深度学习异常检测方法综述

预印本

悉尼RaghavendraChalapathy大学资本市场合作研究中心（CMCRC）rcha9612@uni.sydney.edu.au

桑杰·乔拉卡塔尔计算研究院（QCRI），HBKUschawla@qf.org.qa

2019年1月24日

抽象

异常检测是已经充分研究不同的研究领域和应用领域中的一个重要问题。本次调查的目的是双重的，首先我们提出了一个结构化和COM的prehensive的深入研究方法概述学习为基础的异常检测。此外，我们审查通过这些方法异常在各个应用领域，并评估其有效性。我们集合状态的最先进的深异常检测研究技术为基础所采用的基本假设和方法不同的类别。在每个类别中，我们列出了基本的异常检测技术，用它的变体和现在的关键假设沿，正常和异常行为之间的区别。此外，对于每一个类别，我们也呈现优点和局限性，并讨论在实际应用领域的tech-niques的计算复杂度。最后，我们概述面对而采用深异常对现实世界的问题检测技术研究开放问题和挑战。

关键词异常，异常性，新颖性，深度学习

1引言

分析真实世界的数据集时，一个常见的需求是确定哪些情况下为不同的所有其他人站出来。这样的情况下被称为异常，异常检测（也称为离群点检测）的目标是确定在一数据驱动的方式的所有这样的情况下（Chandola等人[2007]）。异常可以通过在数据中的错误造成的，但有时是表示新的，先前未知的，潜在的过程;霍金斯[1980]限定了离群值作为观察该偏离，以便从显著其他观察为，它是由不同的机制产生引起怀疑。在机器学习的更广阔的领域，近年来目睹深层神经网络的增殖，具有在各种应用领域前所未有的效果。深学习是机器学习，通过学习来表示数据作为概念的神经网络的层内的嵌套层级实现良好的性能和灵活性的子集。深学习优于传统机器学习作为数据规模增大，如图1所示。在最近几年，深学习基于异常检测算法变得越来越流行，并已申请了一组不同的如在图2中所示的任务;研究表明，深度学习完全超越了传统的方法（Javaid等人[2016年]，鹏Marculescu[2015年]）。本次调查的目的是双重的，首先我们提出的在深异常检测（DAD）的研究方法，结构化和全面的检讨。此外，我们还讨论通过在各个应用领域DAD方法，并评估其有效性。

2什么是异常？

异常的性质也被称为异常，离经叛道，或在数据挖掘和统计文献离群值（AG-garwal[2013]）。如图3所示，N1和N2是由多数意见，并因此认为是正常数据实例区域中的区域，而区域O3，和数据点O1和O2是它们位于更远离本体的几个数据点数据点，并因此被认为是异常。出现由于几个

的arXiv：1901.03407v2[cs.LG]2019年1月23日

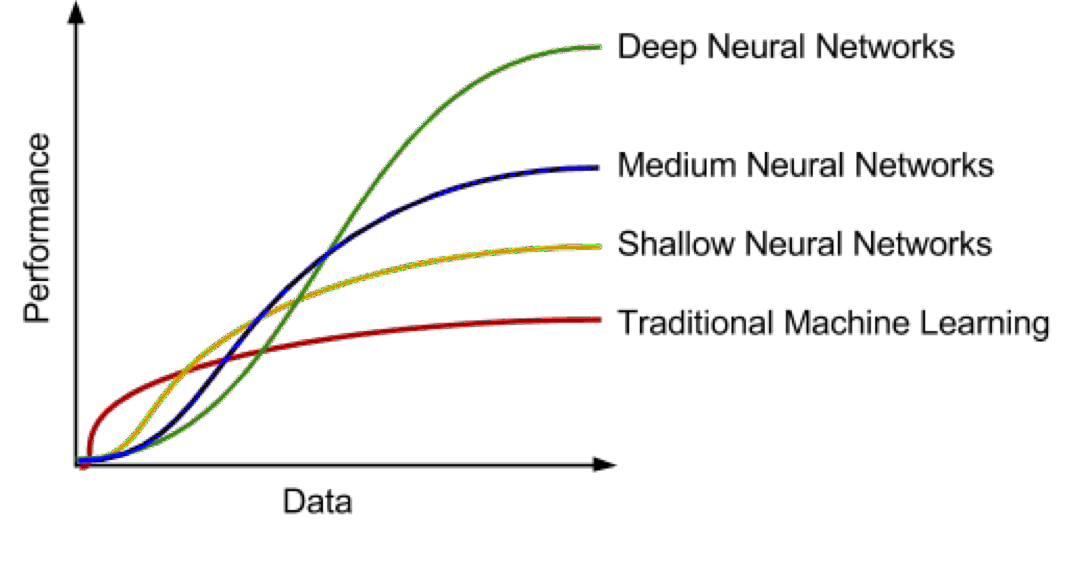


图1：深的性能比较学习算法基于Vs的传统算法的Alejandro[2016]。

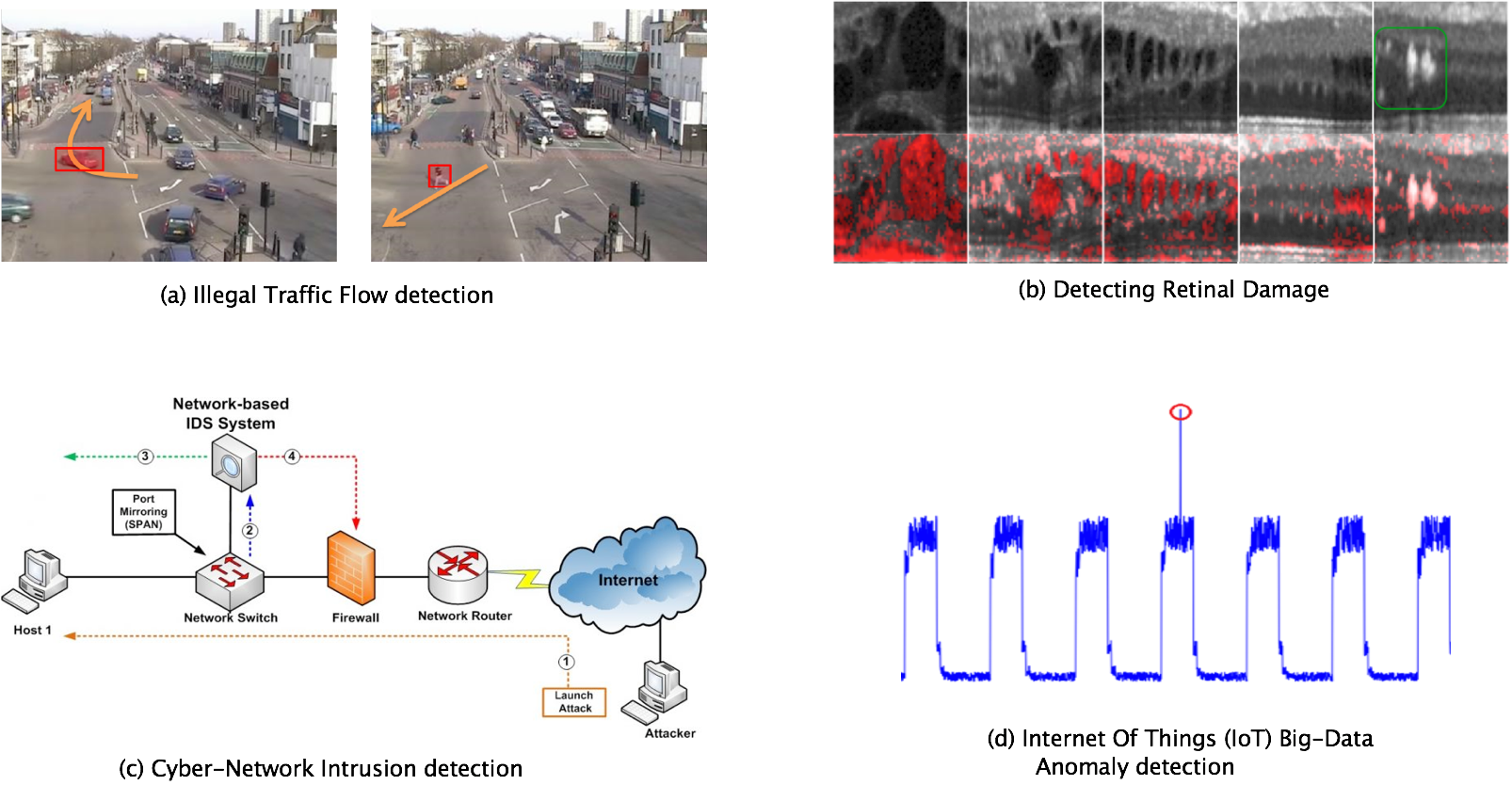


图2：应用的深刻学习，基于异常检测算法。（一）视频监控，图像分析：非法流量的检测谢等人。[2017]，（b）卫生保健：检测视网膜损伤Schlegl等。[2017]（C）网络：网络的入侵检测Javaid等。[2016]（d）传感器网络的事情（IOT）因特网大数据异常检测Mohammadi等人。[2017]

原因，如恶意操作，系统故障，故意的欺诈行为。这些异常现象揭示的数据令人振奋的见解，并经常传达有关数据有价值的信息。因此，异常检测认为是各种决策制度的重要一步。

3什么是新奇？

新颖性检测是一种新型的（新）或不可观测的图案在所述数据的标识（Miljkovi'c[2010]）。检测到不被认为是异常数据点的新奇;相反，他们都被应用到常规的数据模型。甲新颖性分数可被分配给这些以前看不见的数据点，使用判决阈值分数（Pimentel等。[2014]）。从该判定阈值，其显著偏离点可以被认为是异常或异常值。例如，在图4的（白色虎）定期老虎之间的图像可以被认为是一个新事物，而（马，豹，狮子，猎豹）的图像被认为是异常。用于异常检测的技术的通常用于新颖检测，反之亦然。

2

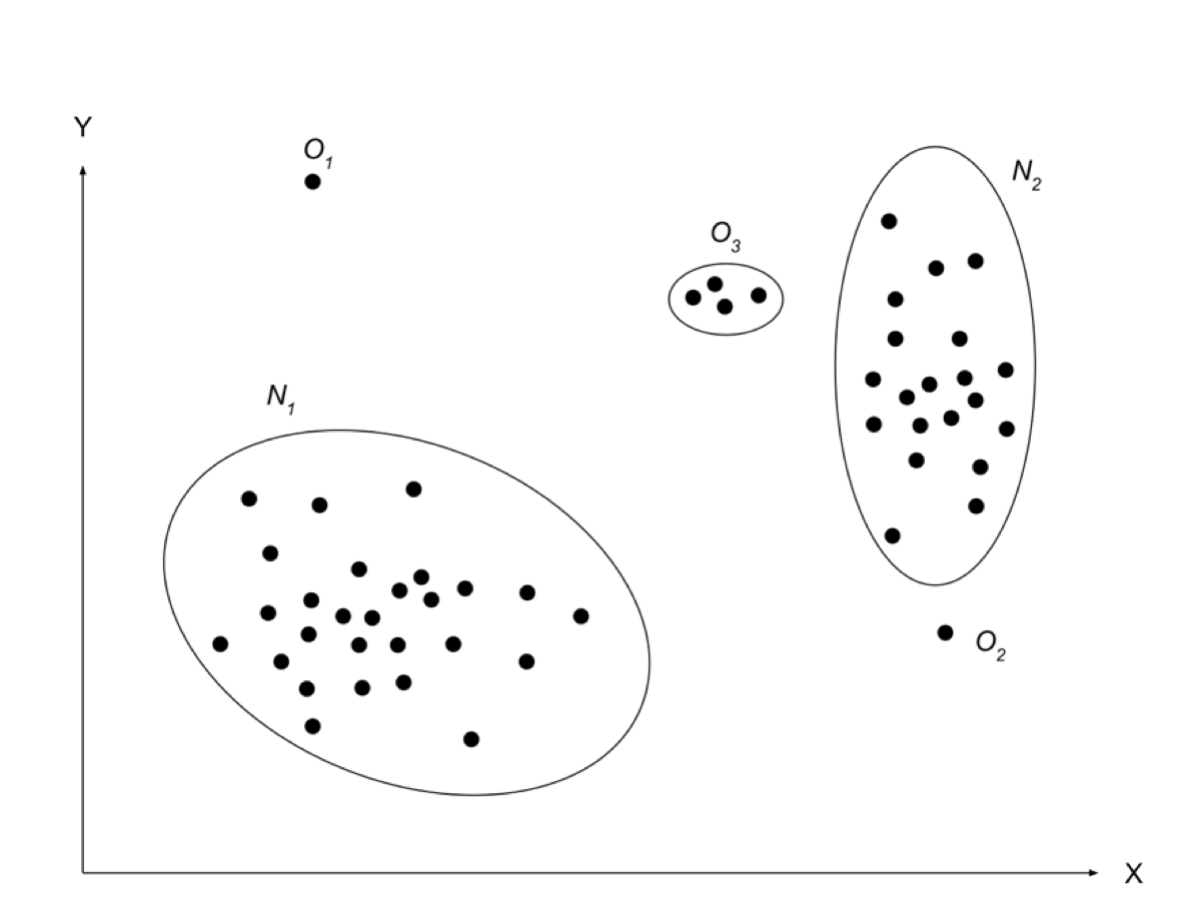


图3：在二维数据组的异常的插图。

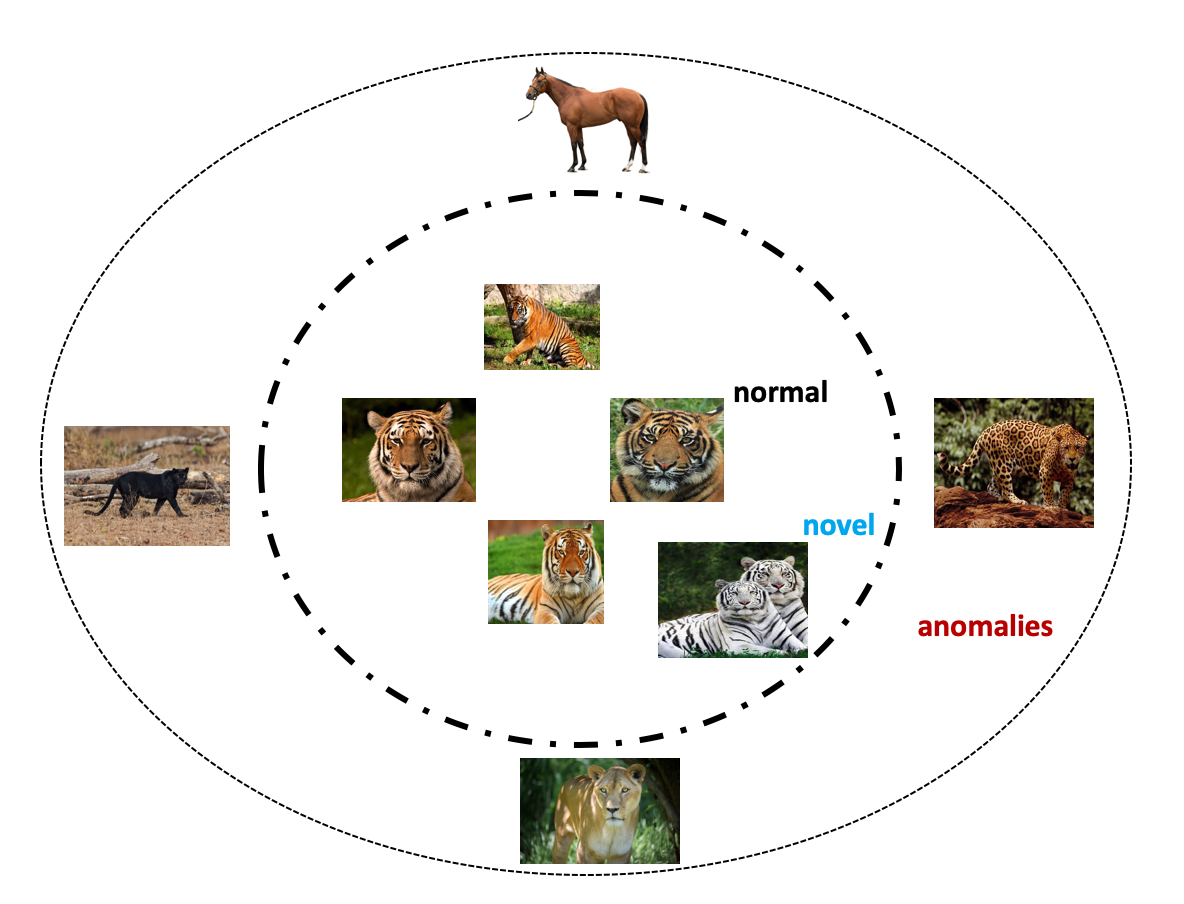


图4：在图像数据集的新颖性的插图。

动机4与挑战：深异常检测（DAD）的技术

的传统算法中检测孤立点•性能是图像（例如医学图像）和数据集序列上次优，因为它未能捕捉复杂的结构在数据中。

•需要大规模的异常检测：随着数据量的增加，让我们说千兆字节的话，它是-来几乎是不可能的传统方法扩展到如此大规模的数据发现异常。

•深度异常检测（DAD）技术学会从数据分层判别特征。此非盟tomatic功能的学习能力消除了开发领域专家手动功能的需要，因此主张解决采取原始输入数据的领域，如文本和语音识别的问题结束到终端。

•正常和异常（错误）的行为之间的边界常常不能精确地在几个数据域定义，并不断发展。这种缺乏明确定义的代表正常的边界姿势的传统和深刻的学习型算法的挑战。

表1：我们的调查，其他相关调查文章的比较。1-我们的调查结果显示，2-Kwon和DonghwoonKwon等。[2017]5-约翰和DerekBall等人。[2017]3-Kiran和Thomas基兰等。[2018]，6-Mohammadi和Al-教法学家Mohammadi等人。[2017]4-Adewumi和洛尼克斯Adewumi和Akinyelu[2017]7-Geert和KOOIet.alLitjens等。[2017]0.1234567

方法

监督✓

无监督✓

混合模式✓

一类神经网络✓

应用

欺诈检测✓✓

网络入侵检测✓✓

医学异常检测✓✓

传感器网络异常检测✓✓

物联网（IOT）大数据异常检测✓✓

登录异常检测✓

视频监控✓✓

工业损伤检测✓

5相关工作

尽管深学习方法在许多机器学习问题方面取得的重大进展，是深度学习的相对稀缺的异常检测方法。Adewumi和Akinyelu[2017年]提供了欺诈检测深基于学习的方法综合性的调查。的深异常检测（DAD）技术的网络的入侵检测的宽综述由Kwon等人提出。[2017]。使用DADtech-早在上世医疗领域的广泛审查由Litjens等人提出。[2017]。对于互联网的DAD技术概述

3

东西（IOT）和大数据异常检测是通过Mohammadi等人提出。[2017]。传感器网络异常检测已经由Ball等人审查。[2017]。的状态的最先进的深学习与各种类别沿着视频异常检测为基础的方法已在吉兰等人提出的。[2018]。虽然在应用DAD技术的一些评论，对异常检测采用深度学习建筑的对比分析的不足。例如，研究对异常检测的大量使用进行了深入自动编码，但缺乏全面调查的各种深架构的最适合给定数据集和appli-阳离子域。我们希望，本次调查填补了这一空白，为研究人员和工程师有志于利用深度学习异常检测一个全面的参考。表1显示了一套由我们的调查所涵盖的研究方法和应用领域。

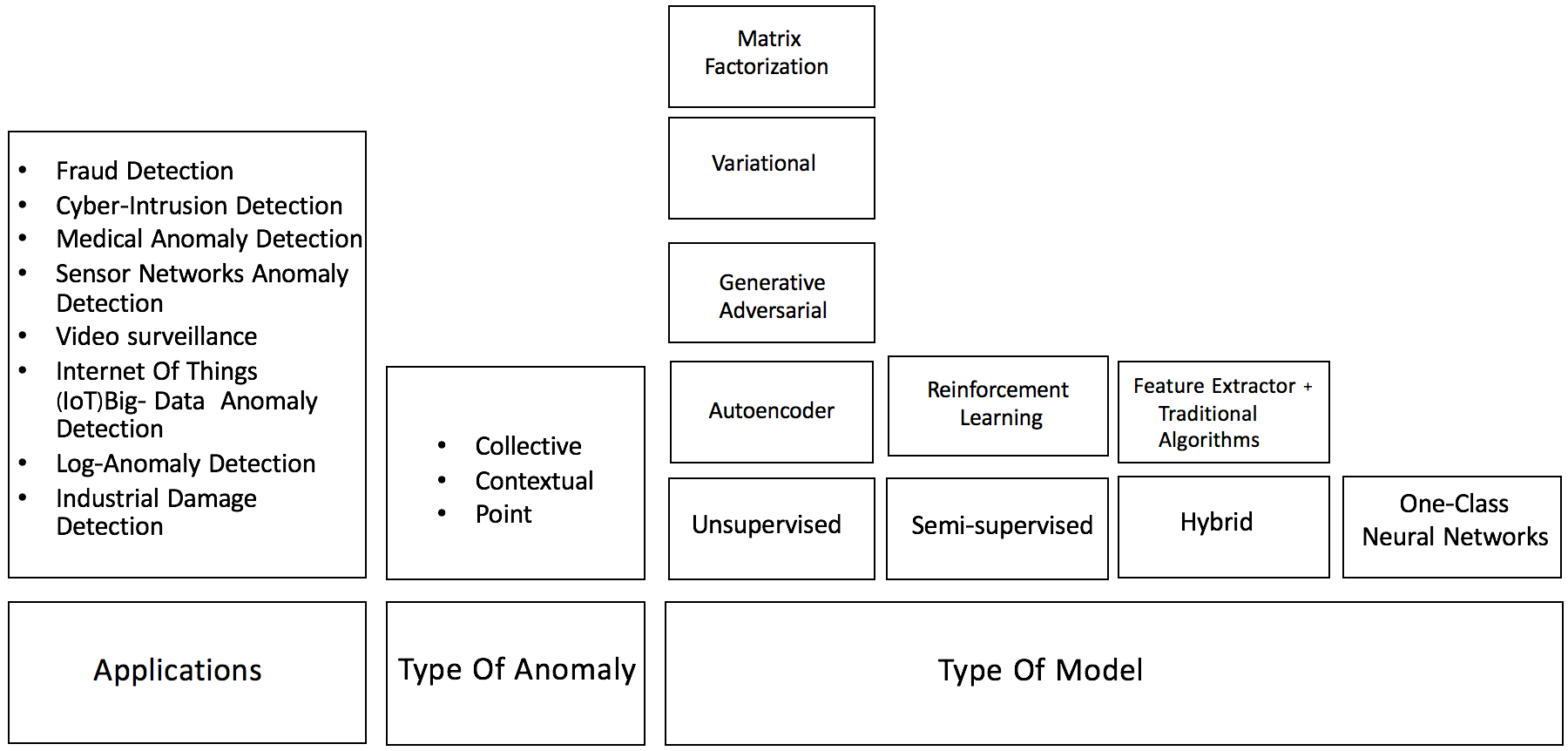


图5：与基于学习深异常检测技术相关联的关键部件。

6点我们的贡献

我们遵循的调查方法（Chandola等人[2007]）深异常检测（DAD）。我们的调查呈现的研究和DAD技术应用的详细介绍和概述结构。我们总结我们的主要contribu-蒸发散如下：

