步影响模型的准确率。GAN可以生成具有真实样本分布的数据，解决数据有偏问题，因此通常学者们更关注GAN模型的生成部分。

文献[75]基于TensorFlow框架使用GAN及高斯判别分析对异常样本进行扩充，提高了异常检测的准确率，另外还并行训练模型，实现准确实时异常检测，适用于工业界的大数据环境中的数据增强和不平衡样本分类。还有学者在研究中发现某些异常样本会对模型的性能产生影响，甚至能够作为系统防御漏洞被黑客攻击，于是开始研究使用GAN生成的异常数据与检测模型优化IDS的防御效果。文献[76]将GAN作为IDS的前置处理单元，使用生成模型对流量数据中的非功能特征进行处理得到生成特征，并结合流量数据中的功能特征构建新的流量数据。将这些生成的流量数据作为异常样本输入到判别模型中，往复进行训练确保D模型能够学习到假的流量示例，将D模型作为IDS的前置单元一方面能够甄别可能存在的黑客通过伪造流量而产生攻击行为，另一方面也可能增强IDS的识别能力，增加其在流量数据处理过程中应对未知威胁的能力，具体的建模过程如图5所示。文献[77]使用自编码器将数据从原始空间映射到潜在空间，之后使用生成对抗网络精确估计潜在分布的概率表示，利用潜在空间的概率分布作为输入数据，建立异常检测模型。文献[78]先使用蒙特卡洛搜索树算法扩充跨站脚本攻击(Cross-Site Scripting，XSS)样本解决数据有偏问题，之后建立基于GAN的XSS检测系统，着重利用判别部分对异常流量进行检测。文献[79]建立基于GAN的入侵检测系统，结合自编码器改善IDS性能并提高检测稳定性，系统在召回率上表现优异，达到了91.15%。

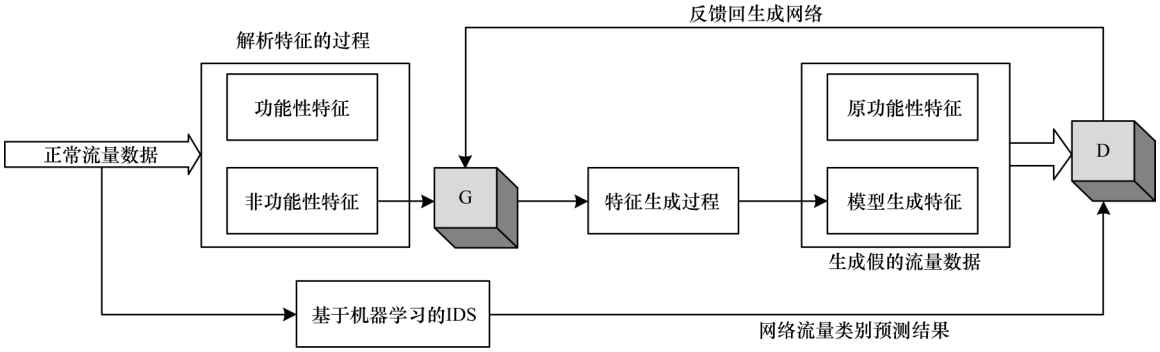

图5 基于对抗样本生成的GAN异常检测流程

Fig.5 Procedure of GAN anomaly detection based on adversarial example generation

学者们主要使用GAN来解决数据中的不平衡问题，在实际使用中需要结合其他算法才能完成用户或实体的行为分析过程。相比其他生成模型或者抽样进行样本扩充的方法，GAN能够生成更真实的样本数据，更能优化模型的检测结果。由于GAN能够采用无监督的方式训练，在当前的异常检测与行为分析领域应用广泛。但在实际应用过程中，GAN也可能出现模式崩溃的问题，而且生成过程对于使用者而言不透明，因此在神经网络参数调节时面临一定的困难。

3.6 深度学习模型性能对比及分析

随着深度学习技术的不断发展，各种类型神经网络的应用为UEBA提供了新思路。神经网络应用于多分类任务时的性能优于统计学习方法，但检测过程的可解释较差，难以还原攻击行为的过程。表3给出了部分深度学习算法的性能对比情况，其中：N/A表示原文献未体现相关指标；性能评价数据来

自原文献，可能存在实验环境及参数的不同。任务类别以多分类为主，整体性能表现略逊于统计学习算法。一方面，对于多分类任务而言，分类结果为某种具体的攻击类型，比二分类任务结果更为细化，因此在算法性能评价时可能存在一定的劣势。另一方面，多分类结果对于后续异常行为分析过程而言，可参考性更高，网络管理者能够从多分类结果中得到更多有用的信息。在检测性能相差不大的情况下，多分类结果比二分类结果更有意义，例如在文献[71]的CNN与RNN使用过程中，不但实现了样本的多分类，而且具有良好的性能表现，适合实际应用。

表3　部分深度学习算法的性能评价对比

Table 3　Comparison of performance evaluation of some deep learning algorithms

深度学习类型	文献编号	深度学习算法	任务类别	性能评价指标			
				Accuracy/%	Recall/%	F1-Score	其他
自编码器	文献[61]	VAE	多分类	N/A	N/A	0.812 0	AUC:0.951 0
	文献[62]	PCA、深度自编码器	二分类	65.00	65.00	0.640 0	N/A
多层感知器	文献[65]	AdaBoost+MLP	多分类	99.55	N/A	N/A	N/A
卷积神经网络	文献[67]	PCA、CNN	多分类	98.02	98.39	0.980 5	N/A
	文献[68]	CNN	多分类	86.37	67.67	N/A	FPR:0.058 4
循环神经网络	文献[71]	CNN、RNN	多分类	99.36	99.81	0.993 8	N/A
	文献[73]	LSTM	多分类	90.78	94.61	0.925 0	AUC:0.951 0
生成式对抗网络	文献[79]	GAN	多分类	74.72	91.15	0.709 7	AUC:0.745 1

4　基于强化学习的UEBA技术

强化学习又被称为增强学习，在模型训练过程中不需要数据样本的标签，主要通过Agent与环境交互的方式进行模型训练，目标是使得Agent获取最大收益。强化学习受行为主义心理学的启发，强调的是“再”学习的过程。与其他统计学习方法相比，强化学习可以不参考给定的类别标签，而是通过结果给予模型的回馈来更新所需参数[80]。通常而言，强化学习有很强的时序性，每次的结果都极大依赖上一步中智能体的状态。强化学习的代表算法包括Q-Learning、状态-动作-奖励-状态-动作（State-Action-Reward-State-Action，SARSA）、深度Q网络（Deep Q Network，DQN）以及深度确定性策略梯度（Deep Deterministic Policy Gradient，DDPG）等算法[81]。强化学习是机器学习的重要组成部分，但目前UEBA中的强化学习技术还应用较少，未来还有很大的发展空间。

恶意实体作为高级可持续威胁攻击的一种，常常隐匿在系统中不容易被发现，行为序列特征与运行环境的交互方式适合使用强化学习进行检测。在文献[82-83]研究中，强化学习用于处理恶意实体的行为序列，筛选恶意行为的特征并根据结果反馈动态调整检测模型。XIAO等[84]研究网络游戏环境中的高级可持续威胁，建立一种基于策略的强化学习算法，通过策略爬坡（Policy Hill-Climbing，PHC）方式增加了策略的不确定性，动态引诱持续威胁实体暴露自身意图。XIAO等[85]还结合边缘计算与强化学习设计一种区块链信任机制，可以处理边缘攻击并识别伪造的实体记录。在工业互联网安全方面，文献[86]针对电力系统的错误数据注入（False Data Injection，FDI）问题，设计一种带有短期记忆功能的Q学习算法保证自动电压控制系统的正常运行。

强化学习与其他类型的机器学习方法不同，训练数据主要来自与环境的各种交互。强化学习的优势在于其奖励与惩罚机制简单，训练逻辑也不复杂，可以对环境信息做出快速反应。随着深度学习的不断发展，深度强化学习也逐渐成为领域内的研究热点。深度强化学习继承了深度学习注意力机制在特征处理方面的优点，同样适合处理时序数据，基于时序数据进行分析不仅可以更好地总结历史行为规律，而且能够挖掘更多异常场景，从而应对部分未知威胁。

5　UEBA公共数据集与特征工程

5.1　公共数据集

5.1.1　KDD CUP 99数据集

KDD CUP 99数据集是1999年KDD[87]竞赛所使用的数据集，在异常检测领域被广泛使用，数据集攻击类型主要分为4个大类和39个小类，训练集包含22种攻击，测试集包含17种攻击，具体类别情况如表4所示。

表4　KDD CUP 99数据集攻击类别

Table 4　Attack categories of KDD CUP 99 dataset

类别名称	攻击大类	攻击小类
正常数据	Normal	正常数据
拒绝服务攻击	DoS	DoS、Apache2、Back、Land、Mailbomb、Neptune、Pod、Smurf、Teardrop、Udpstorm
本地超级用户非法越权访问	U2R	U2R、Buffer_overflow、Loadmodule、Perl、Rootkit
远程主机未授权访问	R2L	R2L、Ftp_write、Guess_passwd、Imap、Multihop、Named、Phf、Sendmail、Snmpgetattack、Snmpguess、Spy、Warezclient、Warezmaster、Worm、Xlock、Xsnoop
端口扫描或监听	Probe	Probe、Mscan、Nmap、Saint、Portsweep、Ipsweep、Satan

KDD CUP 99数据集中的每个连接的前41项为属性值,最后1项为类别标签,具体特征含义在数据集kddcup_names.txt文件中进行了描述。

KDD CUP 99数据集由美国国防部高级研究计划局(DARPA)于1998年在麻省理工学院林肯实验室所进行的一个网络安全渗透测试评估项目相关数据抽取收集而来,经哥伦比亚大学的Sal Stolfo教授和北卡罗来纳州立大学的Wenke Lee教授经过分析处理后得到。DARPA在MIT的项目模拟了美国空军局域网的一个网络环境,收集了9周的网络连接和系统审计数据,仿真各种用户类型、网络流量及攻击手段,并在1998年[88]、1999年[89]、2000年[90]公开发布过3次数据集,均广泛用于异常检测领域。历次数据内容基本不变,1999版数据集在1998版数据集的基础上,增加了攻击类型和对于Windows NT系统的操作,而2000版本的数据集则将攻击类型扩充至58种。

NSL-KDD[91]是KDD CUP 99数据集的改进版本,解决了KDD CUP 99数据集中数据冗余、测试数据与训练数据重复、正负样本比例失衡等问题,同样广泛作为UEBA的benchmark数据集。

5.1.2 UNSW-NB15数据集

UNSW-NB15数据集[92]由新南威尔士大学Cyber Range实验室在2015年利用PerfectStorm工具创建,整个数据集包含Fuzzers、Analysis、Backdoors、DoS、exploit、Generic、Reconnaissance、Shellcode、Worms等9种攻击大类,并未进行细致划分。每个样本有49个特征,在UNSW-NB15_features.csv文件中进行了描述。

5.1.3 CIC-IDS 2017数据集

CIC-IDS 2017数据集[93]是加拿大网络安全研究所公开的IDS模拟数据集,解决了之前公共异常检测数据集中攻击手段陈旧、流量多样性差、攻击样本数量少等问题。CIC-IDS 2017数据集包含大量新型攻击手段,且更接近于真实企业环境,除了流量数据之外,还包含一部分经过IDS分析后的结果,实现了包括暴力FTP、暴力SSH、DoS、Heartbleed、Web攻击、SQL注入、僵尸网络、DDoS等8种攻击。

该数据集还有CIC-IDS 2012[94]、CIC-IDS 2018[95]等其他版本,CIC-IDS 2018同样是目前应用范围较广的网络安全数据集。加拿大网络安全研究所还有各类安全设备日志、主机操作记录、软件运行日志等其他类型的UEBA数据集[96],能够提供学者们进一步对各类用户与实体的威胁行为进行识别。