•大多数对一个特定的应用领域或感兴趣的特定研究领域DAD技术要么专注现有的调查（基兰等人[2018]，Mohammadi等人[2017年]，Litjens等人[2017年]，Kwon等人[2017]，Adewumi和Akinyelu[2017]，Ball等人[2017]）。本文旨在提供国家的最先进的研究技术DAD以及一些现实世界的应用这些技术的综合OUT-线呈现。

•近年来一些新的深度学习与基础大大降低可计算性等要求异常检测技术已经开发出来。本文的目的是调查这些技术，并将其划分为一个有组织架构更好的理解。我们引入两个亚类混合国防部-ELS（Erfani等[2016a]）和一类神经网络技术（Chalapathy等[2018A]），如图5中所示根据训练目的的选择。对于每一个类别中，我们讨论这两种假设，并获得最佳性能采用的技术。此外，在每个类别中，我们也提出了挑战，优势和劣势，并提供DAD方法计算复杂的概述。

7组织

本章是通过在图5中第8节中描述以下结构组织的，我们确定确定问题的制剂和突出显示与异常检测相关联的丰富性和复杂性的各种方面。我们引进和定义两种类型的模型：上下文和集体或群体异常。在第9章，我们简要地描述到异常检测已经应用深度学习，基于不同的应用领域。在随后的章节中，我们提供了基于它们所属的研究领域深基于学习的技术分类。基于所使用的培养目标和标签的可用性深学习型异常检测

4

数据实例DAD模型体系结构的类型

顺序

视频，语音

蛋白质序列，时间序列CNN，RNN，LSTM

文本（自然语言）非顺序

图像，传感器之外（数据）CNN，AE和其variantsTable2：输入数据的表示出的性质和相应的深异常在文献中提出的检测模型架构。CNN：卷积神经网络，LSTM：长短期记忆网络AE：自动编码。

技术可以被分类为受监管（第10.1节），无监督（10.5节），混合（第10.3节），以及一类神经网络（第10.4节）。对于技术每个类别我们也讨论他们的计算复杂性训练和测试阶段。在8.4节我们讨论点，情境和集体（集团）深学习，基于异常检测技术。我们目前的局限性进行了一些讨论，并在第12节的各种现有技术的相对性能13包含总结发言。

深学习型异常检测的8个不同的方面。

本节提出并讨论深的不同方面的学习，基于异常检测。

输入数据的性质8.1

在深异常检测方法深层神经网络体系结构的选择主要取决于输入数据的性质。输入的数据可以被宽泛地分类为顺序的（例如，语音，文本，音乐，时间序列，蛋白质序列）或非顺序数据（例如，图像，其他数据）。表2示出的输入数据和在异常检测用深模型体系结构的性质。根据特征（或属性）的数目附加输入的数据可以被进一步分类为低或高维数据。DAD技术已经学习高维原始输入数据内复杂的分层特征关系（LeCun等人[2015]）。在DAD技术中使用的层的数目是由输入数据尺寸驱动，更深的网络显示，以产生高维数据更好的性能。后来，在第10种视为异常检测各种型号在深度审查。

8.2基于可用的标签

标签指示所选择的数据实例是正常还是异常值。异常是罕见的实体，因此它是挑战性，以获得他们的标签。此外，异常行为可能会随时间而改变，例如，的异常性质有这么显著改变，它仍然在马奇水处理厂被忽视，很长一段时间，这导致了1.5亿升未经处理的污水排放到当地水的泄漏（Ramotsoela等人[2018]）。深异常检测（DAD）的模型可以被宽泛地分类为基于标签的availabil-两者均程度三类。（1）监督深异常检测。（2）半监督深异常检测。（3）无监督深异常检测。

8.2.1监督的深层异常检测

监督深异常检测包括培养了深监督二元或多级分类器，使用正常的和异常的数据实例的标签。例如监督DAD车型，配制成在检测罕见的品牌多类分类助剂，违禁药物点名和欺诈性保健事务（Chalapathy等[2016a，b]）。尽管监管DAD方法的改进性能，这些方法都不如流行的半监督或无人监督的方法，由于缺乏标记的训练样本的可用性。此外，深监督分类器的性能使用的异常检测器的次优由于类不平衡（正类实例的总数都远远超过负类数据的总数）。因此，我们不考虑本次调查监督DAD方法的审查。

8.2.2半监督深刻的异常检测

正常情况下的标签是更容易获得比异常，其结果是，半监督DAD技术被广泛采用，这些技术利用现有的单（通常正类）的标签来分离

五

异常值。在异常检测使用深自动编码的一个常用的方法是训练他们在没有异常数据采样的半监督方式。具有足够的训练样本，正常类自动编码的会产生用于正常情况下低重建误差，过异常事件（Wulsin等人[2010]，纳迪姆等人[2016]，Song等人[2017]）。我们认为在10.2节这些方法的详细审查。

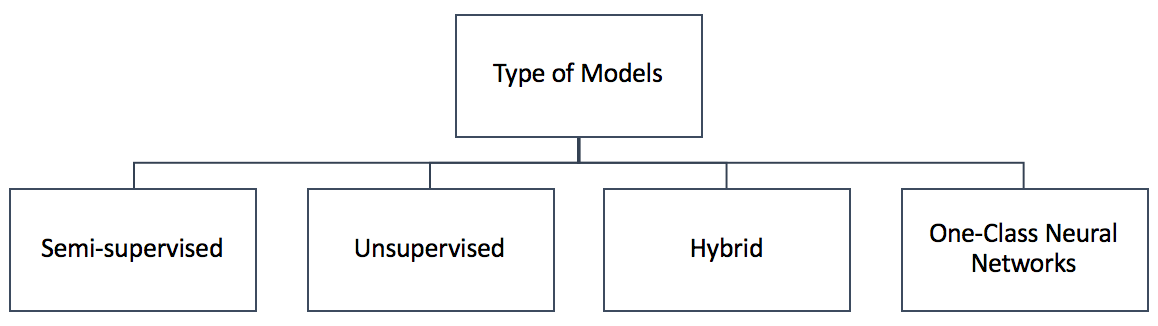


图6：基于深度学习模型的异常检测的类型分类。

8.2.3深无监督异常检测

无监督深异常检测技术检测仅基于数据IN-立场的固有特性的异常值。无监督DAD技术在未标记的数据样本的自动贴标签使用，因为标记的数据是非常困难的获得（帕特森和Gibson[2017]）。无监督DAD模型的变体（Tuor等人[2017]）被证明优于传统的方法如主成分分析（PCA）（Wold的等。[1987]），支持向量机（SVM）科尔特斯和Vapnik等[1995]与隔离森林（Liu等人。[2008]）中的应用领域，例如健康和网络安全技术。自动编码都是无监督DAD模型的核心。这些模型假定不是异常数据实例失败，这将导致较高的假阳性率正常情况下的高发病率。另外无监督学习算法，诸如限制波尔兹曼机（RBM）（Sutskever等人[2009]），深波尔兹曼机（DBM），深信念网络（DBN）（Salakhutdinov和拉罗歇尔[2010]），广义去噪自动编码（Vincent等人[2008]），回归神经网络（RNN）（Rodriguez等。[1999]）长短期存储器网络（Lample等人[2016]），其用于检测离群值中详细11.7节中讨论。

根据培养目标8.3

在本次调查中，我们介绍了深异常检测的两个新类别基于训练objec-表3-6（DAD）技术采用1）深的混合动力车型（DHM）。2）一类神经网络（OC-NN）。

8.3.1深度混合模型（DHM）

深混合模型异常检测使用深层神经网络主要是自动编码为特征提取，特征自动编码的隐藏交涉中得知被输入到传统的异常检测algo-rithms如单类SVM（OC-SVM）来检测异常值（安卓等[2016a]）。图7示出了用于异常检测的深混合模型体系结构。在转移之后学习从模型获得丰富的代表进行功能的成功对大数据集预先训练，混合动力车型也采用这些预先训练转移模型的学习与巨大的成功特征提取（Pan等人[2010]）。混合模型的变体，提出了通过厄根等。[2017]它参考特征提取器的联合培养沿与OC-SVM（或SVDD）目标最大化检测性能。这些混合的一个显着缺点是接近定制异常检测缺乏训练的目标，因此这些模型不能提取富差动功能，以检测离群值。为了克服这种限制异常检测诸如深一类分类定制物镜（拉夫等人[2018A]）和一类神经网络（Chalapathy等[2018A]）被引入。

8.3.2单类神经网络（OC-NN）

一类神经网络（OC-NN）Chalapathy等。[2018A]方法由基于核的一类clas-sification它结合深网络提取的数据的逐步丰富表示与创建周围正常数据的紧包络的一类目标的能力的启发。在OC-NN方法对以下重要原因新的突破：在隐藏层数据表示由OC-NN驱动目标，并且因此

6

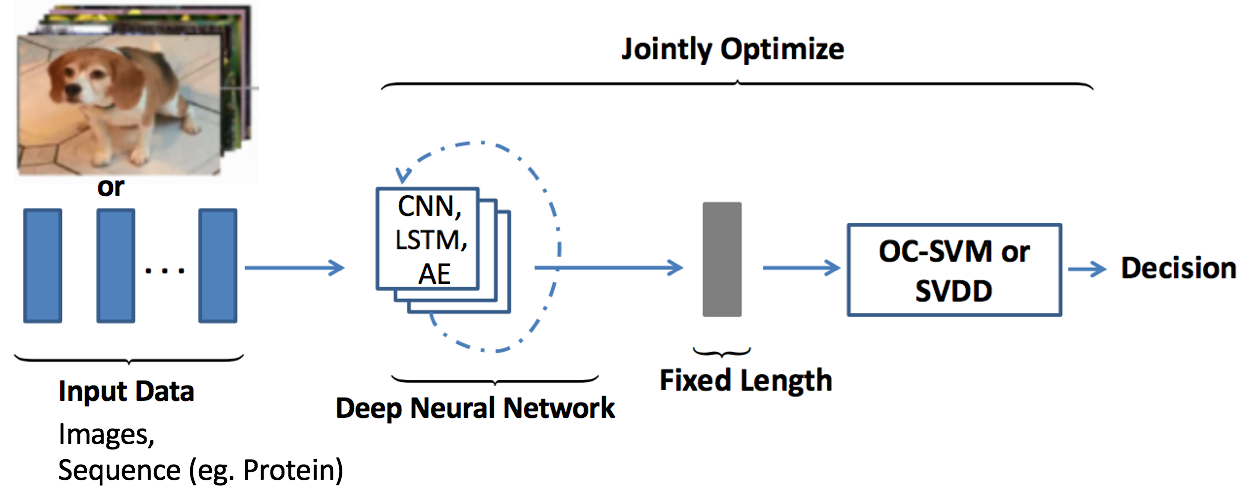


图7：深混合模型架构。

定制的异常检测。这是从深特征使用自动编码，然后进料的特征到像一个类SVM（OC-SVM）一个单独的异常检测方法，其使用学到，ING的混合方法的其它方法的偏离。培训和一类神经网络的评估细节在仲重刑10.4讨论。（深SVDD）一类神经网络结构深支持向量数据描述的另一种变型（拉夫等人[2018A]）列车深神经网络由正常数据实例密切映射到球的中心来提取变化的常见因素，是示为上MNIST生产性能改进（LeCun等人[2010]）和CIFAR-10（Krizhevsky和Hinton的[2009]）的数据集。

8.4类型的异常

异常大致可分为三种类型：点异常，上下文异常和集体异常。深异常检测（DAD）方法已被证明检测所有三类异常的大获成功。

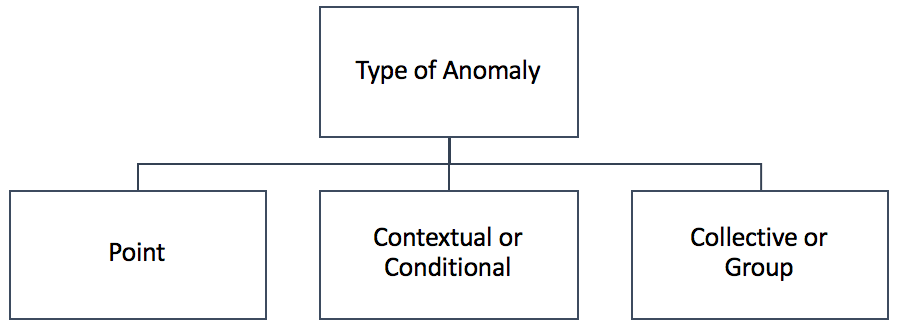


图8：深学习技术分类为基础的的异常类型。

8.4.1异常点

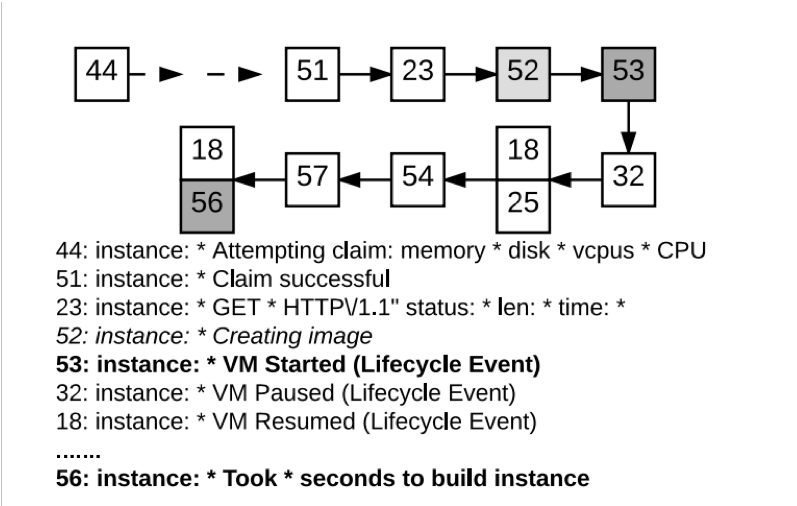
大多数文学作品集中在一点异常。点异常往往代表发生随机的不规则或偏差，可能没有特别的解释。例如，在图10中，使用了在摩纳哥的餐厅高消费信用卡交易似乎一点异常，因为它显著从交易的其余部分偏离。一些真实世界的应用，考虑点异常检测，在第9节进行了综述。

8.4.2上下文异常检测

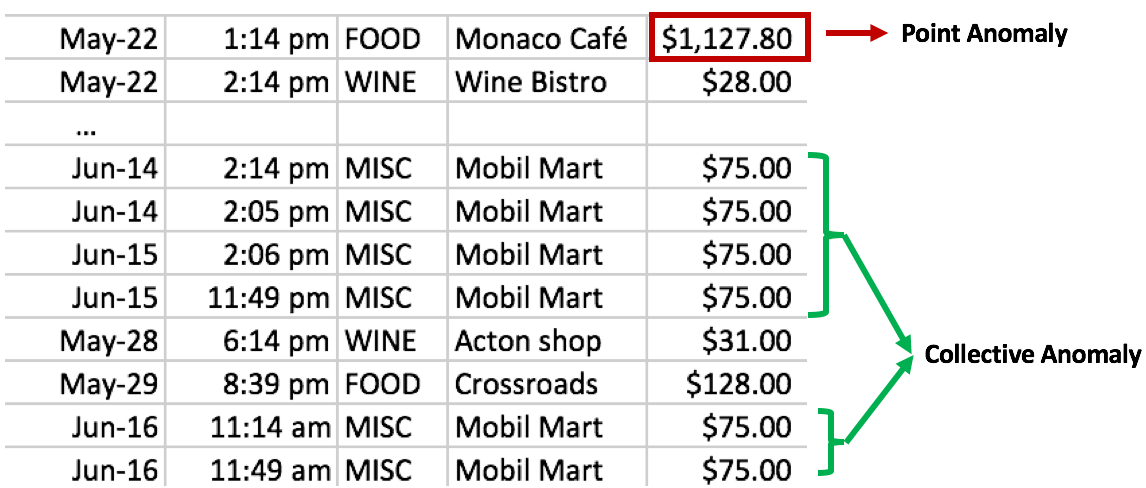
异常也被称为条件异常一个上下文是可以被认为是在一些特定的上下文anoma-LOUS数据实例（Song等人[2007]）。语境异常是由同时考虑情境和行为特征识别。上下文的特点，正常使用的时间和空间。虽然行为特征可能是

7

花钱的模式，系统日志事件的发生或任何特征来描述正常行为。图9a示出了通过只六月之前大幅下降所指示的内容相关的异常考虑温度数据的例子;这个值是不表示在此期间发现了正常值。图9b示出了使用深长短期存储器（LSTM）（Hochreiter和施米德休伯[1997]）基于模型来识别异常的系统日志事件（Du等人[2017]）在给定的上下文（例如被检测到的事件53作为感你离题了）。



（a）温度数据Hayes和Capretz[2015]。



（b）系统记录Du等。[2017]。

图9：上下文异常检测的插图。

8.4.3集体或群体异常检测。

各个数据点的异常集合被称为集体或组的异常，其特征在于，而在一组显示出不寻常的特征观察各孤立的各个点显示为正常的数据实例。例如，考虑欺诈性信用卡交易的说明，在图10所示的记录数据，如果会发生“MISC”的单一的交易，也许可能没有看上去那么反常。价值$75的交易的以下组肯定似乎是集体或群体异常的候选。组异常去tection（GAD）与不规则组分布（例如，使用自动编码器模型的一个变体中检测到的图像的像素的不规则混合物的强调（Chalapathy等人[2018B]，邦当等人[2016]，阿拉亚等人[2016]，Zhuang等人[2017]）。

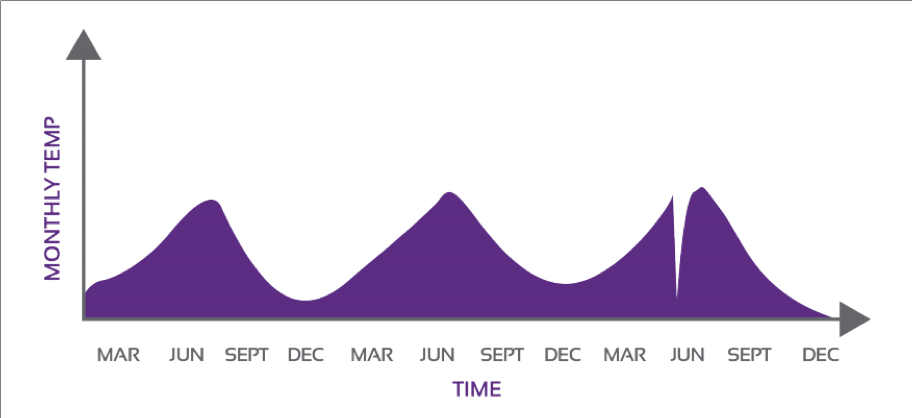


图10：信用卡欺诈检测：龙虎斗点和集体异常。

8.5输出DAD技

异常检测方法的一个关键方面是在其中检测到异常的方式。通常，通过异常检测方法所产生的输出或者是异常分数或二进制标签。

8.5.1异常评分：

异常评分描述离群的每个数据点的水平。数据实例可以根据异常的得分进行排序，以及一个域特定阈值（俗称决定得分）将由主题专家被选择来识别异常。在一般情况下，决定分数揭示不是二进制标签的更多信息。例如，在深SVDD接近决定得分是数据点的距离的从所述球体的中心的度量，其是远离中心的数据点被认为异常（拉夫等人[2018B]）。

8

表3：卷积神经网络，LSTM：长短期记忆网络GRU：门控重复单元，DNN：深层神经网络SPN：和积NetworksTechniques模型体系结构第ReferencesDiscriminativeLSTM，CNN-LSTM-GRU在HIDSCNN采用DAD技术的例子，DNN

第11.7，11.6，11.1Kim等人。[2016]，Chawla等。[2018]，Chen等人。[2018]，Sohi等。[2018]，Vinayakumar等。[2017]混合动力GAN10.3节Aghakhani等。[2018]，Li等。[2018]生成性AE，SPN，第11.8节，11.3Gao等。[2014]，Peharz等。[2018]，乌默尔等。[2018]

8.5.2标签：

而不是分配分数，一些技术可以分配类别标签为正常或异常的每个数据实例。使用自动编码无监督异常检测技术测量用于获得异常分数残差矢量（i，E重构误差）的大小，以后，重建误差被任一排或阈值处理由领域专家的标签数据的实例。

深异常检测的9个应用程序

在本节中，我们将讨论深异常检测的几个应用程序。对于每一个应用领域，我们讨论以下四个方面：异常的-the概念;-nature数据;-challenges与检测异常相关联;-现有深异常检测技术。

9.1入侵检测

入侵检测系统（IDS）是指识别与计算机相关的系统的恶意活动（Phoha[2002]）。IDS可以被称为主机入侵检测（HIDS）到大型网络的网络入侵检测（NIDS）单个计算机上部署。的深异常检测技术的入侵检测的分类是在图11IDS取决于检测方法被分类成基于签名或基于异常。使用基于签名的入侵检测系统不能有效地检测新的攻击，对此没有具体的签名模式是可用的，因此，基于异常的检测方法是比较流行的。在本次调查中，我们专注于入侵检测采用深异常检测（DAD）的方法和体系结构。