5.1.4 Masquerading User Data数据集

DUMOUCHEL等[97]研究内部人员操作行为对整个系统安全性的影响,构建伪装者用户数据(Masquerading User Data,MUD),共包括50个文件,每个文件都是一个用户的Unix系统的操作数据。每个文件都有15 000条数据,前5 000条为正常用户操作数据,后10 000条中包括随机的异常数据。DUMOUCHEL等为用户操作数据提供了标注,将每100条数据看作一个序列,同时用0和1对序列进行标注,0代表正常,1代表该序列存在伪装者行为。该数据集作为为数不多的用户行为异常检测公共数据集得到了广泛应用。

5.2 用户特征工程

特征工程是整个UEBA过程中的关键一环,对整个分析模型的最终效果起着至关重要的作用。部分特征工程方法比较如表5所示。

表5 部分特征工程方法对比

Table 5 Comparison of some feature engineering methods

文献编号	数据类型	数据来源	特征工程
文献[37]	真实数据	owasp日志	对特征进行编码器编码
文献[42]	公共数据集	KDD CUP 99	先使用改进的K-Means对样本聚类,再对聚类簇进行异常识别
文献[46]	公共数据集	KDD CUP 99	属性离散化、数据归一化,使用改进K-Means进行标签更新
文献[49]	模拟数据、公共数据集	NS-2、TestBed模拟数据、WIDE公共数据集	使用方差和均值来表现流量数据的波动程度并进行min-max归一化
文献[51]	模拟数据	基于TPC-E数据库的模拟数据	使用独热编码处理用户行为数据
文献[56]	公共数据集	NSL-KDD、UNB ISCX 12和UNSW-NB 15	利用Co-clustering算法进行降维并进行特征归一化
文献[57]	真实数据、公共数据集	DARPA DDoS攻击数据集、CAIDA“DDoS攻击2007”数据集、CICIDS“DDoS攻击2017”数据集和真实数据	特征归一化后通过滤波模型排序、划定阈值及筛选

在进行实体行为数据分析的过程中,面临安全设备种类多、属性特征繁杂等问题,因此标准化、归一化方法使用较多。由于部分数据的字符属性没有先后顺序或者大小区别,因此使用独热编码编译字符属性也是常用手段。同时,学者们还通过考察同一类型数据在不同数据集中的特征抽取方式来完善已有数据,例如参考各类公共数据集中对时间串的处理方法,将其进行细化分割为季度、月、周等特征。

用户行为数据的特征相对流量数据而言更匮乏,在实际企业环境下内网主机安装的通常都是Unix类的系统,主机命令有限。在进行用户行为分

析时，行为种类少、数据维度低，很难对各类行为进行区别，很大程度上会影响最终的检测结果。笔者在研究数据的过程中，发现有以下两种方式可以增强用户及实体行为表述准确性：

1）使用“操作行为”与“操作对象”结合的方式细化动作，例如“cd Download”动作要比“cd”的表述性强。较少的主机指令与各类文件名、对象名以及指令参数等结合后，能够使得行为集合指数级扩充。此外，还可以引入词频-逆文档频度（Term Frequency-Inverse Document Frequency，TF-IDF）加权技术对行为频次做进一步处理以增强不同用户或实体行为间的差别度量。

2）参考其他数据集特征对现有数据进行改进。例如，KDD CUP 99数据集中TCP连接基本特征中的连接持续时间（duration）、是否连接同一主机（land）、登录失败次数（num_failed_logins）等参数可以作为目标特征从而对已有数据进行处理。从原始数据中挖掘信息是特征维度提升的重要手段，表6给出了特征处理的部分样例。

表6　主机行为特征处理部分样例

Table 6　Some examples of host behavior feature processing

特征	数据类型	维度	内容描述
时间相关	离散型	5	操作时间的年、月、日、时、分
星期	连续型	7	操作时间为周几
连续登录时间	连续型	1	本次session连续时间
连续操作次数	连续型	1	本次session连续操作数量
操作对象	离散型	1	操作对象名
连续操作当前对象次数	连续型	1	对当前对象的操作次数之和
操作的对象数量	连续型	1	本次session连续操作的数量之和
访问系统敏感位置次数	连续型	1	本次session访问敏感位置次数之和
登录失败次数	连续型	1	登录失败的次数
是否登录管理员用户	离散型	1	登录管理员用户为1，否则为0
是否远程连接其他主机	离散型	1	出现ssh等指令为1，否则为0
⋮	⋮	⋮	⋮

具体的特征构造方法要视情况而定，例如一般日志中的操作时间记录为一个时间字符串，很难发现其中的规律。如果将该时间串转换为年、月、日、时、分、季度、周几、是否为下班时间、是否为工作日等特征，可以增加原始数据的维度，便于后续算法分析。对于“是否为工作日”特征，可以根据取值的不同建立“工作日行为模型”与“非工作日行为模型”，通常分别处理比混合建模效果更好。

6　UEBA技术的局限性与发展方向

6.1　内部威胁分析的局限性

内部威胁分析的数据源以主机操作、数据库、堡垒机、服务器等日志文件为主。这类数据带有一定的时序特征，通过上下文行为关联可以还原事件的真实情况，在对于威胁的细粒度分析中具有关键价值。内部行为日志威胁分析的难点主要包括以下3个方面：

1）多源异构数据融合。数据质量低的问题主要源自企业内部设备环境复杂、系统版本杂乱。在企业中，员工工作场景下所使用的设备多种多样，连接内网服务器的方式也较为灵活，不利于记录员工个人主机的行为数据以及内网服务器操作数据。除了员工个人设备直连服务器主机外，由于涉密或者数据保护的需要，部分企业采用审计系统实现服务器访问认证的3A原则[98]管控员工的资源登录认证过程，但认证的安全性与记录操作行为的简便性存在一定负相关关系，越安全的系统可能越复杂，复杂系统不利于便捷记录员工的操作行为。

2）用户与实体行为序列的上下文关联。用户的某一行为不是孤立存在的，而是需要根据上下文行为确定该行为属性。如果一次攻击样本呈现带有时序性的攻击序列状态，那么在对用户行为分析时也需要确定一个事件窗口。用户行为被事件窗口切割后，会保留一条完整的证据链，从开始尝试入侵到入侵结束的一系列行为都应该被包含在事件窗口中，而实际环境下很难判断威胁行为开始的时间。