9.1.1基于主机的入侵检测系统（HIDS）：

这样的系统被安装了通过监听系统调用或事件主机内发生监视恶意活动或违反政策的单个主机或计算机软件程序（豇豆和Kruegel[2005]）。该系统呼叫日志可以通过程序或通过导致日志，如图9b所示的用户交互来产生。恶意相互作用导致不同的序列，这些系统调用的执行。HIDS还可以监视系统，其存储的信息，在随机存取存储器（RAM）的状态，在文件系统中，日志文件或其他地方进行有效的序列。深异常检测施加HIDS（DAD）技术需要处理可变长度以及数据的顺序性。该DAD技术具有与序列数据或者模拟或计算序列之间的相似性。一些成功的全DAD技术HIDS如表3所示。

9.1.2网络入侵检测系统（NIDS）：

NIDS系统处理通过检查每个网络数据包监视可疑流量的整个网络。由于实时流的行为，数据的性质就是指对具有高容量，速度，各种大数据。网络数据还具有与其相关联的时间方面。一些成功的全DAD技术NIDS如表4所示。本次调查还列出了用于在入侵检测所面临的DAD技术表5的挑战评估DAD入侵检测方法的数据集是异常的性质不断变化随着时间的入侵者适应他们的网络攻击，以逃避现有的入侵检测解决方案。

9

表4：在使用NIDSDAD技术的实例。CNN：卷积神经网络，LSTM：长短期记忆网络RNN：回归神经网络，RBM：受限玻尔兹曼机DCA：扩张型卷积自动编码，DBN：坚定信念网络AE：自动编码，SAE：叠放自动编码GAN：剖成对抗性网络，CVAE：卷积变Autoencoder.Techniques模型体系结构第ReferencesGenerativeDCA，SAE，RBM，DBN，CVAE

部分11.6，11.8，11.1，11.5Yu等人。[2017]，事[2017]，Zolotukhin等。[2016]，Cordero的等。[2016]，Alrawashdeh和珀迪[2016]，Tang等人[2016]，洛佩兹-Martin等人。[2017]铝Qatf等。[2018]，米尔斯基等。[2018]，Aygun和Yavuz的[2017]混合动力GAN10.3节Lin等人。[2018]，Yin等。[2018]中，环等。[2018]，拉塔[2018]，Intrator等。[2018]，Mat-subara等。[2018]，Nicolau等。[2016]，Rigaki[2017].DiscriminativeRNN，LSTM，CNN11.7节，11.6Yu等人。[2017]，Malaiya等。[2018]Kwon等人。[2018]，Gao等。[2014]，Staudemeyer[2015]，纳瑟尔等。[2018]

表5：数据集用于入侵检测的

数据集IDS描述类型ReferencesCTU-UNBNIDSCTU-UNBUCS[2017]数据集CON组从CTU-13数据集[20]和正常流量各种僵尸网络流量从UNBISCXIDS2012的数据集sistsShiravi等。[2012]

十六进制Yu等人。[2017]

Contagio-CTU-UNBNIDSContagio-CTU-UNB六种类型的网络流量数据的数据集CON组sists。亚当等人。[2008]

文本Yu等人。[2017]。

NSL-KDD1NIDS的NSL-KDD数据集是其前身KDD-99数据集的改良版本。UCS[2017]

文本Yin等。[2017]，Javaid等人。[2016]，Tang等人[2016]，Yousefi-阿扎等。[2017]，Mohammadi的和Namadchian[2017]，洛佩兹-Martin等人。[2017]DARPAKDD-CUP99

NIDSDARPAKDDStolfo等。[2000]本次大赛的任务是建立一个网络入侵探测器，能够优越性有“坏”的连接，称为入侵或攻击，和“好”的正常连接之间guishing预dictive模型。

文本Alrawashdeh和Purdy的[2016]，Van等。[2017]，Mohammadi的和Namadchian[2017]

MAWINIDS的MAWIFontugne等。[2010]数据集由网络traf-FICcapturedfrom日本和美国之间的主干链路。每daysince2007

文字德罗等人。[2016]

现实的全球网络环境（RGCE）

NIDSRGCE果酱[2009]包含realis-抽动互联网服务提供商（ISP）和许多不同的网络服务惠及作为真正的互联网。

文本Zolotukhin等。[2016]

ADFA-LDHIDS的ADFALinux的数据集（ADFA-LD）。该数据集提供了一个反面的临时Linux的数据集evalua-重刑传统HIDS克里奇和胡[2014]

文本Kim等人。[2016]，Chawla等。[2018]

系统调用的UNM-LPRHIDS下设到HIDS系统大学[2012]评价

文本Kim等人。[2016]

感染PDF样本

HIDS下设集感染的PDF样本，用于监视恶意流量的

文本陈等人。[2018]

10

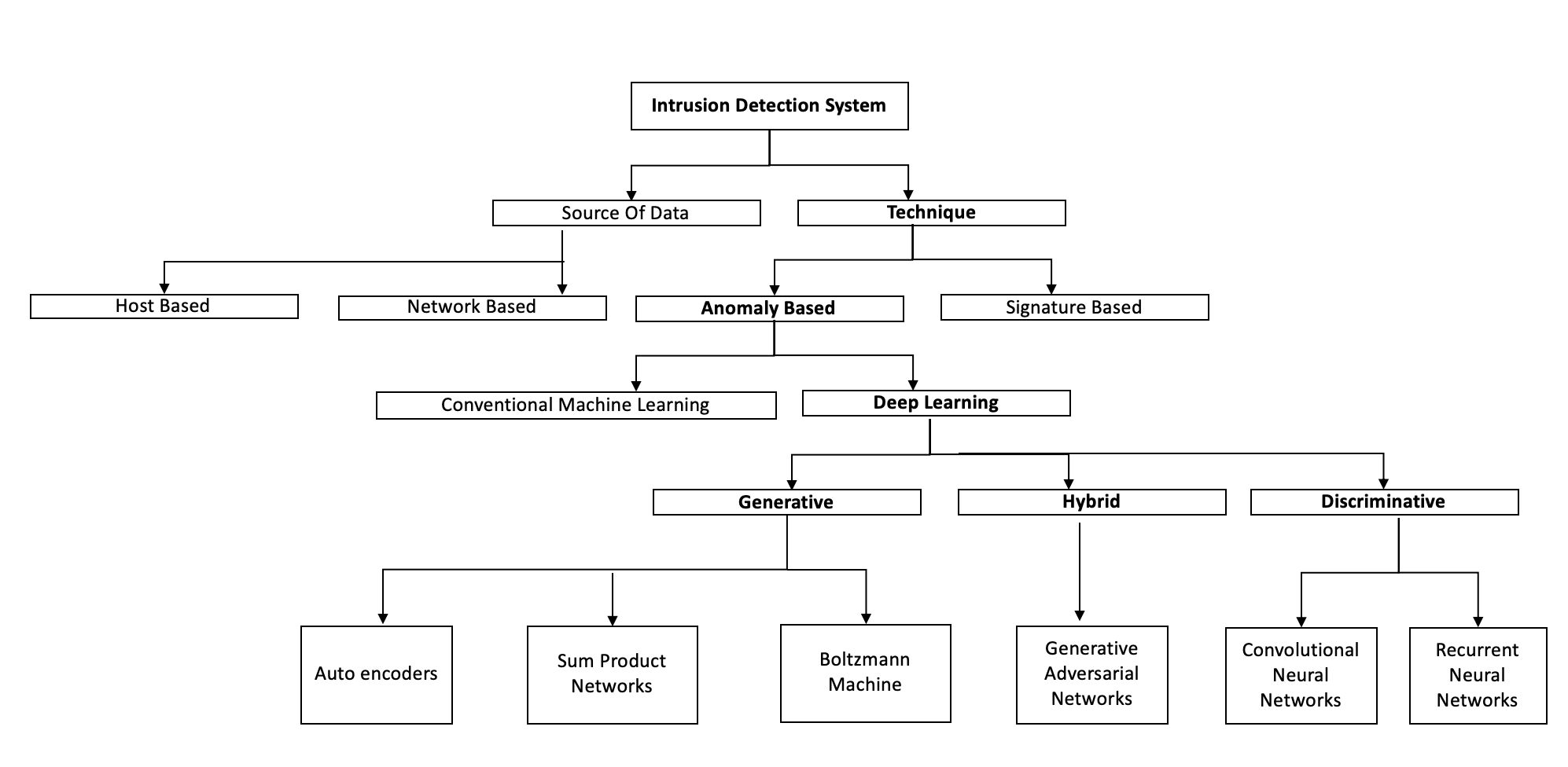


图11：深学习方法的入侵检测分类。

9.2欺诈检测

欺诈是欺骗存取宝贵资源故意行为（Abdallah等人[2016]）。该Pricewaterhouse-库珀（普华永道）2018（Lavion[2018]，赵[2013]）全球经济犯罪调查发现，7200家公司他们调查了一些自然的经验欺诈的一半。欺诈检测是指检测的不同行业从事非法活动，在12示出。

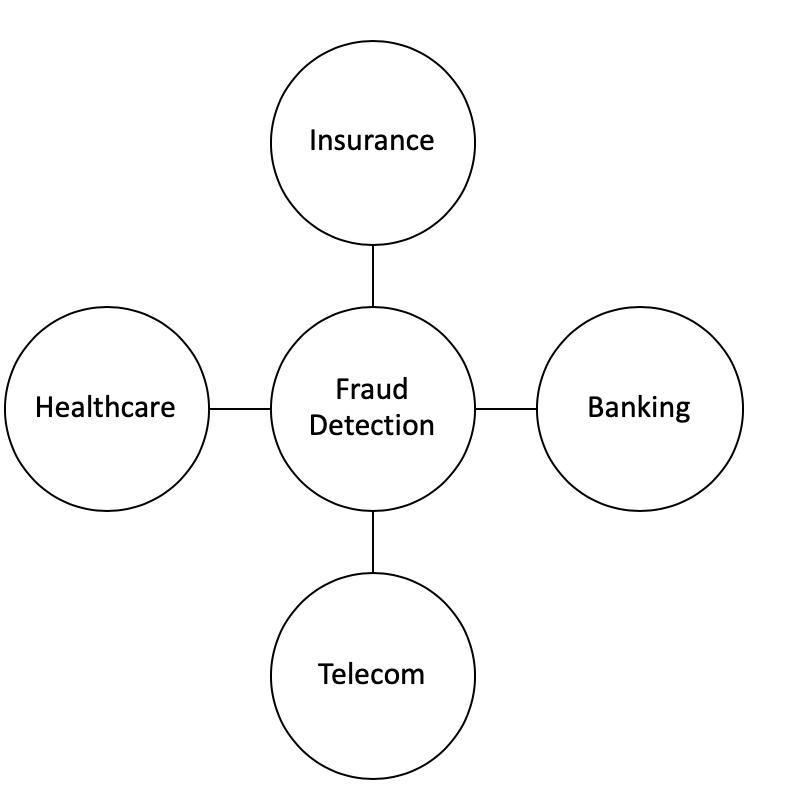


图12：欺诈检测跨各种应用领域。

欺诈在电信，保险（医疗卫生，汽车等）的权利要求，银行业（纳税申报索赔，信用卡交易等）代表政府和私营企业显著的问题。检测和防止欺诈不是一个简单的任务，因为造假是一种自适应的犯罪。许多传统的机器学习算法已在欺诈检测成功应用（Sorournejad等人[2016]）。与检测欺诈相关的挑战是，它需要实时检测和预防。本节重点介绍了欺诈检测深异常检测（DAD）技术。

11

表6：在信用卡欺诈检测使用DAD技术的例子。AE：自动编码，LSTM：长短期记忆网络RBM：限制Botlzmann机，DNN：深层神经网络GRU：门控重复单元，RNN：回归神经网络CNN：卷积神经网络，VAE：变自动编码GAN：创成对抗性网络

技术用过部分ReferencesAE11.8节Schreyer先生等人。[2017]楔形等。[2017]，保等人。[2016]，Ren-斯特罗姆和Holmsten[2018]，和Kazemi的Zarrabi[2017]，Zheng等人。[2018A]，Pumsirirat和颜[2018]RBM11.1节Pumsirirat和颜[2018]DBN11.1节Seeja和Zareapoor[2014]VAE11.5节Sweers等。[2018]GAN11.5节Fiore等。[2017]，Choi和张[2018]DNN11.1节Dorronsoro等。[1997]，G'omez等。[2018]LSTM，RNN，GRU11.7节维泽和Omlin[2009]，Jurgovsky等。[2018]，Heryadi和Warnars[2017]，Ando等。[2016]，Wang等人。[2017A]，Alowais和Soon[2012]，阿马拉辛哈等。[2018A]，Abroyan[2017A]，LP等人。[2018]CNN11.6节Shen等人。[2007]，Chouiekh和哈吉[2018]，Abroyan[2017b]，Fu等人。[2016年]，鲁[2017年]，王等人。[2018A]，Abroyan[2017A]，Zhang等人。[2018A]

表7：在移动蜂窝网络中的欺诈检测使用DAD技术的实例。CNN：卷积神经网络，DBN：坚定信念网络SAE：叠放自动编码，DNN：深层神经网络GAN：创成对抗性网络

技术中使用第ReferencesCNN11.6节Chouiekh和哈吉[2018]SAE，DBN11.8节，11.1Alsheikh等。[2016]，Badhe[2017]DNN11.1节Akhter和Ahamad[2012]，耆那[2017]GAN11.5节Zheng等。[2018B]

9.2.1银行诈骗

信用卡已经成为对商品和服务进行网上购物流行的付款方式。信用卡诈骗涉及的支付卡信息被盗，并把它作为基金的交易欺诈源。信用卡欺诈检测的许多技术在过去几年中被提出（Zhou等人[2018]，Suganya和Kamalraj[2015年]）。我们将简要回顾一些DAD技术如表6所示信用卡欺诈检测所面临的挑战是，欺诈没有一致的模式。在信用卡欺诈检测的典型方法是保持每个用户的使用配置文件，并监视用户配置文件来检测任何偏差。由于有几十亿信用卡用户的个人信息的方法的这种技术不是很可扩展性。由于DAD的技术技术的固有性质的可扩展性正在获得广泛的传播采用信用卡欺诈检测。

9.2.2移动蜂窝网络欺诈

近年来，移动蜂窝网络技术的迅速部署和发展支持十亿用户和移动设备的极大多样化。由于这种广泛采用，低移动蜂窝服务费率，移动蜂窝网络现在面临着欺诈行为，例如有针对性地盗取客户的私人信息，并从客户短信相关的骗局勒索钱财语音诈骗。检测这样的欺诈是最重要的利益，而不是一件容易的事，由于体积和移动蜂窝网络的速度。传统的机器学习方法与静态特征的工程技术无法适应不断变化的欺诈性质。表7列出DAD技术移动蜂窝网络的欺诈检测。

9.2.3保险欺诈

一些传统的机器学习方法已成功地应用于检测保险索赔欺诈（Joudaki等人（2015年），罗伊和乔治[2017]）。对于欺诈检测的传统方法是基于特征

12

表8：在保险欺诈检测中使用DAD技术的实例。DBN：坚定信念网络，DNN：深层神经网络CNN：卷积神经网络，VAE：变自动编码GAN：创成对抗性网络

DBN11.1节Viaene等。[2005]VAE第11.5节的Fajardo等。[2018]GAN11.5节Fiore等。[2017]，Choi和张[2018]DNN11.1节强等。[2009]CNN11.6节Shen等人。[2007]，张某等人。[2018A]

表9：在医疗保健欺诈检测中使用DAD技术的实例。RBM：受限Botlzmann机，甘：剖成对抗性网络

技术中使用第ReferencesRBM11.1节Lasaga和Santhana[2018]GAN11.5节GhasediDizaji等。[2018]，鳍layson等。[2018]CNN11.6节埃斯特瓦等。[2017]

这是欺诈行为指标。与这些传统方法所面临的挑战是，需要手动的专业知识提取强大的功能。另一个挑战是，保险欺诈检测是关于欺诈的发生率比债权总人数远远不足，同时，各欺诈是其独特的方式。为了克服这些限制几个DAD技术提出了在表8中示出。

9.2.4医疗保健欺诈

医疗是在人们的生活，浪费，滥用的一个组成部分，并通过诈骗数百亿美元，每年推高医疗费用。医疗保险索赔欺诈是一个显著贡献的医疗费用增加，但其影响可以通过欺诈检测得到缓解。几种机器学习模型已经在医疗保险欺诈有效使用（巴德和Khoshgoftaar[2017年]）。表9礼物DAD方法保健欺诈识别的概述。

9.3恶意软件检测

恶意软件，简称恶意软件。提出为了保护合法用户免受恶意软件，基于机器学习的有效的恶意软件检测方法（Ye等人[2017]）。在经典的机器学习方法，恶意软件检测的过程通常分为两个阶段：特征提取和分类/聚类。传统的恶意软件检测的性能接近关键取决于所提取的特征和分类/聚类的方法。在恶意软件检测问题相关的挑战是数据的规模，例如考虑到数据字节的特定序列分类问题可能是两个百万时间步骤的顺序的。此外，恶意软件在本质上是很适应，其中，攻击者会使用先进的技术来隐藏恶意行为。这有效地解决这些挑战和检测恶意软件一些DAD技术示于表10。

9.4医学异常检测

几项研究已经进行了解深度学习的medi-CAL和生物信息学（最小的理论和实际应用等。[2017年]，曹等人[2018A]，赵等人[2016年]，汗和Yairi[2018]）。寻找在地区罕见的事件（异常），如医学图像分析，临床脑电图（EEG）记录，使诊断和各种医疗条件提供预防治疗。基于深度学习体系结构取得了巨大成功用于医疗检测异常，如表11所示。在医疗领域呈现显著挑战不平衡数据的大量检测到异常值。另外，对于长而深的学习技术已被视为黑盒技术。尽管深学习模型产生优秀perfor-曼斯，这些模型缺乏解释能力。近来具有良好的解释能力模型提出，并显示出国家的最先进的生产性能（Gugulothu等人，阿马拉辛哈等人[2018B]，彩[2018]）。

13

表10：用于恶意软件检测DAD技术的实例。AE：自动编码，LSTM：长短期记忆网络RBM：限制Botlzmann机，DNN：深层神经网络GRU：门控重复单元，RNN：回归神经网络CNN：卷积神经网络，VAE：变自动编码GAN：剖成对抗性网络，CNN-BiLSTM：CNN-双向LSTM

技术所用的章节参考文献

AE11.8节优素菲，阿扎尔等人。[2017]，Hardy等。[2016]，优素菲-阿扎等。[2017]，德保拉等人。[2018]，Sewak等。[2018]，凯贝蒂等。[2017]，德保拉等人。[2018]，David和内塔尼亚胡[2015]word2vec11.4节Cakir的和Dogdu[2018]，Silva等。[2018]CNN11.6节Kolosnjaji等。[2018]，Suciu等。[2018]，Srisakaokul等。[2018]，Srisakaokul等。[2018]，King等人。[2018]，黄和花王[2017]，Guo等。[2017]，阿卜杜勒萨拉姆等人。[2018]，拉夫等人。[2017]，Karbab等。[2018]，Martinelli的等。[2017]，McLaughlin等。[2017]，吉尔伯特等。[2018]，Kolosnjaji等。[2017]DNN11.1节Rosenberg等。[2018]，Wang等人。[2017b]DBN11.1节大卫和内塔尼亚胡[2015]，Yang等人。[2016]，Ding等人。[2016]，雨欣和四溢[2017]，Selvaganapathy等。[2018]，雨欣和四溢[2017]，Hou等人。[2017]LSTM11.7节Tobiyama等。[2016]，胡和Tan[2017]，Tobiyama等。[2018]，Passalis和TefasCNN-BiLSTM11.6节，11.7

Le等。[2018]，Wang等人。[2017b]

甘11.5节Kim等人。[2018]混合模型（AE-CNN），（AE-DBN）

第10.3节王等人。[2018B]，Li等。[2015]

RNN11.7节HaddadPajouh等。[2018]

表11：DAD技术用于医疗异常检测的实施例。AE：自动编码，LSTM：长短期记忆网络GRU：门控重复单元，RNN：回归神经网络CNN：卷积神经网络，VAE：变自动编码GAN：剖成对抗性网络，KNN：K近邻RBM：受限玻尔兹曼机。

技术用过部分ReferencesAE11.8节王等人。[2016]，考顿等人。[2018]，Sato等人。[2018]DBN11.1节Turner等人。[2014]，Sharma等人。[2016]，Wulsin等。[2010]Ma等。[2018]，Zhang等人。[2016]，Wulsin等。[2011]Wu等。[2015A]RBM11.1节Liao等。[2016]VAE11.5节Xu等人。[2018]，Lu和许[2018]GAN11.5节GhasediDizaji等。[2018]，陈和Konukoglu[2018]LSTM，RNN，GRU11.7节洋和高[2018]，佳岗和Yu[2016年]，考顿等人。[2018]，O'Shea等。[2016]，拉提夫等人。[2018]，Zhang和邹[2018]，Chauhan保持和维格[2015]，Gugulothu等人，阿马拉辛哈等。[2018B]CNN11.6节施密特Erfurth等。[2018]，埃斯特瓦等。[2017]，Wang等人。[2016]，IAKOVIDIS等。[2018]混合动力（AE+KNN）11.6节Song等。[2017]

14

表12：用于检测社交网络中的异常DAD技术的实例。CNN：卷积神经网络，LSTM：长短期记忆网络AE：自动编码，DAE：降噪自动编码SVM：支持向量机，DNN：深层神经网络

技术所用的章节参考文献

AE，DAE11.8节张某等人。[2017]，卡斯特里尼等。[2017]CNN-LSTM11.6节，11.7Sun等人。[2018]，Shu等人。[2017]，Yang等人。[2018]DNN11.1节Li等人。[2017A]混合模型（CNN-LSTM-SVM）

第10.3节委[2017年]

表13：在学习系统日志中使用异常检测技术的深的实例。CNN：卷积神经网络，LSTM：长短期记忆网络GRU：门控重复单元，DNN：深层神经网络AE：自动编码，DAE：降噪自动编码

技术参考节

LSTM11.7节Hochreiter和施米德休伯[1997]，Brown等人。[2018]，Tuor等。[2017]，Das等人。[2018]，马尔霍特拉等。[2015]AE11.8节Du等。[2017]，Andrews等人。[2016a]，樱和Yairi[2014]，提出中止等。[2018A]，提出中止等。[2016]LSTM-AE第11.7节，11.8

格罗弗[2018]，Wolpher[2018]

RNN11.7节布朗等人。[2018]，Zhang等人。[2018B]，Nanduri和雪利酒[2016]，蜂鸣等。[2017]DAE11.8节马奇等。[2015]提出中止等。[2016]CNN11.6节路等。[2018]，Yuan等人。[2018A]，Racki等。[2018]，Zhou等人。[2016]，Gorokhov等。[2017]，Liao等。[2017]，Cheng等人。[2017]，Zhang等人。[2018C]

9.5深度学习在社交网络异常检测

近年来，在线社交网络已经成为人们日常生活中不可或缺的一部分。在社交网络中异常是一个社交网络中的个人往往不规则的非法行为模式;这样的人可能被识别为垃圾邮件发送者，性犯罪者，在线欺诈的，假的用户或谣言贩子。检测这些不规则图案是最重要的，因为如果没有检测到，这样的个人的行为可以有一个严重的社会影响。传统的异常检测技术和挑战，以检测在社交网络中的异常的调查是在文学（一个很好的研究课题刘和乔拉[2017年]，Savage等人[2014]，阿南德等人[2017年]，Yu等[2016]，Cao等人[2018B]，Yu等人[2016]）。数据呈现的异质性和动态性显著挑战DAD技术。尽管存在这些挑战，在表12中示出的几个DAD技术示优于大反映最新技术的方法。

9.6日志异常检测

异常检测日志文件旨在查找文本，它可以表明原因和系统故障的性质。最常见的，特定领域的正则表达式是从通过模式匹配发现新的故障过去的经验构建。这种方法的限制是，很容易不被检测故障的较新的邮件（梅蒙[2008]）。在这两种格式的日志数据的语义的非结构化和多样性带来显著挑战登录异常检测。异常检测技术要适应并发的设定产生的日志数据，并实时检测异常。继深层神经网络的实时文本分析的成功，几个DAD技术，表13所示型号为自然语言序列中的日志数据显示在检测异常值是非常有效的。

9.7物联网（IOT）的大数据异常检测

的IoT被识别为设备的网络互相连接用的软制品，服务器，传感器和等在事物（IOT）的因特网的领域中，通过气象站，收音机频率识别（RFID）标签，IT产生的数据基础设施组件，以及其他一些传感器大多时间序列顺序的数据。异常检测在这些

15

表14：DAD技术的例子在物联网（IOT）的大数据异常检测使用。AE：自动编码，LSTM：长短期记忆网络DBN：坚定信念网络。

技术参考节

AE11.8节洛和Nagarajany[2018]，钼和哈马迪Kwasinski[2018]DBN11.1节Kakanakova和扬诺夫[2017]LSTM11.7节Zhang等人。[2018D]，Mudassar等。[2018]

表15：在工业操作中使用DAD技术的例子。CNN：卷积神经网络，LSTM：长短期记忆网络GRU：门控重复单元，DNN：深层神经网络AE：自动编码，DAE：降噪自动编码，SVM：支持向量机SDAE：叠放降噪自动编码，RNN：回归神经网络。

技术参考节

LSTM11.7节Inoue等。[2017]，Thi等人。[2017]，Kravchik和Shab-泰[2018]Huang等。[2018]，Park等人。[2018A]，Chang等人。[2018]AE11.8节圆和贾[2015]，阿拉亚等人。[2017]，Qu等。[2017]，樱和Yairi[2014]，Bhattad等。[2018]DNN11.1节洛迪等。[2017]CNN11.6节Faghih-Roohi等。[2016]，Christiansen的等。[2016]，Lee等人。[2016]，Faghih-Roohi等。[2016]，Dong等人。[2016]，Nanduri和雪利酒[2016]，Fuentes等。[2017]Huang等。[2018]，Chang等人。[2018]SDAE，DAE11.8节燕宇（2015年），罗钟[2017年]，Dai等。[2017]RNN11.7节Banjanovic-Mehmedovic等。[2017]，Thi等人。[2017]混合模型（DNN-SVM）10.3节Inoue等[2017]

物联网的网络识别虚假，互联设备的这些庞大规模的错误行为。与异常检测相关联的挑战之一是，不同种类的设备相互连接这使得系统更加复杂。使用深学习（DL），以便于分析和学习在的IoT域的彻底综述由呈现（Mohammadi等人[2018]）。表14示出了所采用的IoT设备DAD技术。

9.8产业异常检测

由风力涡轮机，电厂，高温能量系统，存储设备，并与旋转机械部件工业系统被暴露于巨大的应力，一天到一天的基础。伤害到这些类型的系统不仅造成经济损失，而且声誉的损失，因此检测和早期修复它们是最重要的。几个机器学习技术已被用来检测在工业系统这样的损伤（Ramot-soela等人[2018]，Mart'ı等人[2015]）。发表利用深度学习模型检测早期产业损害几篇论文表现出极大的承诺（ATHA和Jahanshahi[2018]，德Deijn[2018]，王等人[2018C]）。造成设备损坏是罕见的事件，从而检测到这样的事件可以被配制为异常值检测的问题。与本领域异常检测相关联的挑战之一是两个卷以及数据的动态性质，因为失败是由于各种因素引起的。是一些不同行业采用的技术DAD在表15中示出。

9.9异常检测时间序列

数据在持续时间称为时间序列的连续记录。时间序列数据，大致可分为单变量和多变量的时间序列。在单变量的时间序列的情况下，仅单可变（或特征）随时间变化。例如，从房间的每个第二内的温度传感器收集的数据是一个单变量的时间序列数据。多变量时间序列由几个变量（或功能），随着时间的推移其变化。这对于每秒一个用于每个轴线（X，Y，Z）产生三维数据的AC-celerometer是多变量的时间序列数据的一个很好的例子。在文献中，类型单变量和多变量的时间序列的异常被CAT-egorized成以下几组：（1）点异常。8.4.1（2）内容相关异常8.4.2（3）集体异常

16

表16：在单变量的时间序列数据中使用DAD技术的例子。CNN：卷积神经网络，GAN：剖成对抗性网络，DNN：深层神经网络，AE：自动编码，DAE：降噪自动编码，VAE：变自动编码，SDAE：叠放降噪自动编码，LSTM：长短期记忆网络，GRU：门控复发单位RNN：回归神经网络，RNN：复制神经网络

技术参考节

LSTM11.7节Shipmon等。[2017A]，Hundman等。[2018]，诸和拉普捷夫海[2017]马尔霍特拉等。[2015]，Chauhan保持和维格[2015]，AS-sendorp[2017]Ahmad等。[2017]，马尔霍特拉等。[2016a]，邦当等。[2016]，Taylor等人。[2016]，Cheng等人。[2016]，LO-ganathan等。[2018]，Chauhan保持和维格[2015]，马尔霍特拉等。[2015]，Gorokhov等。[2017]，穆尼尔阿等。[2018]AE，LSTM-AE，CNN-AE，GRU-AE

11.8节Shipmon等。[2017b]，马尔霍特拉等。[2016B]，Filonov等。[2016]，Sugimoto等。[2018]，Oh和韵[2018]，Ebrahimzadeh和克莱因伯格，Veeramachaneni等。[2016]，斗等。[2014]RNN11.7节Wielgosz等。[2017]，Saurav等。[2018]，Wielgosz等。[2018]，Guo等。[2016]，Filonov等。[2017]CNN，CNN-LSTM11.6节，11.7Kanarachos等。[2017]，都等人，Gorokhov等。[2017]，Napoletano等。[2018]尚穆根等。[2018]，梅德尔和Savakis[2016]LSTM-VAE第11.7节，11.5Park等人。[2018B]，S¨olch等。[2016]DNN11.1节阿马拉辛哈等。[2018B]GAN11.5节Li等人。[2018]，Zenati等。[2018]，Lim等人。[2018]，拉普捷夫海，Wei等人。[2018]

8.4.3。近来，许多深学习模型已经提出了如表16和表17所示分别检测单变量和多变量的时间序列数据内的异常。一些挑战来检测使用深度学习模型的数据在时间序列异常是：

•缺少其中的异常发生可以被定义限定的图案的。

•输入数据内的噪声严重影响了算法的性能。

•随着时间序列数据的长度增加了计算的复杂性也增加。

•时间序列数据通常是不固定的，非线性的和动态发展。因此DAD模型应该能够实时检测异常。

9.9.1单变量时间序列深异常检测

在深度学习领域提供了机会的进步，以提取丰富的层次特点，可以极大地提高离群单变量的时间序列数据中检测。的行业标准工具和数据集（包括深学习型和非深学习为主）为基准的单变量和多变量的时间序列数据异常检测算法的列表呈现，并保持在Github上库2表16显示采用各种深架构对于单变量的时间序列数据内异常检测。

9.9.2多元时间序列深异常检测

异常检测多元时间序列数据是一项艰巨的任务。有效的多元异常检测使故障隔离诊断。RNN和LSTM基础的方法3被示出为在多变量的时间序列数据集内检测帧间pretable异常表现良好。DeepAD，基于深度学习一个通用框架多元时间序列异常检测是通过提出（布达等人[2018]）。可解释的，使用深注意基于模型设计异常检测系统是有效的在说明中的异常检测（Yuan等人[2018B]，过和Lin[2018]）。表17示出了用于多变量的时间序列数据内异常检测通过了各种深架构。

2https：//github.com/rob-med/awesome-TS-anomaly-detection3https：//github.com/pnnl/safekit

17

表17：在多变量的时间序列数据中使用DAD技术的例子。CNN：卷积神经网络，GAN：剖成对抗性网络，DNN：深层神经网络，AE：自动编码，DAE：降噪自动编码，VAE：变自动编码，SDAE：叠放降噪自动编码，LSTM：长短期记忆网络，GRU：门控复发单元

技术参考节

LSTM11.7节努奇等。[2018]，Hundman等。[2018]，Assendorp等。[2017]提出中止等。[2018B]AE，LSTM-AE，CNN-AE，GRU-AE

11.8节张某等人。[2018E]Guo等。[2018]，Fu等人。[2019]，侨等。[2018]

CNN，CNN-LSTM11.6节，11.7Basumallik等。[2019]尚穆根等。[2018]LSTM-VAE第11.7节，11.5Ikeda等人。[2018]，Park等人。[2018B]GAN11.5节Assendorp[2017]，Li等。[2018]，Li等。[2019]考顿等人。[2018]DNN-RNN11.7节Tuor等。[2017]，Tuor等。[2018]

表18：在多变量异常检测用数据集。

数据集说明参考

美国航空航天局梭阀数据1包括从火星Sci-ENCE实验室和SMAP误sions飞船异常数据和实验

Hundman等。[2018]2

对于船只的行为异常检测血管3多元时间数据分析

马亚[2017年]

斯瓦特和WADI安全水处理（SWAT）和配水（WADI）

Li等人。[2019]

信用卡欺诈检测

标记为欺诈真正的匿名信用卡交易

达尔Pozzolo等。[2015]

纽约市出租车客运count5纽约市出租车客运数据流

崔等人。[2016]

1https://cs.fit.edu/~pkc/nasa/data/2https://github.com/khundman/telemanom3http://conferences.inf.ed.ac.uk/EuroDW2018/papers/eurodw18-Maia.pdf4https://www.kaggle.com/peterkim95/multivariate-gaussian-anomaly-detection/数据

5https://github.com/chickenbestlover/RNN-Time-series-Anomaly-Detection

9.10视频监控

视频监控也俗称为闭路电视（CCTV）涉及监测感兴趣的指定区域，以保证安全性。在视频监控应用未标记的数据是大量使用，这是监督的机器学习和深入学习方法显著的挑战。因此，视频监控应用已被建模为由于缺乏标记数据的可用性异常检测的问题。几个作品已经研究用于视频异常检测状态的最先进的深模型和基于模型和检测的标准的类型进行了分类它们（基兰等人[2018]，冲泰[2015]）。强大的全天候视频监控系统所面临的挑战进行了详细的（Boghossian和黑色[2005]）讨论。缺乏在现实生活中的视频监控异常的显式定义的是一个显著的问题是礼篮DAD方法的性能为好。在视频监控使用DAD技术在表19中示出。

18

表19：用于视频监控DAD技术的例子。CNN：卷积神经网络，LSTM：长短期记忆网络RBM：受限玻尔兹曼机，DNN：深层神经网络AE：自动编码，DAE：降噪自动编码OCSVM：一类支持向量机，CAE：卷积自动编码SDAE：叠放降噪自动编码，STN：空间变压器网络部

技术所用的章节参考文献

CNN11.6节Dong等。[2016]，Andrewsa等人，Sabokrou等。[2016a]，Sabokrou等。[2017]，MU-纳瓦尔等。[2017]，Li等。[2017b]，Qiao等。[2017]，特里帕西等。[2018]，Nogas等。[2018]，Christiansen的等。[2016]，Li等。[2017b]，SAE（AE-CNN-LSTM）

部11.8，11.6，11.7冲泰[2017]，Qiao等。[2017]，Khaleghi和莫因[2018]

AE11.8节巧等人。[2017]，Yang等人。[2015]，Chen等人。[2015]，Gutoski等人，D'Avino等人。[2017]，Dotti等。[2017]，Yang等人。[2015]，Chen等人。[2015]，Sabokrou等。[2016B]，Tran和霍格[2017]，Chen等人。[2015]，D'Avino等人。[2017]，哈桑等[2016]，Yang等人。[2015]的Cinelli[2017]，Sultani等。[2018]混合模型（CAE-OCSVM）

第10.3节Gutoski等，Dotti等。[2017]

LSTM-AE11.7节，11.8D'Avino等人。[2017]STN11.2节Chianucci和Savakis[2016]RBM11.1节穆纳瓦尔等。[2017]LSTM11.7节梅德尔和Savakis[2016]，Luo等人。[2017A]，本-Ar1和Shwartz-谢夫[2018]，辛格[2017]RNN11.7节Luo等人。[2017b]，周某和张某（2015年），胡等人。[2016]，冲泰[2015]AAE11.5节Ravanbakhsh等。[2017A]

10深异常检测（DAD）的型号

在本节中，我们将讨论各种DAD车型分类基于标签的可用性和培养目标。对于每个模型类型域，我们将讨论以下四个方面：-assumptions;型模型体系结构;-computational复杂性;-的优点和缺点;

10.1监督深异常检测

监督异常检测技术是在性能上优于相比无监督异常检测技术，因为这些技术使用标记的样品（G¨ornitz等人[2013]）。监督异常检测从一组注释的数据实例（训练），然后学习的分离边界，一个测试实例分类为正常或异常的类与学习模型（测试）。假设：深监督学习方法依赖于分离数据类，而监督的技术集中于解释和理解数据的特点。基于异常检测技术多类分类假设训练数据中包含标记的多个正常类的实例（希尔顿等人[2013]，Jumutc和Suykens[2014]Kim等人[2015]，Erfani等人[2017]）。多等级的异常检测技术学习分类器来从类的其余异常类之间进行区分。一般地，监督异常检测深learning-基础的分类方案具有两个子网络，特征提取网络随后是分类器网络。深模型需要的训练样本（数千或数百万量级）有效地学习功能交涉判别不同类的实例有相当数量。由于缺乏干净的数据标签的可用性深监督异常检测技术是不那么受欢迎，因为半监督和无人监督的方法。计算复杂性：深的计算复杂性监督基于异常检测方法技术依赖于输入数据维数和隐藏层的数目使用反向传播算法进行训练。高维数据往往有更多的隐藏层，以确保输入的含义，完整层次学习酒店特色计算复杂度也与隐藏层的数量线性增加，需要更大的模型训练和更新时间。

优点和缺点：监督DAD法的优点如下：

•监督DAD方法比半监督和无人监督的模型更加准确。

19

表20：半监督DAD车型概述AE：自动编码，DAE：降噪自动编码，KNN：K-近邻寇根：损坏剖成对抗性网络，DBN：坚定信念网络AAE：对抗性自动编码，CNN：卷积神经网络SVM：支持矢量机器。

技术参考节

AE11.8节兹和范斯坦[2017]，Estiri和Murphy[2018]RBM11.1节Jia等人。[2014]DBN11.1节Wulsin等。[2010]，Wulsin等。[2011]科根，GAN第11.5节Gu等。[2018]Akcay等。[2018]，Sabokrou等。[2018]AAE11.5节Dimokranitou[2017年]混合模型（DAE-KNN奥特曼[1992]），（DBN-随机森林浩[1995]），CNN-救济基拉和伦德尔[1992]，CNN-SVM科尔特斯和Vapnik等人[1995年]

第8.3.1Song等人。[2017]，Shi等。[2017]，Zhu等人。[2018]

CNN11.6节拉卡等。[2017]，佩雷拉和帕特尔[2018]RNN11.7节Wu和普拉萨德[2018]GAN11.5节基里格和弗莱什曼[2018]，Gu等。[2018]

•基于分类技术测试阶段是快速的，因为每个测试实例需要对预先计算的模型进行比较。

是的监督DAD技术的缺点如下：

•多级监督的技术需要各种正常类和异常情况，这通常是不适用准确的标签。

•深度监督技术未能分开异常数据正常的，如果在特征空间是高度复杂和非线性的。

10.2半监督深刻的异常检测

半监督或（一类分类）DAD技术假定所有训练实例都只有一个类的标签。基于深学习半监督技术异常检测的综述由基兰等人提出。[2018]和Min等人。[2018]。DAD技术学会周围正常情况下的具有区分边界。该不属于多数类的测试实例标记为异常（佩雷拉和帕特尔[2018]，查德等人[2010]）。各种半监督DAD模型体系结构示于表20中所示。

假设：半监督提出要依靠以下假设的一个得分数据实例为异常DAD方法。

•接近和连续性：点，这是接近对方无论是在输入空间和学习的特征空间更可能共享同一个标签。

•强大的功能是深层神经网络层的隐藏层内学习并保留辨别属性从异常数据点分离正常。

计算复杂性：的计算复杂度半监督DAD方法为基础的技术是类似于监督DAD技术，其主要依赖于输入数据的维数和

20

表21：杂交DAD技术的实例。CNN：卷积神经网络，LSTM：长短期记忆网络DBN：坚定信念网络，DNN：深层神经网络。AE：自动编码，DAE：降噪自动编码，SVM：支持向量机科尔特斯和Vapnik等人[1995]SVDD：支持向量数据描述，RNN：回归神经网络的救济：特征选择算法基拉和伦德尔[1992]，KNN：K-近邻特曼[1992]CSI：捕获，分数，并集成Ruchansky等。[2017]。

技术参考节

AE-OCSVM，AE-SVM

11.8节，安卓等。[2016a]

DBN-SVDD，AE-SVDD

第11.1节，Erfani等。[2016a]，Kim等人。[2015]

DNN-SVM21DInoue等[2017年]DAE-KNN，DBN-随机森林浩[1995]，CNN-救济，CNN-SVM

第11.1,11.8

Song等人。[2017]，Shi等。[2017]，Zhu等人。[2018]，Urbanowicz等。[2018]

AE-CNN，AE-DBN11.1，11.6,11.8

王等人。[2018B]，Li等。[2015]

AE+KNN11.8节歌等。[2017]CNN-LSTM-SVM第11.6,11.7

卫[2017年]

RNN-CSI11.7Ruchansky等。[2017]CAE-OCSVM11.8节Gutoski等人，Dotti等。[2017]

用于代表特征学习隐藏层的数目。

优点和缺点：的优点深半监督异常检测技术是以下操：

在半监督学习模式的培训•剖成对抗性网络（甘斯）都表现出极大的承诺，即使有极少数的标签数据。

•使用标记的数据（通常是一类的），可生产unsu-pervised技术相当的性能改进。

由（鲁发[2009]）提出半监督技术的基本缺点，即使在深学习环境都适用。此外，隐藏层内提取的分层特征可能并不代表较少的反常实例因此是容易产生过拟合问题。

10.3混合深异常检测

深学习模型被广泛用作特征提取学习强大的功能（Andrews等[2016a]）。在深混合动力车型，深模型中了解到的代表性特点是输入像单级径向基函数（RBF），支持向量机（SVM）分类传统算法。所述混合模型采用两个步骤的学习和被示出为状态的最先进的生产结果（Erfani等人[2016a，b]上，Wu等人[2015B]）。在异常检测用深混合体系结构示于表21中。

假设：提出了异常检测深层混合模型依赖于以下假设来检测异常值之一：

•鲁棒特征在深神经网络的隐藏层内提取，有助于分离不相关特征，其可以隐藏异常的存在。

•建立在复杂的高维空间强大的异常检测模型需要特征提取和异常检测器。中使用的各种异常检测器地连同在表21中示出

计算复杂性：混合模型的计算复杂度包括所述以及传统的算法中使用的两个深的体系结构的复杂性。另外，深的网络结构和参数，是指在一个相当大的空间搜索优化的参数的非平凡的选择的一个固有问题介绍了使用混合模型内深层的计算复杂度。此外考虑到经典算法，例如线性

21

SVM其与d具有预测O（d）的复杂输入维数。对于大多数的内核，包括多项式和RBF中，复杂度为O（ND），其中n是支持向量的数目虽然近似值O（D2）被认为是与RBF内核支持向量机。