3）用户与实体行为类别标签。用户在操作过程中，系统难以通过动作判断其行为属性，因此样本标签较少。无论是二分类问题还是多分类问题，样本标签的质量都直接影响分类结果的优劣。无监督数据意味着用于异常行为识别的可选模型较少，很难在模型端进行改进。

6.2　外部入侵检测的局限性

近几年互联网高速发展，网络技术水平也不断提高，企业的网络安全意识不断完善。外部威胁包括黑客攻击、病毒入侵、安全漏洞等方面。目前，外部威胁分析的难点主要包括以下3个方面：

1）监控手段单一、设备智能化程度不够。IDS、

IPS、WAF、网络探针等各类网络安全设备在实际企业的网络安全外部威胁防御中占有重要比重，但其中的多数通过网络安全策略对流量数据进行管控，安全策略采用规则匹配方式对流量进行处理，检测效果有限，规则更新滞后。

2）数据量大。科技发展迅猛，网络设备无论是数量上还是质量上都突飞猛进，单位时间内产出的各种网络设备、流量等日志呈现指数增长趋势。越来越多的流量数据在硬盘内大量堆积，无论是在线处理还是离线分析都会占用大量的计算资源。数据量大也会导致分析时间的增加，检测结果更为滞后，系统暴露在风险下的时间更长。

3）样本数据分布不平衡。在模型训练过程中，很多算法通常有数据均匀分布这样一个基本假设。少量攻击流量数据掺杂在大量正常数据中，如果采取正常模型训练模式，则可能会导致不准确的模型结果。在样本较少的情况下，尽管也能从中学习到相应的检测规则，但结果可能会存在一定的过拟合现象，仅针对某些场景有效果，缺少普适性，难以应对未知威胁。

6.3 UEBA技术的发展方向

UEBA作为人工智能产业在网络安全领域的应用之一，具有广阔的发展前景。从发展趋势来看，在早期研究中，以数据集扩充、实验扩充和增加模型能够识别的威胁行为种类为主，更加注重从数据量、威胁类型等方面对模型进行优化。在中期研究中，学者们开始考虑模型性能与系统的运行效率，积极优化模型检测速度。在近期研究中，学者们更加注重检测质量，准备通过特征优化、检测过程可视化等方式对模型进行改进。总体而言，整个UEBA研究重点具有明显的“分析数量-分析速度-分析质量”发展趋向。

UEBA技术与各行各业深度融合的同时，也暴露出一定的缺陷。典型异常检测算法的对比分析如表7所示。

表7 典型异常检测算法对比

Table 7 Comparison of typical anomaly detection algorithms

异常检测类型	异常检测算法	算法描述	优势	劣势
有监督统计学习	特征匹配[35]、加权特征计算[36]	最简单的异常检测算法，根据某些检测逻辑对数据进行匹配或者对特征赋予权重并进行异常值计算	算法简单，训练速度快，根据异常规则进行识别的准确率较高	检测逻辑固定，不具备检测未知威胁的能力
有监督统计学习	KNN[42]	代表性分类算法，通过计算样本间的相似程度进行分类	检测逻辑简单，能够发挥数据标签的作用，适合增量式训练，便于模型移植	事先设置的超参数K对数据分类结果的影响很大
有监督统计学习	SVM[46]	有严谨的数学推导过程，分类效果较好，在产业界被广泛应用	在高维数据中有良好的表现，对非线性数据也可以进行较好处理	为二分类算法，需要结合其他算法才能完成多分类任务，且时间复杂度高，核函数选取难
无监督统计学习	K-Means[46]	基于欧式距离的聚类算法，两个目标的欧式距离越小，相似度越大	实现简单，收敛速度快，聚类效果好	K值难以确定，在非凸数据上表现较差，对异常值敏感，易达到局部最优
无监督统计学习	DBSCAN[49]	基于某一邻域内的密度进行聚类，通过不断扩张核心区域完成聚类构建	可以自动确定聚类个数，发现任意形状的聚类，过滤噪声数据点	缺乏高维数据的检测能力，全局参数不一定适合每个类别，训练速度慢
半监督统计学习	半监督K-Means[57]	基于已知数据的标签建立学习器，对未标记样本进行标注	解决了样本标签匮乏的问题，更适合应用于产业界	已有标签质量会极大影响模型预测效果
自编码器	深度自编码器[62]	基于反向传播算法与最优化方法实现，目的是学习一种数据间的映射关系	可以通过模型叠加使用的方式对数据进行降维，解决了数据维度过高的问题	对噪声值比较敏感，在异常检测任务中需要保证训练数据均为正常样本
多层感知器	AdaBoost+MLP[65]	结构简单的全连接网络，可以使用多种激活函数进行数据的非线性处理	结构简单，快速地解决了非线性划分问题	容易过拟合，可调试的参数过多，随着层数的增多梯度消失现象严重
卷积神经网络	CNN[68]	通过设计好的卷积核对图像进行处理，可以使用多种网络结构组合构建深度网络	快速处理高维数据，自动进行特征提取，能够保留原始图像在结构上的关系	池化过程可能丢失数据信息，容易陷入局部收敛
循环神经网络	LSTM[73]	解决了长序列训练过程中的梯度消失和爆炸问题，比普通的RNN表现效果更好	能够处理带有时序属性的数据，gate单元使得该网络可以长期保存信息	并行能力有所欠缺，结构复杂导致运行速度较慢
生成式对抗网络	GAN[79]	通过学习真实数据分布来生成假的数据，生成模型与判别模型的博弈过程会使生成数据更真实	尤其解决了异常检测中数据分布不平衡的问题，训练过程对样本标签的要求较低，能够进行无监督和半监督训练	难以判断何时达到生成模型与判别模型的均衡，容易陷入梯度消失和局部最优问题