优点和缺点的混合DAD技术的优点如下：

•特征提取显著降低了“维数灾”，特别是在高维域。

•混合模型是更可扩展性和计算效率的，因为线性或非线性内核型号减少输入维度操作。

混合型DAD技术的显著缺点是：

•混合方法是次优的，因为它无法自通用损耗函数来代替定制目标异常检测特征提取器的hid-巢穴层内来影响代表性学习。

•较深混合模型往往效果更好，如果各个层是（萨克斯等人[2011]），其引入的计算开支。

10.4一类神经网络（OC-NN），用于异常检测

一类神经网络（OC-NN）结合深网络来提取地连同一类的目标，数据的逐渐丰富表征值的能力，诸如超平面（Chalapathy等[2018A]）或超球面（拉夫等[2018A]）来从所有异常值分离正常数据点。在OC-NN的方法是新颖的以下重要原因：在隐藏层的数据表示通过优化定制的异常检测的目标函数如在实验结果所示（了解到Chalapathy等[2018A]，拉夫等人。[2018A]）demon-施特拉特该OC-NN可以实现比现有的国家的最先进的方法复杂的数据集可比较的或更好的性能，同时具有合理的训练和测试时间比现有的方法。

假设：提出了异常检测的OC-NN模型依赖于以下假设检测OUT-liers：

•OC-NN模型提取深层神经网络的隐藏层内的数据分布内变化的常见因素。

•执行组合的表示学习并产生异常值的分数的测试数据实例。

•异常样品不含有变异的共同因素，因此隐藏层无法捕捉异常的表示。

计算复杂性：一个OC-NN模型的计算复杂度作为对IN-cludes混合模型唯一选择的深网络的复杂性（萨克斯等人[2011]）。OC-NN模型不要求数据存储进行预测，从而具有非常低的存储复杂。然而，很明显的是，OC-NN的训练时间是正比于输入尺寸。

是OC-NN的优点如下：优点和缺点：

•OC-NN模型联合训练深层神经网络，同时优化输出空间的数据，包含超球球化或超支平面。

•OC-NN提出的交替最小化算法学习OC-NN模型的参数。我们观察到OC-NN目标的子问题相当于解决这是良好定义的位数的选择问题。

OC-NN的异常检测的显著缺点是：

•培训时间和模型更新时间可长高维输入数据。

•模型的更新也将需要更长的时间，因为在输入空间的变化。

22

表22：的无监督DAD技术的例子。CNN：卷积神经网络，LSTM：长短期记忆网络DNN：深层神经网络，GAN：剖成对抗性网络AE：自动编码，DAE：降噪自动编码，SVM：支持向量机STN：空间变压器网络，RNN：回归神经网络AAE：对抗性自动编码，VAE：变自动编码。

技术参考节

LSTM11.7节辛格[2017]，Chandola等。[2008]，Dasigi和Hovy[2014]，马尔霍特拉等。[2015]AE11.8节阿巴蒂等。[2018]，宗等人。[2018]，Tagawa等的[2015]，斗等。[2014]，樱和Yairi[2014]Wu等。[2015A]，Xu等人。[2015]，Hawkins等。[2002]，Zhao等人。[2015]，Qi等。[2014]，Chalapathy等。[2017]，Yang等人。[2015]，Zhai等人。[2016]，Lyudchik[2016]，Lu等。[2017]，特拉等人。[2017]，Meng等人。[2018]，标准杆恰米等。[2017]STN11.2节Chianucci和Savakis[2016]GAN11.5节Lawson等人。[2017]RNN11.7节Dasigi和Hovy[2014]，Filonov等。[2017]AAE11.5节Dimokranitou[2017]，Leveau和乔利[2017]VAE第11.5节所述的和Cho[2015]，Suh等人。[2016]，S¨olch等。[2016]，Xu等人。[2018]，Mishra等人。[2017]

10.5无监督深层异常检测

无监督DAD是研究在这两个基本的机器学习研究和工业拖至应用程序的一个必要环节。在无监督异常检测地址的挑战，提出并显示产生如在表22中示出的自动编码国家的最先进的性能的几个深度学习框架是在异常检测中使用的无监督基本架构深（Baldi的[2012]）。

假设：提出了异常检测深无监督模型依赖于以下assump-蒸发散来检测异常值之一：

•在原来的或潜在的功能空间“正常”区域可以从原始的或潜在的功能空间“反常”的区域区分开来。

•相比所述数据集的剩余部分中的大部分数据的情况下是正常的。•无监督异常检测算法产生的数据实例的离群得分基于的固有特性的数据集，例如距离或密度。深层神经网络的隐藏层的目的是捕获数据集内的这些固有特性（Goldstein和内田[2016]）。

计算复杂性：该自动编码在与二次成本离群点检测所采用的最常见的结构，最优化问题是非凸的，类似于任何其他神经网络结构。模型的compu-tational复杂性取决于运营，网络参数和隐层的数目。然而，训练自动编码器的计算复杂度是比传统的方法如主成分分析（PCA），因为PCA是基于矩阵分解高得多（Meng等人[2018]，Parchami等人[2017]）。

优点和缺点：无监督深异常检测技术的优点如下：

•获知固有数据特征从一个异常数据点分开正常。数据并且便于离群点检测中这种技术识别共性。

•具成本效益的技术，以找到异常，因为它不需要训练algo-rithms注释的数据。

无监督深异常检测技术的显著缺点是：

•往往是具有挑战性的学习数据中的共性在一个复杂和高维空间。•在使用自动编码压缩的右度的选择，即，降维经常是一个超参数，需要以获得最佳效果调谐。

23

•无监督技术技术对于噪声非常敏感，数据损坏和往往比监督或半监督技术更少accu-率。

10.6杂项技术

本节探讨，这是证明是有效的和有前途的各种DAD技术，我们讨论这些技术及其应用领域背后的关键思想。

10.6.1迁移学习基于异常检测

深度学习长期被批评为需要有足够的数据来产生良好的结果。无论Litjens等。[2017]和Pan等。[2010]目前深陷转会学习的方法进行审查，并说明其意义学习很好的功能表示。转移学习是机器学习的必备工具来解决训练数据不足的根本问题。它的目的是通过放松假设训练和未来的数据必须是在同一个特征空间，并具有相同的分布从源域转移知识的目标域。深陷转会表示学习已经由（Andrews等人探讨。[2016B]，Vercruyssen等人[2017]，李等人[2012]，Almajai等人[2012]，Kumar和瓦德站[2017]良等[2018]）被示出，以产生非常有希望的结果。利用传送学习异常检测的开放式研究的问题是，转移能力，这是定义的程度如何拥有从一个任务转移的知识，提高分类性能到另一个。

10.6.2零射门学习基于异常检测

零出手学习（ZSL）旨在表彰训练组中从未有过的对象（Romera，帕雷德斯和托[2015年]）。ZSL实现这两个阶段：首先约在自然语言描述或属性中的对象（俗称元数据）的知识被捕获其次然后这种知识一组新的类之间的用于分类的实例。因为一个可能不能在训练获得所有可能的类的图片此设置在现实世界中很重要的。这种方法相关的主要挑战是获得元数据有关数据的实例。在异常和新颖性检测使用ZSL的但是几种方法被示出状态的最先进的生产结果（Mishra等人[2017]，Socher等人[2013]，冼等人[2017]，Liu等人[2017]，里韦罗等人[2017]）。

基于异常检测10.6.3合奏

深神经网络的一个显着的问题是，它们对输入的数据内的噪声敏感，并且通常需要大量的训练数据来执行鲁棒（Kim等人[2016]）。为了在有噪声的数据甚至实现鲁棒性的想法对自动编码器的连接结构随机变化被示出为获得显著更好的性能。由各种随机连接自动编码的自编码合奏由Chen等人实验。[2017年]达到几个标准数据集可喜的成果。合奏方法仍然已经显示出产生改善的分集，从而避免过拟合问题，同时减少训练时间的研究的活跃领域。

基于异常检测10.6.4聚类

基于聚类的几个异常检测算法已经在文献中提出（酯类等。[1996]）。Clus-的TeringBay涉及分组基于特征相似的模式一起提取检测新的异常。的时间和空间复杂度与类要群集数线性增长（斯里卡特等人[2010]），这使得基于实时实际应用异常检测望而却步聚类。输入数据的维数降低提取深层神经网络的隐藏层这确保可扩展性复杂和高尺寸的数据集内的特征。深度学习支持群集的方法异常检测利用e.gword2vec（Mikolov等[2013]）模式以获得正常的数据和异常的语义介绍，以形成集群和检测异常值（元等。[2017年]）。作品多次依靠混合模型的变种，支持自动编码器获得群集能够发现异常代表性特征一起。

基于异常的检测10.6.5深强化学习（DRL）

深强化学习（DRL）方法已经吸引了显著兴趣，因为其学习复杂的行为，在高维数据空间的能力。检测力度使用深强化学习异常已提出德拉Bourdonnaye等。[2017年]，成强黄[2016年]。异常检测器基于的DRL不考虑有关异常，探测器识别到新的异常始终如一的概念，任何假设

24

通过提高累积回报信号的知识。DRL基于异常的检测是一个非常新颖的概念，需要研究的空白，它的应用进一步调查和鉴定。

10.6.6统计技术深异常检测

希尔伯特变换是统计信号处理技术，其导出实值信号的解析表示。该属性是通过利用用于与健康相关的时间序列数据集异常实时检测（Kanarachos等人[2015]），并示出是一种非常有前途的技术。本算法结合小波分析，神经网络和希尔伯特的能力以顺序的方式变换检测实时异常。统计技术DAD技术的话题还需要进一步调查，充分了解自己的潜力和适用性的异常检测。

11层深层神经网络结构的定位异常

11.1深层神经网络（DNN）

“深”中的“深神经网络”指的是层的，通过该数据的特征被提取的数（施米德休伯[2015]，Bengio等人[2009]）。深架构克服了传统机器学到，ING的限制可扩展性的方法，并概括于数据中的需要人工特征工程新变化（等人[2015]LeCun）和。深信念网络（动态贝叶斯网）是类，它包括被称为受限玻尔兹曼机（RBMS）图形模型mul-tiple层深的神经网络。在使用动态贝叶斯网异常检测的假设是，RBMS用作定向编码器-解码器网络与BP算法（Werbos[1990]）。动态贝叶斯网不能捕捉到异常样品的特性变化，从而导致高recon-结构调查错误。动态贝叶斯网被示为有效地扩展到大的数据和改善解释性（Wulsin等人[2010]）。

11.2时空时空网络（STN）

长期研究人员探讨技术学习的空间和时间关系的特征（Zhang等人[2018F]）。深度学习架构是杠杆在学习空间方面（CNN使用的）和TEMporal功能（使用LSTMs）分别表现良好。时空时空网络（设定的STN）包括组合这两个CNN的和LSTMs提取时空特征深层神经架构。的时间特征（建模经由LSTM附近的时间点之间的相关性），空间特征（建模经由本地CNN的局部空间相关性）被证明是有效的检测离群点（Lee等人[2018]，SZEK'ER[2014]，啮等人[2018]，Dereszynski和Dietterich[2011]）。

11.3和积网络（SPN）

积和网络（SPN）在向无环图与变量叶，以及内部节点，和加权边缘构成的总和和产品。的SPN被认为是具有超过许多层的快速精确概率推理混合物模型的组合（潘和多明戈斯[2011]，Peharz等人[2018]）。结节的主要优点是，与图形模型，结节超过高树宽机型更可跟踪，而无需近似推理。此外，的SPN被示出为捕获不确定性其输入以令人信服的方式，得到坚固的异常检测（Peharz等人[2018]）。结节被证明是在许多数据集骄人的成绩，同时仍有许多关于异常检测有待进一步探讨。

11.4Word2vec模型

Word2vec是用于产生字的嵌入一组深神经网络模型（Mikolov等人[2013]）。这些模型能够捕获诸如语句，时间序列数据的数据实例中的顺序关系。获得字嵌入特征作为输入被示出，以改善在几个深度学习功能architec-性能（Rezaeinia等人[2017]，耐立等人[2017]，Altszyler等人[2016]）。异常撬动word2vec的嵌入检测模型被示出为显著提高性能（施纳贝尔等人[2015]，Bertero等人[2017]，Bakarov等人[2018]，Bamler和MANDT[2017]）。

11.5生成模型

生成模型的目的是学习，以产生具有一些变化的新的数据点的确切数据分布。两种最常见和有效的生成方法是变自动编码（VAE）（金玛和威灵

25

[2013]）与生成对抗式网络（GAN）（Goodfellow等人[2014A，B]）。GAN架构称为对抗性自动编码（AAE）的变体（Makhzani等人[2015]）使用对抗性训练强加也示于自动编码器的隐藏层内学到的潜代码的任意之前有效地学习输入分布。利用学习输入分布，几个剖成对抗性网络为基础的异常检测（GAN-AD）的框架的这种能力（Li等人。[2018]，Deecke等人[2018]，Schlegl等人[2017]，Ravanbakhsh等人[2017b]，艾德[2018]）提议被示为有效地识别高维和复杂的数据集的异常。然而传统的方法如K最近邻（KNN）被示为在比较深生成模型时，其具有更少数量的异常的情况下表现得更好（Skv'ara等人[2018]）。

11.6卷积神经网络

卷积神经网络（CNN），是神经网络的用于分析的视觉图像的流行的选择（Krizhevsky等人[2012]）。CNN的从具有复杂结构的高维数据中提取复杂隐藏的功能能力，使其作为特征提取器使用在对顺序和图像数据集离群点检测（Gorokhov等人[2017]，金[2014]）。异常检测CNN的基于框架的评价目前仍然是活跃的研究领域（Kwon等人[2018]）。

11.7序列模型

回归神经网络（RNNs）（威廉姆斯[1989]）被示为捕获时间序列数据的功能。与RNNs的限制是，它们不能捕捉上下文随着时间的步骤的增加，为了解决此问题，长短期存储器（Hochreiter和施米德休伯[1997]）网络进行了介绍，它们是包括RNNs的特定类型的可存储约一时间步骤的信息的存储单元。门控重复单元（Cho等人[2014]）（GRU）类似于LSTMs，而是使用一组门的控制的信息的流动，而不是单独的存储器单元。异常检测在顺序数据吸引在文献显著兴趣，因为它在宽范围的在第9.9节中所示的工程问题的应用程序。长短期记忆（LSTM）基于神经网络的算法异常检测已经研究并报道，以产生相对于常规方法显著性能增益（厄根等人[2017]）。

11.8自动编码

与具有线性激活函数沿单层自动编码几乎等同于主成分分析（PCA）（皮尔逊[1901]）。虽然PCA被限制为线性维数降低，自动编码器同​​时启用线性或非线性tranformations（远流等[2008，2014]）。一个自动编码的流行的应用是异常检测。自动编码也由名称复制神经网络（RNN）引用的（Hawkins等人[2002]，Williams等人[2002]）。自动编码通过重构所述输入数据，从而有效地学习恒等函数表示多个隐藏层内的数据。在自动编码，在-姿态（这是大多数在异常检测任务）对正常数据单独训练时，不能重构异常数据样本，因此，产生大的重构误差。其产生高的残余误差的数据样本被认为是异常值。提出了自动编码器的体系结构的几种变体，如在异常检测图13中的农产品有希望的结果示出。自动编码器体系结构的选择取决于数据的性质，卷积网络是优选的图像数据组，而基于长短期记忆（LSTM）模型倾向于以产生用于顺序数据良好的结果。努力都卷积和LSTM层，其中所述编码器是卷积神经网络（CNN）和解码器是多层LSTM网络来重构输入图像组合被证明是有效的在数据内检测异常。使用组合模型，如门控重复单元自动编码（GRU-AE），卷积神经网络自动编码（CNN-AE），长短期记忆（LSTM）的自动编码（LSTM-AE）消除了准备手工制作的功能需求并有利于在异常检测任务，用最少的预处理使用原始数据。虽然自动编码是异常检测简单而有效的架构，性能被破坏，原因是嘈杂的训练数据（Zhou和Paffenroth[2017年]）。

12个的相对优势和劣势：深异常检测方法

每一个在前面的章节中讨论的深异常检测（DAD）技术有其独特的优势和劣势。关键是要了解哪些异常检测技术是最适合于一个给定的异常检测的问题上下文。鉴于DAD是一个活跃的研究领域，这是不可行的为每一位异常检测等问题的理解。因此，在本节中，我们分析了几个简单的问题设置的相对优势和不同类别的技术弱点。在第10.1节中所示的基于分类监督DAD技术是在场景中更好的选择由等量的标签的对于正常

26

自动编码

连续数据

SDAEAEGRU-AELSTM-AE

图片

DAECNN-LSTM-AECNN-AECAE

图13：自动编码器架构用于异常检测。AE：自动编码利乌等。[2014]，LSTM：长短期记忆网络Hochreiter和施米德休伯[1997]SDAE：叠放消噪自动编码器Vincent等人。[2010]，DAE：去噪自动编码Vincent等人。[2010]GRU：门控重复单元Cho等。[2014]，CNN：卷积神经网络Krizhevsky等。[2012]CNN-LSTM-AE：卷积长短期记忆自动编码哈克等人。[2018]CAE：卷积自动编码Masci等人。[2011]

和反常情况。监督DAD技术的计算复杂性是一个关键的方面，特别是当技术应用于真实的域。虽然基于分类，监督或半监督的技术有昂贵的培训，测试通常是快，因为它使用一个预先训练模式。在第10.5节呈现无监督DAD技术被广泛使用，因为标签获取是一个昂贵和费时的过程。大部分的无监督深刻的异常检测的要求先验被假定的异常分布因此模型在处理噪声数据不太可靠。混合模型在第10.3节提取物强大的功能示为效果最好的经典异常检测算法的深层神经网络和进料的隐藏层内。混合模式的做法是不理想的，因为它无法在隐藏层影响代表性学习。在第一个超平面，例如10.4联合深网络以提取与所述一个级目标，沿数据的逐渐丰富表示的能力所描述的一类神经网络（OC-NN）（Chalapathy等[2018A]）或超球面（拉夫等人[2018A]）与所有正常数据点从异常数据点分开。进一步的研究和探索是必要的理解更好地提出这个新架构的优势。

13结论

在本次调查文章中，我们已经讨论了在深学习型异常检测各种研究方法以及它在各个领域的应用。本文讨论了深刻的异常检测，并提出应对这些挑战的几个现有解决方案的挑战。对于深部异常检测技术，每个类别中，我们提出了关于与它的优势和劣势沿着正常和异常数据的概念的假设。本次调查的目的是调查和识别各种深度学习模型的异常检测和评估其是否适合给定的数据集。当选择一个深学习模型到特定域或数据，这些假设可以被用作准则来评估在该域的技术的有效性。基于异常的检测深度学习仍是活跃的研究，以及可能的未来工作将是扩展和更复杂的技术，提出了更新此调查。

Varun的Chandola，阿瑞丹姆班纳吉和Vipin库马尔。异常检测：调查。ACM计算机调查，2007年。

D.霍金斯。异常数据的识别。查普曼和霍尔，伦敦，1980年。

艾哈迈德Javaid，Quamar尼牙孜，卫青Sun和曼苏尔阿拉姆。网络入侵检测系统中的深学习方法。在9日EAI国际会议论文集仿生信息和COM的munications科技（前身为BIONETICS），21-26页。ICST（学院计算机科学，社会-信息与通信工程），2016年

焕凯鹏和拉杜Marculescu。多尺度组合性：识别使用深度学习社会动态的组成结构。公共科学图书馆·一个，10（4）：e0118309，2015。

27

Bahnsen亚历杭德罗·科雷亚。建筑采用的AI深学习应用。2016年URL的https：//blog.easysol。净/可湿性粉剂内容/上传/2017年/06/image1.png。

雪梅谢晨晔王，陈舒，光明石和芝罘赵。基于深度学习实时违章停车检测系统。在深学习技术，23-27页2017年国际会议论文集。ACM，2017年。

托马斯Schlegl，菲利普Seeb¨ock，塞巴斯蒂安Waldstein酒店中号，乌苏拉·施密特Erfurth，和GeorgLANGS。无监督异常检测与生成对抗网络引导标志物的发现。在国际会议上的信息处理在医学影像，146-157页。斯普林格2017年。

迈赫迪·穆罕默迪，阿拉巴马州的Al-教法学家，萨迈赫苏鲁尔和穆赫辛Guizani。深学习IOT大数据和流分析：调查。预印本的arXiv的arXiv：1712.04301，2017年。

CharuÇAGGARWAL。介绍了异常值分析。在异常值分析，1-40页。斯普林格，2013。

DubravkoMiljkovi'c。回顾新奇的检测方法。在MIPRO，第33届国际公约的2010和程序，593-598页。IEEE，2010。

马可·皮门特尔AF，大卫克利夫顿，雷克利夫顿，和莱昂内尔·塔拉桑科。新颖性检测的审查。信号处理，99：215-2492014。

Donghwoon权，贤珠金，金Jinoh，丙桑徐，IkkyunKim和KuinamĴ金。深学习型网络异常检测的调查。集群计算，1-13，2017年页。

John发球，德里克·安德森牛逼，并赐僧灿。理论，工具，为社会的挑战：在遥感深度学习的综合考察。[应用的遥感，11（4）：042609，2017年。

乙拉维基兰，迪利普马修·托马斯，和兰芝斯Parakkal。对于unsu-深度学习为基础的方法的概述pervised和半监督在视频异常检测。预印本的arXiv的arXiv：1801.03149，2018。

AderemiØAdewumi和洛尼克斯一个Akinyelu。机器学习和自然灵感基于信用卡欺诈检测技术的调查。国际期刊系统保证工程与管理，8（2）的：937-953，2017年。

海尔特Litjens，Thijs的KOOI，巴巴克EhteshamiBejnordi，阿尔诺ArindraAdiyosoSETIO，弗朗西斯琼皮，穆赫辛Ghafoorian，吉荣AWM范德Laak，布拉姆范Ginneken，和克拉拉我S'anchez。在医学图像分析深度学习的调查。医学图像分析，42：60-88，2017年。

萨拉中号Erfani，SutharshanRajasegarar，沙尼卡·卡伦西克拉，和克里斯托弗·莱基。高维和大规模异常检测用线性一个类SVM深学习。模式识别，58：121-134，2016a。

RaghavendraChalapathy，阿迪亚梅农和桑杰·乔拉。异常检测使用的一类神经网络。预印本的arXiv的arXiv：1802.06360，2018A。

亚·莱卡，约书亚·本焦，和杰弗里·辛顿。深度学习。自然，521（7553）：436，2015年。

丹尼尔Ramotsoela，阿德南·阿布·福兹，和GerhardHancke。在临界水系统基础设施的情况下研究工业无线传感器网络的异常检测的调查。传感器，18（8）：2491，2018。