当前研究方法的缺陷主要集中在:1)易陷入局部最优;2)标签质量对结果的影响大;3)噪声数据对结果的影响大;4)未知行为判断不足。缺陷1不仅出现在UEBA领域,在整个计算机行业内都是如此,模型陷入局部最优可能在健壮性与检测准确度方面均表现不佳。缺陷2和缺陷3主要涉及数据质量问题,需要对原始数据进行处理。针对缺陷4应增加模型泛化能力,保证其更好地学习到异常行为规律。

考虑到UEBA的发展趋势以及当前存在的缺陷,将针对以下问题做进一步研究:

1)未知威胁识别问题。根据先验知识建立威胁识别模型,一般在面对未知异常行为时的表现性能不佳,而未知威胁给系统带来的潜在风险更为突出,因此未来将建立面向未知威胁的异常检测算法。

2)数据有偏问题。无论是内部风险还是外部威胁,往往是少量异常样本掺杂在大量正常样本中,很多算法极易受到有偏样本分布的影响,因此未来将解决数据有偏分布问题,建立适应性更强的UEBA方法。

3)行为序列划分问题。在现有行为数据的分析模型中,很多模型利用时间、会话ID等属性进行硬划分。这种划分方法在时间维度上割裂了异常事件的前后关联,不利于威胁链条的完整呈现。因此,未来将解决行为序列的划分问题,在保证其时序性完整的同时,避免多序列划分可能带来的算法复杂度增加问题。

4)局部最优问题。在异常检测任务中,陷入局部最优意味着判别模型的准确率较低,对于流量数据的错误判断会对正常业务产生极大影响。因此,未来将建立收敛于全局最优的异常检测模型,以获得更加准确的预测效果。

7 结束语

本文阐述基于机器学习的UEBA技术研究进展,对统计学习、深度学习、强化学习中的典型算法进行对比分析,介绍被广泛使用的经典数据集并讨论如何通过特征工程手段生成新的可利用特征,随后分析UEBA技术在数据处理、行为关联、类别确定、智能分析等方面的局限性和需要解决的问题,从使用方法、算法性能、关键技术等角度出发对典型异常检测方法的优劣势进行归纳总结。由于网络规模的不断扩大,设备类型多样化、数据类型复杂化使得机器学习模型在用户与实体行为分析领域的应用范围越来越广,结合的紧密程度也逐步加深。尽管现有UEBA技术在实际异常检测中取得了较好的效果,但在攻击行为全过程解析方面还存在不足,多数分析方法只能找到异常点而不能找出异常序列,但有些持续性威胁并非只在某一点产生异常,必须通过完整的行为链条进行判断,并且随着网络技术发展加快,攻击技术在越来越趋于隐蔽的同时,也呈现出多样化态势。因此,在日趋复杂的安全形势、不断进化的攻击手段等背景下,后续将针对未知威胁识别、入侵事件还原等问题对用户与实体行为分析技术进行更深入的研究,进一步提高用户与实体行为分析模型的处理效率与检测质量。

参考文献

[1] CHANG L, CHEN W, HUANG J B, et al. Exploiting multi-attention network with contextual influence for point-of-interest recommendation[J]. Applied Intelligence, 2021, 51(4): 1904-1917.

[2] ALHIJAWI B, AL-NAYMAT G, OBEID N, et al. Novel predictive model to improve the accuracy of collaborative filtering recommender systems[J]. Information Systems, 2021, 96: 1-30.

[3] ZHU X, LIU H, LEI Z, et al. Large-scale bisample learning on ID vs. spot face recognition[J]. International Journal of Computer Vision, 2019, 127(6): 684-700.

[4] MURALIDHARAN A, MOSTOFI Y. Path planning for minimizing the expected cost until success[J]. IEEE Transactions on Robotics, 2019, 35(2): 466-481.

[5] JAGIELSKI M, OPREA A, BIGGIO B, et al. Manipulating machine learning: poisoning attacks and countermeasures for regression learning[C]//Proceedings of 2018 IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2018: 19-35.

[6] BÉCUE A, PRAÇA I, GAMA J. Artificial intelligence, cyber-threats and industry 4.0: challenges and opportunities[J]. Artificial Intelligence Review, 2021, 54(5): 3849-3886.

[7] KAUR H, PANNU H S, MALHI A K. A systematic review on imbalanced data challenges in machine learning[J]. ACM Computing Surveys, 2019, 52(4): 1-36.

[8] SINGH K, SINGH P, KUMAR K. User behavior analytics-based classification of application layer HTTP-GET flood attacks[J]. Journal of Network and Computer Applications, 2018, 112: 97-114.

[9] SHASHANKA M, SHEN M Y, WANG J S. User and entity behavior analytics for enterprise security[C]//Proceedings of 2016 IEEE International Conference on Big Data. Washington D. C., USA: IEEE Press, 2016: 1867-1874.

[10] ALEXEY L, MIKHAIL P, ANATOLIY B. Scalable data processing approach and anomaly detection method for user and entity behavior analytics platform[C]//Proceedings of 2020 International Symposium on Intelligent and Distributed Computing. Berlin, Germany: Springer, 2020: 344-349.