RaghavendraChalapathy，伊赫桑扎雷Borzeshi，和MassimoPiccardi。药物名称识别复发性神经architec-功能的调查。预印本的arXiv的arXiv：1609.07585，2016a。

RaghavendraChalapathy，伊赫桑扎雷Borzeshi，和MassimoPiccardi。双向LSTM-CRF临床概念提取。预印本的arXiv的arXiv：1611.08373，2016B。

DrausinWulsin，贾斯汀·布兰科，拉姆摩尼和布莱恩利特。半监督异常检测使用的坚定信念网脑电图波形。在机器学习和应用（ICMLA），2010年第九届国际会议，436-441页。IEEE，2010。

Mutahir纳迪姆，Ochaun马歇尔，Sarbjit辛格，方兴，和晓红元。半监督的网络入侵检测深层神经网络。2016年

宏超宋，竹青江，爱东男人，和博扬。一种混合半监督用于高维数据的异常检测模型。计算智能和神经科学，2017年，2017年。

28

约什-帕特森和亚当·吉布森。深度学习：一个从业者的研究方法。”O'ReillyMedia公司”，2017年。

亚伦Tuor，塞缪尔·卡普兰，布莱恩·哈钦森，妮可·尼科尔斯和肖恩·罗宾逊。深度学习在结构化网络安全数据流，无人监管的内部威胁检测。预印本的arXiv的arXiv：1710.00811，2017年。

斯万特·沃尔德，金Esbensen，和保罗Geladi。主成分分析。化学计量学和智能实验室系统，2（1-3）：37-52，1987。

科琳娜科尔特斯和弗拉基米尔·万普尼克。支持矢量网络。机器学习，20（3）：273-297，1995。

飞刘永，启冥寿，和周志华。隔离森林。在数据挖掘，2008年ICDM'08。第八届IEEE国际会议，413-422页。IEEE，2008。

伊利亚Sutskever，杰弗里·ê韩丁和格雷厄姆w^泰勒。复发时间受限玻尔兹曼机。在神经信息处理系统，1601-1608页，2009年进展。

鲁斯兰Salakhutdinov和雨果拉罗歇尔。深玻耳兹曼机的高效学习。在人工智能和统计，693-700页，2010第十三届国际会议论文集。

帕斯卡尔·文森特，雨果拉罗歇尔，约书亚·本焦，和皮埃尔-安托万Manzagol。提取和合成强大的功能与降噪自动编码。在机器学习，1096-1103页的第25届国际会议论文集。ACM，2008。

保罗·罗德里格斯，珍妮特·怀尔斯，和Jeffrey大号埃尔曼。反复出现的神经网络学会了算。连接科学，11（1）：5-40，1999年。

纪尧姆Lample，米格尔·罗斯，桑迪普萨勃拉曼尼亚，哉川，和克里斯-戴尔。神经architec-功能的命名实体识别。预印本的arXiv的arXiv：1603.01360年，2016年。

JeroneTA安德鲁斯，爱德华Ĵ莫顿和路易斯d格里芬。检测使用自动编码器的异常数据。Interna-周志武杂志机器学习和计算，6（1）的：21，2016a。

Sinno加林潘，杨强等。在迁移学习的调查。知识和数据工程，22IEEE交易（10）：1345年至1359年，2010。

托加耳根，阿里·哈桑·米尔扎和苏莱曼塞尔达尔Kozat。无监督和半监督与LSTM神经网络异常检测。预印本的arXiv的arXiv：1710.09207，2017年。

卢卡斯·鲁夫，尼科G¨ornitz，卢卡斯Deecke，邻省艾哈迈德·西迪基，罗伯特Vandermeulen，亚历山大活页夹，EM-曼努埃尔·穆勒，和马吕斯Kloft。深一类分类。在国际会议上机器学习，4390-4399页，2018A。

亚·莱卡，科琳娜科尔特斯，和克里斯托弗JC伯吉斯。MNIST手写数字数据库。AT＆T实验室[在线]。可用：HTTP：//晏。lecun。COM/exdb/MNIST，2，2010。

亚历克斯Krizhevsky和杰弗里·辛顿。学习从微小的图像特征多层。技术报告，2009年。

Xiuyao宋，吴明溪，克里斯托弗杰梅因和桑杰Ranka。有条件的异常检测。631-645，2007：知识与数据工程，19（5）IEEETransac-蒸发散。

塞普·霍赫里特和尤尔根·施米德赫伯。长短期记忆。神经计算，9（8）：1735至80年，1997年。

闵读，菲菲李，郑Guineng和维韦克Srikumar。Deeplog：异常检测和诊断，从通过深入学习系统日志。在计算机和通信安全，1285年至1298年网页2017年ACMSIGSAC会议论文集。ACM，2017年。

迈克尔·海斯和仪AMCapretz。对于大的传感器数据的上下文异常检测框架。轴颈大数据，2（1）：2，2015年。

RaghavendraChalapathy，爱德华·托特和桑杰·乔拉。采用深生成模型组异常检测。预印本的arXiv的arXiv：1804.04876，2018B。

LOIC邦当，詹姆斯·麦克德莫特，Nhien安乐Khac等。基于长短期记忆回归神经网络集体异常检测。在国际会议未来数据和安全工程，141-152页。斯普林格年，2016年。

29

丹尼尔乙阿拉亚，卡塔琳娜托Grolinger，哈尼˚FElYamany，仪AMCapretz和GBitsuamlak。集体CON组文本异常检测的智能建筑框架。在神经网络（IJCNN）年，2016年在国际联席会议，511-518页。IEEE2016。

Naifan庄，TuoerhongjiangYusufu，叶军，和健阿华。小组活动识别与鉴别再当前卷积神经网络。在自动面部及手势识别（FG2017年），2017年第12届IEEE国际会议，页526-531。IEEE，2017年。

卢卡斯拉夫，罗伯特Vandermeulen，尼科Goernitz，卢卡斯Deecke，邻省艾哈迈德·西迪基，亚历山大活页夹，EM-曼努埃尔·穆勒，和马吕斯Kloft。深一类分类。在珍妮弗Dy和安德烈亚斯·克劳斯，编辑，第35届国际会议上机器学习，机器学习研究论文集的第80卷，第4393-4402，的Stockholmsmässan，瑞典斯德哥尔摩，7月10日至一十五日2018B的诉讼。PMLR。URLhttp://proceedings.mlr.press/v80/ruff18a.html。

虚象VPhoha。互联网安全字典，第1卷泰勒＆弗朗西斯，2002年。

焦万娜豇豆和克里斯托弗Kruegel。基于主机的入侵检测。2005年。

Gyuwan金，Hayoon毅，李江河，Yunheung白南舜和Sungroh尹。基于LSTM系统调用语言建模和设计基于主机的入侵检测系统强大的集成方法。预印本的arXiv的arXiv：1611.01726年，2016年。

阿诗玛乔拉，布赖恩·李，希拉伦，和保罗·雅各布。基于主机的入侵检测系统联合CNN/RNN模型。第二次国际研讨会对AI的法律程序中的安全，2018。

李晨，萨尔明苏丹娜，和拉维Sahita。Henet：有效英特尔R⃝处理器跟踪深学习方法开发的检测。在2018IEEE安全与隐私研讨会（SPW），109-115页。IEEE，2018。

索罗什中号Sohi，Fatemeh赶集网和让-皮埃尔·塞弗特。递归神经网络用于增强基于特征的网络入侵检测系统。预印本的arXiv的arXiv：1807.03212，2018。

řVinayakumar，KP索曼和PrabaharanPoornachandran。申请网络入侵检测卷积神经网络。在计算，通信和情报（ICACCI），2017年国际会议上的进展，1222年至1228年的网页。IEEE，2017年。

HojjatAghakhani，亚拉文Machiry，希林Nilizadeh，克里斯托弗Kruegel，和Giovanni豇豆。检测使用生成对抗网络欺诈的评论。预印本的arXiv的arXiv：1805.10364，2018。

李丹，陈大成，乔纳森吴作栋，看-kiong伍。异常检测与多元时间序列生成对抗性的网络。预印本的arXiv的arXiv：1809.04758，2018。

倪稿，凌高，全利高，与王海。基于坚定信念网络的入侵检测模型。在先进的云和大数据（CBD），2014年第二次国际会议，247-252页。IEEE2014。

罗伯特Peharz，安东尼Vergari，卡尔Stelzner，亚历杭德罗·莫利纳，马丁特拉普，克里斯蒂安Kersting和佐宾·拉马尼。概率学深用随机积网络。预印本的arXiv的arXiv：1806.01910，2018。

穆罕默德法赫德乌默尔，穆罕默德谢尔，以及亚新碧。一种基于流两级入侵检测模型用于下一代网络。公共科学图书馆·一个，13（1）：e0180945，2018。

杨禹俊龙和治平蔡。通过堆叠扩张卷积编码autoen-网络入侵检测。安全和通信网络，2017年，2017年。

VrizlynnLL的事情。IEEE802.11网络异常检测和攻击分类：深学习方式。在无线通信和网络会议（WCNC），2017年IEEE，1-6页。IEEE，2017年。

米哈伊尔Zolotukhin，蒂莫H¨am¨al¨ainen，泰罗Kokkonen和亚尔莫Siltanen。通过在加密流量检测应用层DDoS攻击增加Web服务的可用性。在电信（ICT）在2016年第23届国际会议，1-6页。IEEE2016。

卡洛斯·科尔德罗Garc'ıa，萨沙Hauke，最大M¨uhlh¨auser和马蒂亚斯菲舍尔。分析基于流的使用复制的神经网络异常intru-锡安检测。在隐私，安全和信任（PST）在2016年第14届年会，第317-324页。IEEE2016。

三十

哈立德Alrawashdeh和卡拉·珀迪。对基于深度学习在线异常入侵检测系统。在机器学习和应用（ICMLA）在2016年第15届IEEE国际会议，195-200页。IEEE2016。

疃唐，卢特菲Mhamdi，德麦克莱诺恩，赛义德·阿里·拉扎扎伊迪，并穆尼尔Ghogho。在软件定义网络的网络入侵检测深刻的学习方法。在无线网络和移动通信（WINCOM）在2016年国际会议，258-263页。IEEE2016。

曼努埃尔·洛佩斯-马丁，贝伦卡罗，安东尼奥·桑切斯-Esguevillas，和Jaime滨海略。条件变autoen-编码器，用于预测和恢复功能应用到入侵检测在IOT。传感器，17（9）：1967，2017年。

Majjed铝Qatf，穆罕默德Alhabib，卡迈勒铝Sabahi等。深学习方法稀疏AUTOEN编码器结合了支持向量机的网络入侵检测。IEEE访问，2018。

Yisroel米尔斯基，托梅尔Doitshman，尤瓦Elovici和阿萨夫Shabtai。狐狸：自动编码在线网络入侵检测的合奏。预印本的arXiv的arXiv：1802.09089，2018。

R可以Aygun和A格克汗Yavuz的。网络异常检测与随机改进的基于自编码模式。在网络安全和云计算（CSCloud），2017年IEEE第四届国际会议，193-198页。IEEE，2017年。

子龙林，勇士，和Zhi学研究。Idsgan：攻击一代对入侵检测剖成对抗网络。预印本的arXiv的arXiv：1809.02077，2018。

川隆阴，岳飞朱，刘胜利，金龙飞，和鹤童张。使用生成对抗网络僵尸网络去tection的增强框架。在人工智能和大数据2018国际会议（ICAIBD），228-234页。IEEE，2018。

马库斯戒指，丹尼尔Schl¨or，迪特·兰德斯和AndreasHotho。使用根儿ative对抗性的网络流量，基于网络流量的产生。预印本的arXiv的arXiv：1810.07795，2018。

迈季拉塔。当深度学习满足安全。预印本的arXiv的arXiv：1807.04739，2018。

YotamIntrator，吉拉德卡茨和阿萨夫Shabtai。Mdgan：使用\多鉴别gen-erative对抗网络推进异常检测。预印本的arXiv的arXiv：1810.05221，2018。

松原隆，立花良介和邦明上原。异常机械部件的检测与非正规得分深根儿ative模型。在2018国际联席会议神经网络（IJCNN），1-8页。IEEE，2018。

米格尔·尼古，詹姆斯·麦克德莫特等。一种混合自动编码器和密度估计模型异常检测。在国际会议上的并行问题从本质解决，717-726页。斯普林格年，2016年。

玛丽亚Rigaki。对抗性深度学习对入侵检测分类，2017年。

仅限RiteshķMalaiya，Donghwoon权，Jinoh金，丙桑徐，赵贤金，并Ikkyun金。实证evalua-深度学习网络异常检测的重刑。在计算，网络和通信2018国际会议（ICNC），893-898页。IEEE，2018。

Donghwoon权，Kathiravan纳塔拉，丙桑徐，赵贤金，并Jinoh金。在网络异常检测的实证研究使用卷积神经网络。在分布式计算系统2018IEEE第38届国际大会（ICDCS），1595年至1598年的网页。IEEE，2018。

拉尔夫ÇStaudemeyer。运用长短期记忆回归神经网络的入侵检测。南非计算机学报，56（1）：136-154，2015年。

Sheraz纳瑟尔，亚西尔·萨利姆，谢赫扎德哈立德穆罕默德Khawar巴希尔，击昏汉，穆罕默德·伊克巴尔Munwar和图Kijun汉。基于深层神经网络的增强型网络异常检测。IEEE访问，6：48231-48246，2018。

加州大学圣地亚哥分校异常检测数据集。2017年。

阿里Shiravi，哈迪Shiravi，MahbodTavallaee和阿里说的格尔巴尼。对发展一个系统的方法来生成入侵检测标准数据集。计算机与安全性，31（3）：357-374，2012。

31

阿米特亚当埃胡德·里夫林，宜兰Shimshoni和DavivReinitz。健壮实时异常事件检测使用多个固定位置的显示器。555-560，2008：模式分析与机器智能，30（3）IEEE交易。

川隆阴，岳飞朱，金龙飞，和新郑他。使用递归神经网络的入侵检测深深的学习方法。IEEE访问，5：21954-21961，2017年。

马哈茂德优素菲，阿扎尔，维杰Varadharajan，莱恩Hamey，和乌代Tupakula。基于自动编码器，功能为学习网络安全应用。在神经网络（IJCNN），2017年在国际联席会议，页3854-3861IEEE，2017年。

的Shahriar穆罕默迪和阿明Namadchian。使用模因分类异常基地ID的新的深学习方法。国际计算机学报，通信和控制，12（5），2017。

ĴStolfo，范伟，李文科，安德烈亚斯Prodromidis，和菲利普K更改。基于成本的建模和数据与应用欺诈和入侵检测挖掘评价。从JAM项目成果由萨尔瓦多，1-15个，2000页。

阮成凡，陈玉Thinh的，和乐青萨克。采用深度学习异常基于网络的入侵检测系统。在系统科学与工程（ICSSE），2017年国际会议，页210-214IEEE，2017年。

罗曼Fontugne，皮埃尔Borgnat酒店，帕特里斯Abry和福田健介。Mawilab：自动化异常标签和性能基准测试相结合多样化的异常去tectors。在第六届国际会议，第8页ACM，2010年提起诉讼。

应用科学，真实的全球网络环境（rgce）的Jamk大学。2009年。

吉迪恩·克里奇和建坤胡。使用不连续的contiguousand系统调用模式的语义的方法来基于主机的入侵检测系统。IEEETRANSACTIONSON计算机，63（4）：807-819，2014。

新墨西哥大学。计算机免疫系统的数据集。2012。

阿伊莎阿卜杜拉·穆罕默德·AizainiMaarof和Anazida伊纳尔。欺诈检测系统：调查。杂志的网络和计算机应用，68：90-1132016。

迪迪埃;等Lavion。普华永道全球经济犯罪和欺诈调查2018年PwC.com，2018年URL的https：//WWW。pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf。

露西马赵。欺诈检测系统，12月12日2013年美国专利申请。13/494741。

SamanehSorournejad，扎赫拉Zojaji，礼萨·埃布拉希米Atani和阿米尔·哈桑Monadjemi。信用卡欺诈检测技术的调查结果显示：数据和技术为导向的观点。CORRABS/1611.06439年，2016年。

周迅，马思聪程，梦竹，成昆郭思达周，彭旭，振华雪和尉氏张。数据的艺术调查的国家矿业为基础的欺诈检测和信用评分。在会议的MATEC网络，成交量189页03002.EDP科学，2018。

小号Suganya和NKamalraj。信用卡欺诈检测调查。国际计算机科学与移动计算，4：241-244，2015年。

马可施赖尔，帖木儿Sattarov，达米安博思，安德烈亚斯Dengel和贝恩德默。采用深的自动编码网络的大规模会计数据异常的检测。预印本的arXiv的arXiv：1709.05254，2017年。

罗伊楔形，詹姆斯·马克斯·坎特，圣地亚哥德卢比奥，塞尔吉奥·伊格莱西亚斯·佩雷斯和格利扬Veeramachaneni。解决欺诈预测的”误报”的问题。预印本的arXiv的arXiv：1710.07709，2017年。

Ebberth大号葆，马塞洛拉代拉，隆美尔Ñ卡瓦略和蒂亚戈Marzag~ao。深度学习异常检测，如巴西出口和反洗钱支持欺诈调查。在机器学习和应用（ICMLA）在2016年第15届IEEE国际会议，954-960页。IEEE2016。

马丁Renstr¨om和TimothyHolmsten。欺诈检测与监督的机器学习，2018无标签的数据。

萨拉·卡齐米和HoumanZarrabi。使用深层网络在信用卡交易中的欺诈检测。在基于知识的工程与创新（KBEI），2017年IEEE第四届国际会议，网页0630-0633.IEEE，2017年。

32

盼盼郑，蜀汉元，吴新涛，李军，和爱东陆。一类对抗网的欺诈检测。预印本的arXiv的arXiv：1803.01798，2018A。

ApapanPumsirirat和柳岩。信用卡欺诈检测采用深度学习基于自动编码器并重新strictedBoltzmann机。国际杂志计算机科学和APPLI-阳离子，9：（1）：18-25，2018。

KRSeeja和MasoumehZareapoor。Fraudminer：基于频繁项集挖掘的新型信用卡欺诈检测模型。科学世界日报，2014年，2014年

汤姆Sweers，汤姆Heskes，和杰西Krijthe。Autoencoding信用卡诈骗罪。2018。

乌戈·菲奥雷，阿尔弗雷多·德桑蒂斯，弗朗西斯佩拉，保罗·扎内蒂和弗朗西斯帕尔米耶。使用生成对抗性的网络对于提高信用卡欺诈检测分类效果。信息科学，2017年。

Hyunsun崔和Eric张。生成歌舞团的鲁棒异常检测。预印本的arXiv的arXiv：1810.01392，2018。

何塞-[RDorronsoro，旧金山Ginel，卡门-[RS'anchez，和卡洛斯圣克鲁斯。神经欺诈检测信用卡业务。神经网络，1997年IEEE交易。

乔恩·安德G'omez，胡安Ar'evalo，罗伯托·帕雷德斯和霍尔迪宁。终端到终端的卡支付欺诈得分神经网络结构。模式识别快报，105：175-181，2018。

B'enard维泽和基督教Omlin。信用卡交易，欺诈检测和机器学习：建模时间LSTM递归神经网络。在神经信息的范例和应用程序，网页231-268施普林格，2009年创新。

约翰内斯Jurgovsky，迈克尔Granitzer，康斯坦丁·齐格勒，西尔维Calabretto，皮埃尔-爱德华·波特尔，丽云氦Guelton，和OlivierCaelen。顺序分级信用卡欺诈检测。专家系统与Applica-蒸发散，100：234-245，2018。

亚亚Heryadi和HARCO莱斯利Hendric吐奶Warnars。学习用于使用CNN欺诈交易识别，堆叠LSTM和CNN-LSTM交易量的时间表示。在控制论和计算智能（Cyber​​neticsCom），在2017年IEEE国际会议，84-89页。IEEE，2017年。

安藤弘，Hidehito五味和英彦田中。使用递归神经网络中检测欺诈性的行为。2016年

林书豪王，刘灿，高翔，洪涛曲，和许巍。基于会话的欺诈检测使用递归神经网络在线电子商务交易。在欧洲联合会议上机器学习与知识发现数据库，241-252页。施普林格，2017A。

穆罕默德·易卜拉欣Alowais上篮文很快。信用卡欺诈检测：个性化或聚合模式。在移动，无处不在，并智能计算（音乐），2012年第三FTRA国际会议，114-119页。IEEE，2012。

Thushara阿马拉辛哈，AchalaAponso和纳奥米Krishnarajah。机器的关键分析基于学习的在金融交易中的欺诈检测AP-proaches。在机器学习技术，12-17页2018年国际会议论文集。ACM，2018A。

NarekAbroyan。神经网络对金融市场的风险分类。2017A。

XuruiLP，韦钰，天宇路旺，陈建斌郑，邱雪涛，胡锦涛赵，夏磊，和玉娇丽。使用GRU为中心的三明治结构化模型交易欺诈检测。2018年计算机IEEE第22届国际会议在支持设计（（CSCWD）），467-472页的协同工作。IEEE，2018。

沉爱华，任城通和梅尧臣邓。分类模型对信用卡欺诈检测中的应用。在服务体系和服务管理，在2007年国际会议，1-4页。IEEE，2007。

鼻翼Chouiekh和哈桑·伊本·哈吉EL。Convnets欺诈检测分析。Procedia计算机科学，127：133-138，2018。

NarekAbroyan。卷积和复发性神经网络进行实时数据分类。在创新Comput-ING科技（所），2017年在第七届国际会议，42-45页。IEEE，2017b。

33

康之福，郑大为，易涂，和李青张。使用卷积神经网络的信用卡欺诈检测。在国际会议的神经信息处理，483-490页。斯普林格年，2016年。

逸飞路。深层神经网络和欺诈检测，2017年。

纯挚王，王已超，志伟烨，闫凌宇，文成县蔡和潘尚。基于BP神经网络优化算法鲸鱼信用卡欺诈检测。在计算机科学与教育2018第13届国际会议（ICCSE），1-4页。IEEE，2018A。