[11] GUPTA R, TANWAR S, TYAGI S, et al. Machine learning models for secure data analytics: a taxonomy and threat model[J]. Computer Communications, 2020, 153: 406-440.
[12] 文雨, 王伟平, 孟丹. 面向内部威胁检测的用户跨域行为模式挖掘[J]. 计算机学报, 2016, 39(8): 1555-1569.
WEN Y, WANG W P, MENG D. Mining user cross-domain behavior patterns for insider threat detection[J]. Chinese Journal of Computers, 2016, 39(8): 1555-1569. (in Chinese)
[13] 李志, 宋礼鹏. 基于用户窗口行为的内部威胁检测研究[J]. 计算机工程, 2020, 46(4): 135-142, 150.
LI Z, SONG L P. Research on internal threat detection based on user window behavior[J]. Computer Engineering, 2020, 46(4): 135-142, 150. (in Chinese)
[14] YANG A M, LIU C S, LI J, et al. Design of intrusion detection system for Internet of Things based on improved BP neural network[J]. IEEE Access, 2019, 7: 106043-106052.
[15] AHMIM A, DERDOUR M, FERRAG M A. An intrusion detection system based on combining probability predictions of a tree of classifiers [J]. International Journal of Communication Systems, 2018, 31(9): 1-17.
[16] BELOUCH M, EL S, IDHAMMAD M. A two-stage classifier approach using RepTree algorithm for network intrusion detection[J]. International Journal of Advanced Computer Science and Applications, 2017, 8(6): 389-394.
[17] SINGH S, YASSINE A. Big data mining of energy time series for behavioral analytics and energy consumption forecasting[J]. Energies, 2018, 11(2): 452.
[18] YU H, ZHANG T, CHEN J, et al. Web items recommendation based on multi-view clustering[C]//Proceedings of the 42nd IEEE Computer Software & Applications Conference. Washington D. C., USA: IEEE Press, 2018: 420-425.
[19] Gartner. Market guide for user and entity behavior analytics [EB/OL]. [2021-08-12]. https://www.gartner.com/en/documents/3134524.
[20] LUNT T F. A survey of intrusion detection techniques[J]. Computers & Security, 1993, 12(4): 405-418.
[21] LUNT T F, JAGANNATHAN R. A prototype real-time intrusion-detection expert system[C]//Proceedings of 1988 IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 1988: 59-66.
[22] HOGLUND G W, VALCARCE E M. The "ESSENSE" of intrusion detection: a knowledge-based approach to security monitoring and control[C]//Proceedings of the 7th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems. New York, USA: ACM Press, 1994: 201-209.
[23] KHAN M A, ABUHASEL K A. An evolutionary multi-hidden Markov model for intelligent threat sensing in industrial Internet of Things [J]. The Journal of Supercomputing, 2021, 77(6): 6236-6250.
[24] ZHANG G, YIN J, LIANG Z H, et al. Prior knowledge SVM-based intrusion detection framework[C]//Proceedings of the 3rd International Conference on Natural Computation. Washington D. C., USA: IEEE Press, 2007: 489-493.
[25] LEWICKI A, PANCERZ K. Ant-based clustering for flow graph mining [J]. International Journal of Applied Mathematics and Computer Science, 2020, 30(2): 561-572.
[26] MIAH S J, VU H Q, GAMMACK J, et al. A big data analytics method for tourist behaviour analysis [J]. Information & Management, 2017, 54(6): 771-785.
[27] WANG K, ZHENG H, LOURI A. TSA-NoC: learning-based threat detection and mitigation for secure network-on-chip architecture[J]. IEEE Micro, 2020, 40(5): 56-63.
[28] XU S J, QIAN Y, HU R Q. Edge intelligence assisted gateway defense in cyber security[J]. IEEE Network, 2020, 34(4): 14-19.
[29] RAHUL-VIGNESWARAN K, POORNACHANDRAN P, SOMAN K P. A compendium on network and host based intrusion detection systems[C]//Proceedings of International Conference on Data Science, Machine Learning and Applications. Berlin, Germany: Springer, 2019: 23-30.
[30] 李航. 统计学习方法[M]. 北京: 清华大学出版社, 2012.
LI H. Statistical learning method[M]. Beijing: Tsinghua University Press, 2012. (in Chinese)
[31] SUABOOT J, FAHAD A, TARI Z, et al. A taxonomy of supervised learning for IDSs in SCADA environments[J]. ACM Computing Surveys, 2020, 53(2): 1-37.
[32] PICCIALLI F, CASOLLA G, CUOMO S, et al. Decision making in IoT environment through unsupervised learning[J]. IEEE Intelligent Systems, 2020, 35(1): 27-35.
[33] VILLA-PÉREZ M E, ÁLVAREZ-CARMONA M Á, LOYOLA-GONZÁLEZ O, et al. Semi-supervised anomaly detection algorithms: a comparative summary and future research directions[J]. Knowledge-Based Systems, 2021, 218: 1-18.
[34] GARCÍA S, LUENGO J, SÁEZ J A, et al. A survey of discretization techniques: taxonomy and empirical analysis in supervised learning[J]. IEEE Transactions on Knowledge and Data Engineering, 2013, 25(4): 734-750.
[35] KEMALIS K, TZOURAMANIS T. SQL-IDS: a specification-based approach for SQL-injection detection[C]//Proceedings of 2008 ACM Symposium on Applied Computing. New York, USA: ACM Press, 2008: 2153-2158.
[36] GU Y P, YU X, GUO K X, et al. Detection, estimation, and compensation of false data injection attack for UAVs[J]. Information Sciences, 2021, 546: 723-741.
[37] BRONTE R, SHAHRIAR H, HADDAD H M. A signature-based intrusion detection system for Web applications based on genetic algorithm[C]//Proceedings of the 9th International Conference on Security of Information and Networks. New York, USA: ACM Press, 2016: 32-39.
[38] GARCÍA-TEODORO P, DÍAZ-VERDEJO J. Anomaly-based network intrusion detection: techniques, systems and challenges[J]. Computers & Security, 2009, 28(1/2): 18-28.
[39] HUTCHINS R, ZEGURA E W, LIASHENKO A, et al. Internet user access via dial-up networks-traffic characterization and statistics[C]//Proceedings the 9th International Conference on Network Protocols. Washington D. C., USA: IEEE Press, 2001: 314-322.
[40] KIM M. Network traffic prediction based on INGARCH model[J]. Wireless Networks, 2020, 26(8): 6189-6202.
[41] DI GESU V, LO BOSCO G, FRIEDMAN J H. Intruders pattern identification[C]//Proceedings of the 19th International Conference on Pattern Recognition. Washington D. C., USA: IEEE Press, 2008: 1-4.

[42] SANDOSH S, GOVINDASAMY V, AKILA G. Enhanced intrusion detection system via Agent clustering and classification based on outlier detection[J]. Peer-to-Peer Networking and Applications, 2020, 13(3): 1038-1045.

[43] LU C W, SHI J P, WANG W M, et al. Fast abnormal event detection[J]. International Journal of Computer Vision, 2019, 127(8): 993-1011.

[44] SU C, CAO J. Improving lazy decision tree for imbalanced classification by using skew-insensitive criteria[J]. Applied Intelligence, 2019, 49(3): 1127-1145.

[45] SOYSAL M, SCHMIDT E G. Machine learning algorithms for accurate flow-based network traffic classification: evaluation and comparison[J]. Performance Evaluation, 2010, 67(6): 451-467.

[46] AL-YASEEN W L, OTHMAN Z A, NAZRI M Z A. Multi-level hybrid support vector machine and extreme learning machine based on modified K-Means for intrusion detection system[J]. Expert Systems with Applications, 2017, 67: 296-303.

[47] 何发镁,马慧珍,王旭仁,等. 基于特征分组聚类的异常入侵检测系统研究[J]. 计算机工程,2020,46(4):123-128,134.
HE F M, MA H Z, WANG X R, et al. Research on anomaly intrusion detection system based on feature grouping clustering[J]. Computer Engineering, 2020, 46(4): 123-128, 134. (in Chinese)

[48] CHEN Y W, TANG S Y, BOUGUILA N, et al. A fast clustering algorithm based on pruning unnecessary distance computations in DBSCAN for high-dimensional data[J]. Pattern Recognition, 2018, 83: 375-387.

[49] TANG D, ZHANG S Q, CHEN J W, et al. The detection of low-rate DoS attacks using the SADBSCAN algorithm[J]. Information Sciences, 2021, 565: 229-247.

[50] BIAN Z K, CHUNG F L, WANG S T. Fuzzy density peaks clustering[J]. IEEE Transactions on Fuzzy Systems, 2021, 29(7): 1725-1738.

[51] RONAO C A, CHO S B. Mining SQL queries to detect anomalous database access using random forest and PCA[C]// Proceedings of International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems. Berlin, Germany: Springer, 2015: 151-160.

[52] 王晓东,赵一宁,肖海力,等. 多节点系统异常日志流量模式检测方法[J]. 软件学报,2020,31(10):3295-3308.
WANG X D, ZHAO Y N, XIAO H L, et al. Multi-node system abnormal log flow mode detection method[J]. Journal of Software, 2020, 31(10): 3295-3308. (in Chinese)

[53] ZHU X J, GOLDBERG A B. Introduction to semi-supervised learning[J]. Synthesis Lectures on Artificial Intelligence and Machine Learning, 2009, 3(1): 1-6.

[54] 李杰铃,张浩. 半监督异常流量检测研究综述[J]. 小型微型计算机系统,2020,41(11):2371-2379.
LI J L, ZHANG H. Survey on semi-supervised anomaly traffic detection[J]. Journal of Chinese Computer Systems, 2020, 41(11): 2371-2379. (in Chinese)

[55] TAHA A, HADI A S. Anomaly detection methods for categorical data[J]. ACM Computing Surveys, 2019, 52(2): 1-35.

[56] IDHAMMAD M, AFDEL K, BELOUCH M. Semi-supervised machine learning approach for DDoS detection[J]. Applied Intelligence, 2018, 48(10): 3193-3208.

[57] GU Y H, LI K Y, GUO Z Y, et al. Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm[J]. IEEE Access, 2019, 7: 64351-64365.

[58] LIU Y, XU Z, LI C G. Online semi-supervised support vector machine[J]. Information Sciences, 2018, 439: 125-141.

[59] GUO H J, ZOU H, TAN J Y. Semi-supervised dimensionality reduction via sparse locality preserving projection[J]. Applied Intelligence, 2020, 50(4): 1222-1232.

[60] DE VRIES S, THIERENS D. A reliable ensemble based approach to semi-supervised learning[J]. Knowledge-Based Systems, 2021, 215: 106-121.

[61] SUN J Y, WANG X Z, XIONG N X, et al. Learning sparse representation with variational auto-encoder for anomaly detection[J]. IEEE Access, 2018, 6: 33353-33361.

[62] ZHOU C, PAFFENROTH R C. Anomaly detection with robust deep autoencoders[C]//Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York, USA: ACM Press, 2017: 23-40.

[63] CAO V L, NICOLAU M, MCDERMOTT J. A hybrid autoencoder and density estimation model for anomaly detection[C]//Proceedings of 2016 International Conference on Parallel Problem Solving from Nature. Berlin, Germany: Springer, 2016: 717-726.

[64] ROY S S, MALLIK A, GULATI R, et al. A deep learning based artificial neural network approach for intrusion detection[C]// Proceedings of 2017 International Conference on Mathematics and Computing. Berlin, Germany: Springer, 2017: 44-53.

[65] SAFARA F, SOURI A, SERRIZADEH M. Improved intrusion detection method for communication networks using association rule mining and artificial neural networks[J]. IET Communications, 2020, 14(7): 1192-1197.

[66] WANG W, ZHU M, ZENG X W, et al. Malware traffic classification using convolutional neural network for representation learning [C]//Proceedings of 2017 International Conference on Information Networking. Washington D. C., USA: IEEE Press, 2017: 712-717.

[67] PRIYANGA S P, KRITHIVASAN K, S P, et al. Detection of cyberattacks in industrial control systems using Enhanced Principal Component Analysis and Hypergraph-based Convolution Neural Network(EPCA-HG-CNN)[J]. IEEE Transactions on Industry Applications, 2020, 56(4): 4394-4404.

[68] HU Y B, ZHANG D H, CAO G Y, et al. Network data analysis and anomaly detection using CNN technique for industrial control systems security[C]//Proceedings of 2019 IEEE International Conference on Systems, Man and Cybernetics. Washington D. C., USA: IEEE Press, 2019: 593-597.