朝晖张，鑫鑫周，张晓波，立志王，和王蓬威。基于网上交易的欺诈检测卷积神经网络模型。安全和通信网络，2018，2018A。

穆罕默德·阿布Alsheikh，杜斯特Niyato，绍伟林，Hwee粉红谭，朱啥。采用深度学习和Apache火花移动大数据分析。IEEE网络，30（3）：22-29，2016。

阿努普Badhe。点击在程序化广告服务的移动广告欺诈检测。神经网络和机器学习，1（1）：1-1，2017年。

穆罕默德IquebalAkhter和MohammadGulamAhamad。通过数据挖掘利用神经NET-工程检测的电信诈骗。国际科学杂志及工程研究，3（3）：601-6，2012。

Vanita耆那教。使用数据流分析和神经网络分类基于数据挖掘的电信欺诈检测的角度分析。国际期刊信息技术，9（3）：303-310，2017年。

玉郑钧，小寒周伟国盛，瘀血，并生陈勇。生成对抗性基于网络的电信诈骗检测在接收银行。神经网络，102：78-86，2018B。

侯赛因Joudaki，阿拉什Rashidian，贝洛兹Minaei-Bidgoli，马哈茂德Mahmoodi等，赞Geraili，马赫迪的Nasiri和穆罕默德阿。利用数据挖掘来检测医疗欺诈和滥用：文学的审查。健康科学全球杂志，7（1）：194，2015年。

日亚罗伊和K·托马斯乔治。检测使用机器学习技术的保险索赔欺诈。在电路，电源及计算技术（ICCPCT），2017年国际会议，1-6页。IEEE，2017年。

斯泰恩Viaene，圭多Dedene，和理查德·A·Derrig。使用贝叶斯学习神经NET-作品自动要求欺诈检测。专家系统与应用，29（3）：653-666，2005。

瓦尔安德烈·法哈多，大卫·芬德利，家RoshanakHoumanfar，CharuJaiswal，假戏梁，和孙红雷谢。沃斯：用于不平衡数据的变分过采样的方法。预印本的arXiv的arXiv：1809.02596，2018。

菲利普强，Joycelin卡雷尔和柯蒂斯光明。神经网络保险欺诈检测，2009年。

理查德·A·鲍德尔和Taghi中号Khoshgoftaar。使用机器学习方法医保欺诈检测。在机器学习和应用（ICMLA），2017年第16届IEEE国际会议，858-865页。IEEE，2017年。

丹尼尔Lasaga和普拉卡什Santhana。深度学习来检测医疗欺诈行为。在2017年KDD研讨会异常检测在金融，114-120页，2018。

卡姆兰GhasediDizaji，小倩王，和黄衡。半监督的基因表达推断生成对抗性的网络。在知识发现和数据挖掘，1435年至1444年页第24届ACMSIGKDD国际会议论文集。ACM，2018。

塞缪尔·芬利森摹，以撒小号小羽，和安德鲁·L光束。针对医疗深度学习系统对抗性攻击。预印本的arXiv的arXiv：1804.05296，2018。

安德烈埃斯特瓦，布雷特Kuprel，罗伯托·诺沃亚一，官高，苏珊中号Swetter，海伦中号布劳和塞巴斯蒂安·史朗。深神经网络的皮肤癌的皮肤科专家级分类。自然，542（7639）：115，2017。

艳芳叶，桃李，唐纳德Adjeroh和SSitharama艾扬格。利用数据挖掘技术在恶意软件检测调查。ACM计算概观（CSUR），50（3）：41，2017年。

威廉·哈代，凌卫臣，市府后，验放烨和李昕。Dl4md：对于Intel的ligent恶意软件检测深学习框架。在数据挖掘国际会议（DMIN）论文集，第61页在计算机科学，计算机工程与应用计算世界大会的指导委员会（WorldComp）年，2016年。

34

亚历山德拉德保拉，萨尔瓦多Favaloro，萨尔瓦多Gaglio，G螺Re和马科莫拉尼亚。通过低级特征和堆叠去噪自动编码恶意软件检测。在对网络安全，ITASEC2018，成交量2058CEUR-WS，2018第二届意大利会议。

莫希特Sewak，桑杰ķ萨海，并与Hemant拉索。深刻学习基于恶意软件检测系统的调查。在可用性，可靠性和安全性，第26页。ACM，2018第13届国际会议论文集。

TemesguenMessay凯贝蒂，OubotiDjaneye-Boundjou，Barath纳拉亚南纳拉亚南，安卡Ralescu，大卫卡普。使用基于深度学习的架构和其对微软的恶意软件类型应用的挑战（2015年大）的数据集自动编码恶意程序的分类。在航空航天和电子会议（NAECON），2017年IEEE国家，70-75页。IEEE，2017年。

奥米德Ë大卫和Nathan小号内塔尼亚胡。Deepsign：深学习自动恶意软件签名生成和分类。在神经网络（IJCNN），2015年国际联席会议，1-8页。IEEE，2015年。

BugraCakir的和埃尔多安Dogdu。恶意软件分类采用深学习方法。在诉讼中ACMSE2018大会，第10页。ACM，2018。

佩德罗·席尔瓦，SepehrAkhavan-Masouleh，和李礼。通过提取图标Infor公司，mation提高恶意软件的检测精度。2018年IEEE会议上多媒体信息处理和检索（MIPR），408-411页。IEEE，2018。

博扬Kolosnjaji，安布拉Demontis，巴蒂斯塔Biggio，达维德Maiorca，乔治·扎琴多，克劳迪娅·埃克特，和FabioRoli。对抗性的恶意软件二进制文件：回避深度学习为可执行的恶意软件检测。预印本的arXiv的arXiv：1803.04173，2018。

屋大维Suciu，斯科特ē顾家，和Jeffrey约翰。探索恶意软件检测对抗性例子。预印本的arXiv的arXiv：1810.08280，2018。

SiwakornSrisakaokul，Zexuan中路，宇豪张，魏阳，和谢韬。Muldef：对神经网络对抗的例子，基于多模式防御。预印本的arXiv的arXiv：1809.00065，2018。

托马斯·金，尼基塔AGGARWAL，MariarosariaTaddeo，和卢西亚诺弗洛里迪。人工智能犯罪：一个interdis-ciplinary可预见的威胁和解决方案的分析。2018。

冬冬县德黄和红，郁考。R2-D2：彩色启发卷积神经网络（CNN）系的Android恶意软件检测。预印本的arXiv的arXiv：1705.04448，2017年。

魏国，滕海王，并继增伟。恶意软件检测与卷积神经网络使用硬件事件。在CCF全国会议上Compujter工程技术，104-115页。斯普林格2017年。

马哈茂德·阿卜杜勒萨拉姆，拉姆克里希南，雨菲黄，和拉维桑德。恶意软件检测使用卷积神经网络的云计算基础架构。2018年云计算IEEE第11届国际大会（云），162-169页。IEEE，2018。

爱德华·拉夫，乔恩·巴克，贾里德西尔维斯特，罗伯特·布兰顿，布莱恩卡坦扎罗和查尔斯·尼古拉斯。恶意软件检测吃全exe文件。预印本的arXiv的arXiv：1710.09435，2017年。

ElMouatez比拉Karbab，穆拉德Debbabi，AbdelouahidDerhab和DjedjigaMouheb。Maldozer：使用深度学习的Android恶意软件检测自动框架。数字调查，24：S48-S59，2018。

法比奥·马蒂内利，菲梅塔Marulli，和FrancescoMercaldo。有效的移动恶意软件检测评估卷积神经网络。Procedia计算机科学，112：2372年至2381年，2017年。

尼尔·麦克劳克林，耶稣马丁内斯德尔林孔，BooJoong康，苏莱曼Yerima，保罗·米勒，Sakir塞泽尔，YeganehSafaei，埃里克Trickel，仇子明赵，亚当Doupe等。的android深恶意软件检测。在第七届ACM会议上的数据和应用安全的法律程序与隐私，301-308页。ACM，2017年。

丹尼尔·吉尔伯特，普约尔MATEU，霍尔迪飞机，和拉蒙维桑。使用卷积神经网络的恶意软件的分类表示为图像。。计算机病毒和黑客技术的，1-14页，2018。

博扬Kolosnjaji，GhadirEraisha，乔治·韦伯斯特，ApostolisZarras和克劳迪娅埃克特。赋权恶意软件分类和分析卷积网络。在神经网络（IJCNN），2017年在国际联席会议，3838-3845页。IEEE，2017年。

35

Ishai罗森伯格，纪尧姆SICARD，和Eli奥米德大卫。终端到终端的深层神经网络和传输学习民族国家的恶意软件自动分析。熵，20（5）：390，2018。

青龙王，文博郭，张凯旋路，亚历山大摹OrorbiaII，新余兴，雪柳，和C李贾尔斯。对手耐深神经网络与应用到恶意软件检测。在知识发现和数据挖掘，1145年至1153年页23ACMSIGKDD国际会议论文集。ACM，2017b。

佳阳，汇祥张，暴雷MAO，和春雷陈。深信念网络的Android恶意软件检测中的应用。ICIC快递信件。B部分，应用范围：研究和调查的国际期刊，7（7）：1505至10年，2016年

雨馨丁，陈晟和徐军。深信念网络基于操作码的恶意软件检测中的应用。在神经网络（IJCNN）年，2016年在国际联席会议，3901-3908页。IEEE2016。

丁吁薪和朱思宜。基于深度学习算法的恶意软件检测。神经计算和应用，1-12个，2017年的网页。

ShymalaGowriSelvaganapathy，MathappanNivaashini和HemaPriya纳塔拉。坚定信念基于网络的去tection和恶意URL的分类。信息安全杂志：全球范围来看，27（3）：145-161，2018。

师父后，阿龙萨斯，凌卫臣，艳芳烨和ThirimachosBourlai。深层神经网络自动的Android恶意软件检测。在关于社会网络分析与挖掘2017年，803-810页进展2017年IEEE/ACM国际会议论文集。ACM，2017年。

顺Tobiyama，山口由纪子，岛田肇，朝范生濑胜，和八木毅。恶意软件检测使用深层神经网络进程的行为。计算机软件与应用学术会议（COMPSAC）年，2016年IEEE第40届，第2卷，577-582页。IEEE2016。

巍巍胡锦涛和颖坦。黑盒攻击对RNN基于恶意软件的检测算法。预印本的arXiv的arXiv：1705.08131，2017年。

顺Tobiyama，山口由纪子，长谷川弘，肇岛田，秋山光昭，和八木毅。一种用于与seq2seq模型估计过程恶意方法。在信息网络2018国际会议（ICOIN），255-260页。IEEE，2018。

尼可拉斯Passalis和阿纳斯塔西Tefas。长期为深层神经网络的随机优化时间平均。神经计算和应用，1-13页。

泉乐，Ois'ınBoydell，布莱恩的MacNamee，和马克·斯坎伦。深度学习在浅水区：非领域专家恶意软件分类。数字调查，26：S118-S126，2018。

金扬金，锡君卜，和宋培赵。零日恶意软件检测使用传送基于深自动编码生成对抗性的网络。信息科学，460：83-102，2018。

王炜，赵梦雪和济钢王。有效的基于深厚的自动编码和卷积神经网络具有的android混合模式的恶意软件检测。杂志环境智能和人性化的计算，1-9页，2018B的。

元成立，戎马，和润海娇。基于深度学习的混合恶意代码检测方法。方法，9（5），2015。

哈米德HaddadPajouh，阿里Dehghantanha，拉乌夫Khayami，和Kim-KWANG雷蒙德周仰杰。对于物联网的恶意软件威胁狩猎深递归神经网络为基础的方法。下一代计算机系统，85：88-96，2018。

Seonwoo敏，李Byunghan和Sungroh尹。深度学习生物信息学。生物信息学简报，18（5）：851-869，2017。

Chensi曹，刘枫，海坛，Deshou宋，文杰舒，李卫忠，赵一鸣，小臣博，和止泻。深学习及其在生物医学中的应用。基因组学，蛋白质组学和生物信息学，2018A。

赵锐，Ruqiang燕，陈蒋正华，克志茂，王鹏，和罗伯特·X高。深度学习和applica-蒸发散机器健康监测：调查。预印本的arXiv的arXiv：1612.07640年，2016年。

36

萨米尔汗和武久Yairi。深学习的系统健康管理中的应用进展。Mechan-的iCal系统和信号处理，107：241-265，2018。

NarendharGugulothu，潘卡马尔霍特拉，Lovekesh维格和高塔姆缴费。稀疏神经网络在高维时间序列的异常检测。

Kasun阿马拉辛哈，凯文·肯尼和米洛斯狂躁。朝解释的深层神经网络基于异常检测。在人类系统的交互2018第11届国际大会（HSI），311-317页。IEEE，2018B。

爱德华财。医生AI：可解释的深度学习建模电子健康记录。博士论文，乔治亚理工学院，2018。

王锴，赵有劲，熊庆余，范敏，Guotan孙，马海口市龙昆和刘彤。基于从多个时间序列生理信号的深度学习研究健康异常检测模型。科学亲编程，2016年，2016年

杰克考顿，伊利亚斯Kyriazakis，托马斯Pl¨otz，和JaumeBacardit。的组合深度学习GRU-自动编码器用于使用多个环境传感器猪的早期检测呼吸道疾病。传感器，18（8）：2521，2018。

佐藤大辅，Shouhei花冈，野村幸，智美Takenaga，三木宗一郎，丈晴吉川，菅直林和安部理。在emer-能动性头部CT卷自动编码无监督异常检测一种原始研究。在医学成像2018：计算机辅助诊断，成交量10575，页面105751P。国际社会对光学和光子学，2018。

JT特纳，亚当页，TinooshMohsenin，和蒂姆·奥茨。高分辨率使用深层信念网络的多通道脑电图癫痫发作的检测数据。2014年春AAAI系列研讨会2014年。

马诺·库马尔·夏尔马，Debdoot薄板和Prabir库马尔比斯瓦斯。异常检测的坚定信念网络。在关于信息通信技术和计算机，第11页。ACM年，2016年的进展国际会议论文集。

马宁，彭宇，王少军，菲利普-HW梁。无人监督的高光谱深异常检测。传感器，18（3）：693，2018。

君命张，严武，白静，和富强陈。基于稀疏的坚定信念网和多分类的组合，自动睡眠阶段分类。435-451，2016：测量和控制，38（4）的理工大学学报。

DFWulsin，JR古普塔，R摩尼，JA布兰科和B利特。快速分类和异常测：用半监督的坚定信念网建模脑电图波形。神经工程的，8（3）：036015，2011。

Ç吴，Y国和Y马。自适应异常检测深网络。在自适应和自适应系统和应用，2015A第七届国际会议论文集。

临夏辽，金王文京和拉杜帕维尔。增强的限制波尔兹曼机prognosability正则预测和健康评估。IEEE交易：电子工业，63（11）：7076-7083年，2016年。

元好问徐，陈Wenxiao，能文钊，李Zeyan，嘉豪卜，直喊丽，刘颖，又尖又钊，裴丹，杨枫，等。通过变自动编码器来对Web应用程序的KPI季节性的无监督异常检测。在万维网上2018年万维网会议记录，187-196页。国际万维网会议指导委员会，2018。

雨辰鲁蓬絮。异常检测使用变的自动编码皮肤病图像。预印本的arXiv的arXiv：1807.01349，2018。

肖然陈和安德Konukoglu。脑MRI病灶的无监督检测使用约束敌对自动编码器。预印本的arXiv的arXiv：1806.04972，2018。

杭州杨家和惠英高。走向可持续发展的虚拟化医疗：使用深层神经网络从中国在线健康咨询提取医疗机构。可持续性，10（9）：3292，2018。

37

Abhyudayñ佳岗和洪宇。双向RNN在电子健康记录的医疗事件检测。在会议纪要。协会为计算语言学。北美章。会议，音量2016年，页473NIH公共访问年，2016年。

蒂莫西·奥谢Ĵ，T查尔斯·克兰西，和罗伯特·w^McGwier。递归神经无线电异常检测。预印本的arXiv的arXiv：1611.00301年，2016年。

西迪基·拉蒂夫，穆罕默德·乌斯曼，Rajib林蛙，和朱奈德·卡迪尔。使用心音深度学习的心跳异常检测感应。IEEE传感器杂志，18（22）：9393-9400，2018。

润田张欠揍。时间序列预测，并使用LSTM神经网络光曲线的异常检测。在物理学学报：会议系列，容量1061012012.页面物理学会出版社，2018。

Sucheta肖汉和Lovekesh维格。通过深长短期记忆NET-作品异常检测心电图时间信号。在数据科学和高级分析（DSAA），2015年到2015年36678对IEEE国际会议，1-7页。IEEE，2015年。

厄休拉·施密特Erfurth，阿米尔Sadeghipour，比安卡小号Gerendas，塞巴斯蒂安Waldstein酒店中号和赫尔沃耶Bogunovi'c。AR-tificial情报视网膜。在视网膜和眼睛研究进展，2018。

季米特里斯ķIAKOVIDIS，斯皮罗斯VGeorgakopoulos，迈克尔Vasilakakis，阿纳斯塔西Koulaouzidis和瓦西里斯PPLA-gianakos。检测和使用深度学习和迭代集群统一定位胃肠道异常。IEEE交易在医学影像，2018。

烟柳和桑杰·乔拉。社交媒体异常检测：挑战和解决方案。在网络搜索和数据挖掘，817-818页第十届ACM国际会议论文集。ACM，2017年。

大卫·萨维奇，张秀珍，星火宇，宝莲周和清脉王。异常检测的在线社交网络。社交网络，39：62-702014。

科坦阿南德，杰伊·库马尔，以及注：Kunal阿南德。异常检测的在线社交网络：调查。在本发明的通信和计算技术（ICICCT），2017年国际会议，456-459页。IEEE，2017年。

玫瑰宇，邱惠达，振文ChingYung林和烟柳。在社交媒体上的异常检测调查。ACMSIGKDD探索通讯，18（1）：1-14，2016。

曹娟，郭俊波，西戎李，志伟晋，汉国和主席李。微博上的谣言自动检测：调查。预印本的arXiv的arXiv：1807.03505，2018B。

张燕，魏林陈，柴姚永吉，CHIEW唐楼，和卜宋利。检测上采用多层自动编码器在线社交网络的传言。在技​​术与工程管理会议（TEMSCON），2017年IEEE，437-441页。IEEE，2017年。

雅格布卡斯特里尼，瓦伦蒂娜Poggioni和朱利亚SORBI。假Twitter的追随者检测的去噪自动编码。在WebIntelligence中国际会议论文集，195-202页。ACM，2017年。

小孙，张晨，丁帅，和长庆权。通过基于深刻的学习方法的社交网络的大数据检测异常的情绪。多媒体工具和应用程序，1-22个，2018页。

梨树，胡旭，和刘兵。文件：文本文档的深开分类。预印本的arXiv的arXiv：1709.08716，2017年。

飙扬，曹劲猛，蓉蓉Ni和泠奏。异常检测通过时空autoencoding和额外关注移动人群。进展多媒体，2018，2018。

李泽，孙Duoyong，人妻朱和罗子涵林。检测使用优化的神经网络模型的组织网络事件相关的变化。公共科学图书馆·一个，12（11）：e0188733，2017A。

卫。混合动力车型在社交网络异常检测。预印本的arXiv的arXiv：1709.08716，2017年。

艾哈迈德奥马尔·梅蒙。日志文件的分类和使用语法推理异常分析。博士论文，2008。

安迪·布朗，阿隆Tuor，布莱恩·哈钦森和妮可·尼科尔斯。递归神经网络的关注机制可解释的系统日志异常检测。预印本的arXiv的arXiv：1803.04967，2018。

38

Anwesha达斯，弗兰克·米勒，查尔斯·西格尔和阿比纳夫毗湿奴。DESH：用于铅失效时间在HPC系统的健康预测深度学习。在对高性能并行第27届国际研讨会论文集和分布式计算，40-51页。ACM，2018。

潘卡马尔霍特拉，Lovekesh维格，高塔姆缴费和普尼特阿加瓦尔。长短期记忆网络在时间序列异常检测。在诉讼中，89页印刷机universitaires鲁汶，2015年。

樱田真由武久和Yairi。异常检测使用具有非线性降维自动编码。在机器学习的MLSDA2014第二届研讨会感官数据分析，第4页。ACM，2014年提起诉讼。

蒂莫提出中止，斯特凡Luettgen，亚历山大西利格和MaxM¨uhlh¨auser。分析业务流程使用距平自动编码。机器学习，1-19页，2018A。

蒂莫提出中止，亚历山大西利格和MaxM¨uhlh¨auser。无监督异常检测使用降噪自动编码嘈杂的商业亲塞斯事件日志。在上发现科学，442-456页的国际会议。斯普林格年，2016年。

Aarish格罗弗。异常检测应用程序日志数据。2018。

马克西姆Wolpher。异常检测中使用LSTM自动编码器，2018非结构化时间序列数据。

冬雪张，杨征，羽纹，徐珏，王Jingchuo，杨宇，和丹萌。基于角色的日志分析中的应用深学习的内部威胁检测。在计算机体系结构和处理器，18-20页的安全为核心设计的第一个研讨会论文集。ACM，2018B。

AnvardhNanduri和Lance雪利酒。异常检测飞机数据使用递归神经网络（RNN）。在综合通讯导航和监视（ICNS），2016年，5C2-1页。IEEE2016。

郑风鸣，李淑芳，郭志敏吴波，田诗明，潘明明德。异常检测的基础上反复神经网络编码器，解码器架构的智能电网。该杂志文章的中国大学和电信，24（6）：67-73，2017年。

埃里克·马奇，法比奥Vesperini，菲利克斯Weninger，弗洛里安·伊本，斯特凡诺Squartini，和比约恩·舒勒。非线性预测与声新奇检测LSTM回归神经网络。在神经网络（IJCNN），2015年国际联席会议，1-7页。IEEE，2015年。

泗阳路，相偎，刘延东李和王礼强。使用卷积神经网络的大数据系统日志，异常检测。2018年IEEE第16届国际CONF上可靠，自主和SecureComputing公司，第16届国际CONF普适智能与计算，第四国际的conf大数据智能和计算和网络科学技术大会（DASC/PICOM/数据通信/Cyber​​SciTech），151页-158。IEEE，2018。

芳芳元，延安曹珉上，沈雁冰刘，建龙谭，和滨兴方。内幕威胁检测与深层神经网络。在国际会议计算科学，43-54页。施普林格，2018A。

DomenRacki，德扬Tomazevic和海伦芬Skocaj。紧凑的卷积神经网络的纹理化表面异常检测。2018年IEEE冬季会议计算机视觉中的应用（WACV），页1331-1339IEEE，2018。

市府周，沉伟，曾丹，梅方，远望伟和枝江张。时空卷积神经网络的异常检测和定位在拥挤的场面。信号处理：图像Communica-重刑，47：358-3682016。

奥列格Gorokhov，米哈伊尔·彼得罗夫斯基和伊戈尔Mashechkin。卷积神经网络在文本数据无监督异常检测。在国际智能数据工程与自动化学习，500-507页。斯普林格2017年。

尼古拉斯·辽，马修Guzdial，和马克·里德尔。在日志和数据级深卷积球员建模。在数字游戏，页41.ACM，2017年的基金会第12届国际会议论文集。

解嘲郑锐任，王大雷和剑锋詹。深卷积神经网络的分布式系统异常事件分类。预印本的arXiv的arXiv：1710.09052，2017年。

博学张，赵奇，冯温泉，和舒畅吕。Alphamex：对于convo-lutional神经网络更智能的全球统筹方法。神经计算，321：36-48，2018C。

39

迈赫迪·穆罕默迪，阿拉巴马州的Al-教法学家，萨迈赫苏鲁尔和穆赫辛Guizani。深学习IOT大数据和流分析：调查。IEEE通信调查与教程，2018。

铁罗和西摹Nagarajany。使用分布式的无线传感器网络的自动编码神经网络的物联网异常检测。在通信2018IEEE国际会议（ICC），1-6页。IEEE，2018。

Fatemeh沙阿穆罕默迪和安德烈斯Kwasinski。神经网络的认知引擎为自主和分布式底层动态频谱接入。预印本的arXiv的arXiv：1806.11038，2018。

伊琳娜Kakanakova和斯特凡诺夫。通过深度学习结构异常检测。在第18届国际计算机系统和技术，73-79页的诉讼。ACM，2017年。

微山县张，郭唔唔，刘昕，刘岩，Jiehan周，李波，清华路，和苏洋。工业物联网设备的基于LSTM分析。IEEE访问，6：23551-23560，2018D。

布尔汗一个Mudassar，钟焕柯和SaibalMukhopadhyay。带班知道源分离的无监督异常事件检测帧-工作。在声学，语音和信号处理IEEE2018国际会议（ICASSP），2671年至2675年的网页。IEEE，2018。

路易斯Mart'ı，Nayat桑切斯丕，Jos'e曼努埃尔·莫利纳和安娜·克里斯蒂娜Bicharra加西亚。基于在石油工业中的应用传感器数据异常检测。传感器，15（2）：2774至2797年，2015年。

迪根ĴATHA和MohammadřJahanshahi。深度学习的评价方法基础上的腐蚀检测卷积神经网络。结构健康监测，17（5）：1110至1128年，2018。

杰弗里·德Deijn。使用卷积神经网络自动车损害的认可。2018。

王帆，约翰·PKerekes，卓异许，延东王。采用深度学习住宅屋顶状况评估体系。[应用的遥感，12（1）：016040，2018C。

井上俊，Yoriyuki山形，玉祁晨，克里斯托弗中号Poskitt，和君太阳。异常检测使用无监督机器学习水treat-换货制度。在数据挖掘研讨会（ICDMW），在2017年IEEE国际会议，一零五八至六五年页。IEEE，2017年。

牙阮氏，Nhien安乐Khac，等。基于LSTM-rnns一类的集体异常检测。在对大型数据和知识为中心的系统XXXVITransac-蒸发散，73-85页。斯普林格2017年。

摩西Kravchik和阿萨夫Shabtai。使用卷积神经网络在工业控制系统中检测网络攻击。在2018年研讨会的Cyber​​-物理系统安全的诉讼和隐私，72-83页。ACM，2018。

冠杰黄，赵贤珠和李晓丹吴。使用生理信号的睡眠阶段分类深基于学习的方法。在国际会议上聪明健康，249-260页。斯普林格，2018。

Donghyun公园，Seulgi金，椰林的，和宰尹荣。Lired：一个重量轻的实时用于边缘使用LSTM回归神经网络计算的故障检测系统。传感器，18（7）：2110，2018A。

芷文昌，孝伟利，和Chein，刘虹。的用于智能机床的人工智能算法的审查。发明，3（3）：41，2018。

叶远和贾贺克斌。一种分布式使用智能计量表数据操作的能量消耗的异常检测方法。在智能信息隐藏和多媒体信号处理（IIH-MSP），2015年国际Confer-ENCE上，310-313页。IEEE，2015年。

丹尼尔乙阿拉亚，卡塔琳娜Grolinger，哈尼˚FElYamany，杨千嬅AMCapretz和吉尔马Bitsuamlak。在建筑能耗异常检测的集成学习框架。能源与建筑，144：191-206，2017年。

壅滞曲，苗族他，杰森德语，和David他。使用深稀疏自动编码器在齿轮点蚀的检测。应用科学，7（5）：515，2017。

阿南德Bhattad，杰森岩石和戴维·福赛思。检测with'nopeeking'autoencoders反常的面孔。预印本的arXiv的arXiv：1802.05798，2018。

40

Faiq哈立德洛迪，赛义德·哈桑Rafay，奥斯曼·哈桑和法拉Awwadl。功率谱的运行硬件木马微控制器的指令条重刑一套检测不包含黄金的电路模型。在欧洲会议上设计，自动化与测试的论文集，294-297页。欧洲设计和自动化学会，2017年。

ShahrzadFaghih-Roohi，SiamakHajizadeh，阿尔弗雷多N'u~nez，罗伯特的Babuska和巴特·德舒特。深convolu-周志武神经网络用于检测轨道的表面缺陷。在神经网络（IJCNN）年，2016年在国际联席会议，2584年至2589年的网页。IEEE2016。

彼得·克里斯蒂安森，拉尔斯·尼尔森ň，金一斯蒂恩，拉斯穆斯ñ约根森和亨里克Karstoft。Deepanomaly：Combin-荷兰国际集团背景减法和深度学习在农业领域的探测障碍物和异常。传感器，16（11）：1904，2016。

院长李，文森特兆，里克·克鲁兹和查尔斯爱特曼。卷积神经网络和轴承的故障分析。在数据挖掘系列（ICDM）巴塞罗那国际会议论文集，第194-200页，2016年

Lingping董，张王永亮，丛林文和洪涛吴。基于形态分析和深入学习摄像机异常检测。在数字信号处理（DSP）年，2016年的IEEE国际会议，266-270页。IEEE2016。

阿尔瓦罗·富恩特斯，塾尹桑金哲，董朝阳公园。一个强大的基于深学习探测器进行实时番茄病虫害识别。传感器，17（9）：2022，2017年。

委燕宇丽洁。准确而可靠的异常检测燃气轮机燃烧室：深学习方式。在预测与健康管理学会，2015年年度会议的论文集。

惠罗和何时生钟。燃气涡轮发动机气路采用深度学习为高斯分布的异常检测。在预测与系统健康管理会议（PHM-哈尔滨），2017年，页1-6。IEEE，2017年。

杰杰傣，回宋，盛合好，并Xiuchen江。清洁进行状态监控基于堆叠降噪自动编码功率equip-换货的数据的方法。IEEE访问，5：22863-22870，2017年。

LejlaBanjanovic-Mehmedovic，阿梅尔Hajdarevic，穆罕默德坎塔尔季奇，FahrudinMehmedovic和IzetDzananovic。基于神经网络的数据驱动在火力发电厂异常检测的建模。Automatika，58（1）：69-79，2017。

多米尼克牛逼Shipmon，贾森中号Gurevitch，保罗中号Piselli，和斯蒂芬·爱德华兹牛逼。时间序列异常检测;检测用特征的限制，在嘈杂的高度周期性数据稀疏实例异常滴。预印本的arXiv的arXiv：1708.03665，2017A。

凯尔Hundman，华伦天奴康斯坦丁诺，克里斯托弗·拉波特，伊恩·科尔韦尔和汤姆瑟德斯特伦。探测航天器异常使用lstms和非参数动态阈值。预印本的arXiv的arXiv：1802.04431，2018。

凌雪珠和尼古拉拉普捷夫海。由浅入深，在尤伯杯时间序列充满信心的预测。在数据挖掘研讨会（ICDMW），在2017年IEEE国际会议，103-110页。IEEE，2017年。

扬保罗Assendorp。深度学习为多元时间序列数据异常检测。博士论文，Hochschule的皮草ANGEWANDTE学问汉堡，2017年。

速不台艾哈迈德，亚历山大拉文，斯科特·珀迪和Zuha阿迦。无监督的实时异常检测ING于流数据。神经计算，262：134-147，2017年。

潘卡马尔霍特拉，Anusha莱玛克里斯南，Gaurangi阿南德，Lovekesh维格，普尼特阿加瓦尔和高塔姆缴费。Lstm-基于编码器的解码器，用于多传感器异常检测。预印本的arXiv的arXiv：1607.00148，2016a。

阿德里安·泰勒，维尔托德勒布朗和纳塔莉Japkowicz。异常检测与长短期记忆网络汽车控制网络数据。在数据科学和高级分析（DSAA）年，2016年的IEEE国际会议，130-139页。IEEE2016。

闵承，徐谦，张建明吕，文音刘，李清，王建平Wang等。MS-LSTM：用于BGP异常检测的多尺度LSTM模型。在2016年的网络协议IEEE第24届国际会议（ICNP），1-6页。IEEE2016。

41

GobinathLoganathan，JagathSamarabandu和Xianbin王。顺序为网络流量实时异常检测序列模式学习算法。在电气和计算机工程2018IEEE加拿大会议（CCECE），1-4页。IEEE，2018。

穆赫辛穆尼尔，邻省艾哈迈德·西迪基，安德烈亚斯Dengel和Sheraz艾哈迈德。Deepant：深学习无监督异常检测方法在时间序列。IEEE访问，2018。

多米尼克Shipmon，杰森Gurevitch，保罗中号Piselli，和史蒂夫·爱德华兹。时间序列异常检测：检测功能有限，并在嘈杂的周期性数据稀疏的例子反常下降的。技术报告，谷歌公司，2017b。URLhttps://arxiv.org/abs/1708.03665。

潘卡马尔霍特拉，毗湿奴电视，Anusha莱玛克里斯南，Gaurangi阿南德，Lovekesh维格，普尼特阿加瓦尔和高塔姆缴费。使用基于LSTM编码器-解码器无监督健康指数多传感器预后。预印本的arXiv的arXiv：1608.06154，2016B。

帕维尔·菲诺弗，安德烈Lavrentyev和阿尔乔姆·沃龙佐夫。多元产业的时间系列网络攻击simula-重刑：使用基于LSTM预测数据模型故障检测。预印本的arXiv的arXiv：1612.06676年，2016年。

海事杉本，Saerom李和冈田幸文。心电图数据定期异常波深学习型检测。在工程师的国际MultiConference论文集和计算机科学家，第1卷，2018。

董尤伯哦，伊尔董洪运。残差基于使用自动编码器贴片机声音异常检测。传感器（巴塞尔，瑞士），18（5），2018。

扎赫拉Ebrahimzadeh和萨曼莎克林伯格。多尺度变化点检测多元时间序列。

格利扬Veeramachaneni，伊格纳西奥阿纳尔多，VamsiKorrapati康斯坦丁Bassias和柯力。艾2：培养了大数据机进行防守。在大数据安全的云（BigDataSecurity），IEEE国际会议上的高性能和智能计算（HPSC），以及智能数据IEEE国际会议和安全（IDS）将在2016年第二届IEEE国际会议，49-54页。IEEE2016。

晃映斗，维克西谢尔斯基和安迪·宋。异常检测使用的培训上一个类的实例复制神经网络。在亚太地区会议上模拟进化和学习，311-322页。斯普林格2014。

马切伊Wielgosz，安杰Skocze'n，和马捷Mertik。回归神经网络在宰后的时间序列LHC超导磁体的异常检测。预印本的arXiv的arXiv：1702.00833，2017年。

萨克蒂Saurav，潘卡马尔霍特拉，毗湿奴电视，NarendharGugulothu，Lovekesh维格，普尼特阿加瓦尔和高塔姆缴费。在线异常使用递归神经网络，概念漂移的适应检测。在对数据的科学数据和管理ACM印度联合国际会议论文集，78-87页。ACM，2018。

马切伊Wielgosz，马捷Mertik，安杰Skocze'n，和Ernesto德Matteis。异常检测器的基于回归神经网络和自适应量化hilumiLHC磁铁模型。人工智能，74的工程应用：166-185，2018。

郭田，赵旭，姚新，陈海丰，卡尔Aberer，和光一Funaya。强大的在线时间序列predic-重刑复发性神经网络。在数据科学和高级分析（DSAA）年，2016年的IEEE国际会议，816-825页。IEEE2016。

帕维尔·菲诺弗，费多尔Kitashov，和安德烈Lavrentyev。RNN为基础的早期网络攻击检测田纳西伊士曼过程。预印本的arXiv的arXiv：1709.02232，2017年。

STRATISKanarachos，斯塔夫罗斯·理查德摹Christopoulos，亚历山大Chroneos，和迈克尔·菲茨帕特里克。通过深度学习算法相结合小波，神经网络和希尔伯特反式形式检测时间序列数据异常。专家系统与应用，85：292-304，2017年。

沭阳杜，Madhulima潘迪和Cuiqun兴。建模方法对时间序列预测和异常检测。

保罗Napoletano，弗拉维奥皮寇利和雷蒙多SCHETTINI。异常检测在纳米纤维材料由基于CNN-自相似性。传感器，18（1）：209，2018。

尚穆根迪夫亚戴维斯布莱洛克和约翰·加塔。瞬间：卷积的方法来学习的时间序列相似性。2018。

42

杰斐逊瑞安·梅德尔和AndreasSavakis。异常检测视频使用预测卷积长短期记忆网络。预印本的arXiv的arXiv：1612.00390年，2016年。

Daehyung公园，优奈星，和查尔斯Ç坎普。使用基于LSTM变分自动编码器用于机器人辅助的进料的多峰异常检测器。IEEE机器人与自动化快报，3（3）：1544年至1551年，2018B。

马克西米利安S¨olch，贾斯汀·拜尔，马文Ludersdorfer和帕特里克·范德Smagt。变推断在高维时间序列上线异常检测。预印本的arXiv的arXiv：1602.07109年，2016年。

HoussamZenati，川盛富，布鲁诺Lecouat，拉夫马内克，和维杰Ramaseshan钱德拉塞卡。高效的GaN基异常检测。预印本的arXiv的arXiv：1802.06222，2018。

吴庆瑞林永吉，卢毅，玉，陈忠，艺，万祥，杰玛罗伊格和尤瓦Elovici。兴奋剂：无监督异常检测与甘剖成数据增强。预印本的arXiv的arXiv：1808.07632，2018。

尼古拉拉普捷夫海。Anogen：深异常发生器。

贾谊伟，赵箭飞，赵眼晕，和志成赵。无监督异常检测基于背景建模交通surveil-枪。在计算机视觉的IEEE会议论文集和模式识别研讨会，129-136页，2018。

特奥多拉桑德拉·布达，宝来恰拉扬和Haytham设备与供应。Deepad：基于深度学习的时间序列异常检测的通用框架。在太平洋地区会议上的知识发现和数据挖掘，577-588页。斯普林格，2018。

叶远，光绪迅，丰隆马，王雅晴，南都，贾可斌，鲁肃，和爱东张。Muvan：多视角关注网络的多元时间数据。在数据挖掘2018IEEE国际会议（ICDM），717-726页。IEEE，2018B。

郭田和陶林。探索LSTM神经网络的过多变量数据的解释性。2018。

安东尼奥·努奇，耸翠，约翰·加勒特，GurvinderSingh案件，和KennethCroley。实时多变量多时间尺度为下一代网络异常检测系统。2018。

扬保罗Assendorp，安德烈亚斯·迈泽尔，H.格伦波伦，和C索默。深学习异常的计算机检测多元时间序列数据。2017年。

蒂莫提出中止，亚历山大西利格和MaxM¨uhlh¨auser。比奈：多元经营过程中使用深度学习异常检测。在对企业国际会议的进程管理，271-287页。施普林格，2018B。

Chuxu张，东进宋，陈Yuncong信阳丰，克里斯蒂安Lumezanu，卫城，京朝倪，檗宗，海丰陈忠和NiteshV乔拉。深神经网络的无监督异常检测与诊断多元时间序列数据。预印本的arXiv的arXiv：1811.08055，2018E。

郭一凡，廖威县，乾隆王，力行羽田喜吉，和潘力。多维时间序列异常检测：基于GRU高斯混合变自动编码器的方法。在机器学到，亚洲会议ING，页97-112，2018。

虚云富，罗辉，石生忠，和林霖。基于分组卷积降噪自动编码飞机发动机故障检测。中国航空学报，2019。

董侨，杨斌，和基督教小号詹森。异常检测使用深层神经网络的多维时间序列。在2018移动数据管理19IEEE国际会议（MDM），125-134页。IEEE，2018。

SagnikBasumallik，马锐，和SaraEftekharnejad。分组数据异常检测的PMU基于状态估计使用卷积神经网络。国际期刊电力与能源系统，107：690-702，2019。

中曾根池田健吾尻，Yuusuke野，Keishiro渡边和圭介石桥。尺寸有助于与变自动编码检测到的异常的估计。预印本的arXiv的arXiv：1811.04576，2018。

李丹，陈大成，石雷，百宏进，吴乔纳森，看-Kiong伍。疯甘：多因素异常检测与生成对抗性网络的时间序列数据。预印本的arXiv的arXiv：1901.049972019年。

43

亚伦·兰德尔Tuor，瑞安Baerwolf，尼古拉斯·诺尔斯，布莱恩·哈钦森，妮可·尼科尔斯和罗伯特·贾斯珀。Recur-租开放词汇事件等级的网络异常检测的神经网络语言模型。在人工智能，2018第三十二次AAAI会议研讨会。

芮埋阿。船舶行为异常检测多元时间的数据分析。2017年。

安德烈德尔Pozzolo，奥利维尔Caelen，里德约翰逊和赞布罗塔邦滕皮。与不平衡分类欠采样校准概率。在计算智能，2015年IEEE研讨会系列上，159-166页。IEEE，2015年。

雨薇崔阿赫亚Surpur，速不台艾哈迈德和杰夫霍金斯。HTM等神经网络模型的在线序列与流数据中学习的比较研究。在神经网络（IJCNN）年，2016年在国际联席会议，一五三○年至1538年的网页。IEEE2016。

JTAAndrewsa，NJaccarda，TWRogersa，TTanaya，和LDGriffina。异常检测的安全成像。

穆罕默德Sabokrou，穆赫辛Fayyaz，马哈茂德法帝等。全卷积神经网络在拥挤的场景快速异常检测。预印本的arXiv的arXiv：1609.00866，2016a。

穆罕默德Sabokrou，穆赫辛Fayyaz，马哈茂德法帝，和莱因哈德Klette。深级联：级联3D深层神经网络的快速异常检测和定位在拥挤的场面。IEEETRANSACTIONSON图片亲cessing，26（4）：一九九二年至2004年，2017年。

阿西姆穆纳瓦尔，PhongtharinVinayavekhin和乔瓦尼·德Magistris。时空异常检测为在无监督特征空间通过预测IN-dustrial机器人。在计算机视觉（WACV），2017年IEEE冬季会议的应用，1017-1025页。IEEE，2017年。

李炜，吴国栋，和钱读。转移深度学习在高光谱图像异常检测。IEEEGeosci。。遥感快报，14（5）：597-601，2017b。

美娜乔，王田，李加坤，李策，志伟林和Hichem斯努西。基于深自编码融合光流异常事件检测。在控制会议（CCC）2017年第36届中国，11098-11103页。IEEE，2017年。

拉夫特里帕蒂，Kuldeep辛格和迪内希·库马尔Vishwakarma。针对人群卷积神经网络是─haviour分析：一项调查。可视化的电脑，1-24页，2018。

雅各布Nogas，Shehroz小号汗，和AlexMihailidis。Deepfall，非侵入性的跌倒检测深时空卷积自动编码。预印本的arXiv的arXiv：1809.00977，2018。

雍奢广冲永豪泰。异常事件检测使用时空的自动编码的视频。在国际研讨会上的神经网络，189-196页。斯普林格2017年。

阿里Khaleghi和Mohammad沙赫拉姆莫因。改进的监控视频异常检测基于一种深刻的学习方法。在（IRANOPEN）AI与机器人和第10的RoboCupIranopen国际研讨会2018年第八届会议，73-81页。IEEE，2018。

环洋，宝源旺，斯蒂芬林，大卫Wipf，民意郭，和拜宁人郭。通过稳健的经常性的自动编码视频集锦的无监督的提取。在法律程序上的计算机视觉IEEE国际会议，4633-4641页，2015年。

正英陈永红田，曾伟和铁军黄。检测基于模糊聚类和多种自动编码器的视频监控异常行为。在多媒体和博览会（ICME），2015年IEEE国际会议，1-6页。IEEE，2015年。

马修斯Gutoski，尼尔森马塞洛·罗梅罗·阿基诺，Manass'es里贝罗，Andr'e的EngenioLazzaretti和HeitorSilv'erio洛佩斯。使用卷积自动编码和单类支持向量机的视频异常检测。

达里奥D'Avino，达维德Cozzolino，乔瓦尼·波吉和路易莎Verdoliva。自动编码器与视频伪造检测复发性神经网络。电子成像，2017年（7）：92-99，2017年。

达里奥Dotti，波帕米雷拉和STYLIANOSAsteriadis。在室内和室外环境的正常和异常活动模式无监督的发现。在VISIGRAPP（5：VISAPP），210-217页，2017年。