[69] 李峰,舒斐,李明轩,等. 基于深度学习的Linux远控木马检测[J]. 计算机工程,2020,46(7):159-164.
LI F, SHU F, LI M X, et al. Detection of remote access trojan in Linux based on deep learning[J]. Computer Engineering, 2020, 46(7): 159-164. (in Chinese)

[70] 徐洪平,马泽文,易航,等. 基于卷积循环神经网络的网络流量异常检测技术[J]. 信息网络安全,2021,21(7):54-62.
XU H P,MA Z W,YI H,et al. Network traffic anomaly detection technology based on convolutional recurrent neural network[J]. Netinfo Security,2021,21(7):54-62. (in Chinese)
[71] LIU H Y,LANG B,LIU M,et al. CNN and RNN based payload classification methods for attack detection[J]. Knowledge-Based Systems,2019,163:332-341.
[72] MANICKAM M,RAMARAJ N,CHELLAPPAN C. A combined PFCM and recurrent neural network-based intrusion detection system for cloud environment[J]. International Journal of Business Intelligence and Data Mining,2019,14(4):504-527.
[73] 麻文刚,张亚东,郭进. 基于LSTM与改进残差网络优化的异常流量检测方法[J]. 通信学报,2021,42(5):23-40.
MA W G,ZHANG Y D,GUO J. Abnormal traffic detection method based on LSTM and improved residual neural network optimization[J]. Journal on Communications,2021,42(5):23-40. (in Chinese)
[74] GOODFELLOW I,POUGET-ABADIE J,MIRZA M,et al. Generative adversarial networks[J]. Communications of the ACM,2020,63(11):139-144.
[75] ZHUO Y,GE Z Q. Gaussian discriminative analysis aided GAN for imbalanced big data augmentation and fault classification[J]. Journal of Process Control,2020,92:271-287.
[76] USAMA M,ASIM M,LATIF S,et al. Generative adversarial networks for launching and thwarting adversarial attacks on network intrusion detection systems[C]//Proceedings of the 15th International Wireless Communications & Mobile Computing Conference. Washington D. C.,USA:IEEE Press,2019:78-83.
[77] 席亮,刘涵,樊好义,等. 基于深度对抗学习潜在表示分布的异常检测模型[J]. 电子学报,2021,49(7):1257-1265.
XI L,LIU H,FAN H Y,et al. Deep adversarial learning latent representation distribution model for anomaly detection[J]. Acta Electronica Sinica,2021,49(7):1257-1265. (in Chinese)
[78] ZHANG X Q,ZHOU Y,PEI S W,et al. Adversarial examples detection for XSS attacks based on generative adversarial networks[J]. IEEE Access,2020,8:10989-10996.
[79] ZHANG X. Network intrusion detection using generative adversarial networks[D]. Christchurch,New Zealand:University of Canterbury,2020.
[80] BARTO A G. Reinforcement learning:connections,surprises,and challenge[J]. AI Magazine,2019,40(1):3-15.
[81] NGUYEN T T,NGUYEN N D,NAHAVANDI S. Deep reinforcement learning for multiagent systems:a review of challenges,solutions,and applications[J]. IEEE Transactions on Cybernetics,2020,50(9):3826-3839.
[82] DEMONTIS A,MELIS M,BIGGIO B,et al. Yes,machine learning can be more secure! A case study on android malware detection[J]. IEEE Transactions on Dependable and Secure Computing,2019,16(4):711-724.
[83] 高洋,王礼伟,任望,等. 基于强化学习的工控系统恶意软件行为检测方法[J]. 工程科学学报,2020,42(4):455-462.
GAO Y,WANG L W,REN W,et al. Reinforcement learning-based detection method for malware behavior in industrial control systems[J]. Chinese Journal of Engineering,2020,42(4):455-462. (in Chinese)
[84] XIAO L,XU D J,MANDAYAM N B,et al. Attacker-centric view of a detection game against advanced persistent threats[J]. IEEE Transactions on Mobile Computing,2018,17(11):2512-2523.
[85] XIAO L,DING Y Z,JIANG D H,et al. A reinforcement learning and blockchain-based trust mechanism for edge networks[J]. IEEE Transactions on Communications,2020,68(9):5460-5470.
[86] CHEN Y,HUANG S W,LIU F,et al. Evaluation of reinforcement learning-based false data injection attack to automatic voltage control[J]. IEEE Transactions on Smart Grid,2019,10(2):2158-2169.
[87] University of California. KDD CUP 1999 data[EB/OL]. [2021-08-12]. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.
[88] MIT Lincoln Laboratory. 1998 DARPA intrusion detection evaluation dataset[EB/OL]. [2021-08-12]. http://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset.
[89] MIT Lincoln Laboratory. 1999 DARPA intrusion detection evaluation dataset[EB/OL]. [2021-08-12]. http://www.ll.mit.edu/r-d/datasets/1999-darpa-intrusion-detection-evaluation-dataset.
[90] MIT Lincoln Laboratory. 2000 DARPA intrusion detection scenario specific datasets[EB/OL]. [2021-08-12]. http://www.ll.mit.edu/r-d/datasets/2000-darpa-intrusion-detection-scenario-specific-datasets.
[91] Canadian Institute for Cybersecurity. NSL-KDD datasets [EB/OL]. [2021-08-12]. https://www.unb.ca/cic/datasets/nsl.html.
[92] University of New South Wales. The UNSW-NB15 dataset [EB/OL]. [2021-08-12]. https://research.unsw.edu.au/projects/unsw-nb15-dataset.
[93] Canadian Institute for Cybersecurity. Intrusion detection evaluation dataset(CIC-IDS2017) [EB/OL]. [2021-08-12]. https://www.unb.ca/cic/datasets/ids-2017.html.
[94] Canadian Institute for Cybersecurity. IDS 2012 datasets[EB/OL]. [2021-08-12]. https://www.unb.ca/cic/datasets/ids.html.
[95] Canadian Institute for Cybersecurity. IDS 2018 datasets[EB/OL]. [2021-08-12]. https://www.unb.ca/cic/datasets/ids-2018.html.
[96] Canadian Institute for Cybersecurity. Datasets research[EB/OL]. [2021-08-12]. https://www.unb.ca/cic/datasets/index.html.
[97] DUMOUCHEL W,JU W H,KARR A F,et al. Computer intrusion:detecting masquerades[J]. Statistical Science,2001,16(1):58-74.
[98] LAMPSON B W. Computer security in the real world[J]. Computer,2004,37(6):37-46.

编辑 陆燕菲