(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107104978 A
(43)申请公布日 2017.08.29

(21)申请号 201710375043.1

(22)申请日 2017.05.24

(71)申请人 赖洪昌
地址 518000 广东省深圳市罗湖区松园路九号茂源大厦707、709、720室

(72)发明人 赖洪昌

(74)专利代理机构 深圳新创友知识产权代理有限公司 44223
代理人 江耀纯

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 17/30(2006.01)

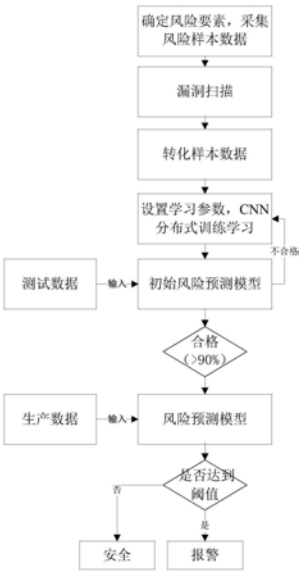
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种基于深度学习的网络风险预警方法

(57)摘要

本发明公开了一种基于深度学习的网络风险预警方法，该方法包含如下步骤：A1.采集全网段网络空间资产风险样本数据，并存入数据库；A2.从数据库中提取数据，进行卷积神经网络分布式训练学习，形成初始风险预测模型；A3.将生产数据输入风险预测模型，评估其风险值，如达到预警阈值，则报警。通过该方法和设备，可对多个目标网络或不存在明显漏洞的目标进行安全风险评估与预警，能从整体上评估一个网络的安全状态；并提升了响应速度，快速发现风险点；同时降低了维护成本，节省人力。



CN 107104978 A

1.一种基于深度学习的网络风险预警方法,其特征在于,包含如下步骤:

A1.采集全网段网络空间资产风险样本数据,并存入数据库;

A2.从数据库中提取数据,进行卷积神经网络分布式训练学习,形成风险预测模型;

A3.将生产数据输入风险预测模型,评估其风险值,如达到预警阈值,则报警。

2.如权利要求1所述的方法,其特征在于,所述步骤A1包括:

A11.确定风险要素,对全网段的网络空间资产风险样本数据进行采集;

A12.将采集到的风险样本数据进行漏洞扫描,并划分安全级别。

3.如权利要求2所述的方法,其特征在于,所述风险要素包括:目标IP、开放端口、服务器系统类型及版本、服务器应用类型及版本、存在的漏洞、数据库类型及版本、弱口令、是否采用CDN加速和防火墙中的一种或多种。

4.如权利要求2所述的方法,其特征在于,所述安全级别划分为:高危、中危、低危、安全四个安全级别,其比例为1:1:1:1,每种安全级别的数量≥5000。

5.如权利要求2所述的方法,其特征在于,所述步骤A1还包括:

A13.将网络空间资产风险样本数据转化为深度学习可识别的二进制样本数据。

6.如权利要求5所述的方法,其特征在于,所述步骤A13包括:

A131.将样本进行图片化处理,裁剪为统一大小;

A132.对裁剪后的图片进行白化处理。

7.如权利要求1所述的方法,其特征在于,所述步骤A2的所述分布式训练学习采用梯度递减的方式,其初始梯度为10^{-4}。

8.如权利要求1所述的方法,其特征在于,所述步骤A2包括:

A21.准备训练环境,训练环境采用Tensorflow GPU模式进行;

A22.从数据库中提取训练样本数据,结合卷积神经网络进行模型训练,得到初始风险预测模型;

A23.从数据库中提取测试样本数据,对初始风险预测模型进行评估测试。

9.如权利要求1所述的方法,其特征在于,所述步骤A22包括:

A221.模型网络结构,采用3个卷积层,第一个用3*3的卷积核,后面两个使用2*2的卷积核,每个卷积层后边都跟最大池化层,之后再跟两个隐藏层和一个输出层,每个卷积层的特征图分别用32、64、128;

A222.使用softmax函数进行回归,最后的输出层不需要softmax回归;

A223.利用训练样本数据进行训练,得到初始风险预测模型。

10.一种包含计算机程序的计算机可读存储介质,其特征在于,所述计算机程序被计算机执行以实现权利要求1-9任一所述的方法。

一种基于深度学习的网络风险预警方法

技术领域

[0001] 本发明涉及网络风险预警技术，尤其涉及一种针对于区域范围内，基于机器深度学习的网络风险预警方法与系统。

背景技术

[0002] 当前网络安全领域，检测一个目标是否安全，都是通过漏洞扫描，端口扫描等传统方式进行，这种方式针对单个目标且存在明显漏洞有效果，对于批量目标或者不存在明显漏洞的目标则无法快速全面的获取其安全状态。

发明内容

[0003] 为解决上述问题，本发明提供一种基于深度学习的网络风险预警方法及设备，其能够对批量目标或者不存在明显漏洞的目标进行快速全面地获取安全状态。

[0004] 本发明提供一种基于深度学习的网络风险预警方法，其特征在于，包含如下步骤：A1.采集全网段网络空间资产风险样本数据，并存入数据库；A2.从数据库中提取数据，进行卷积神经网络(CNN)分布式训练学习，形成风险预测模型；A3.将生产数据输入风险预测模型，评估其风险值，如达到预警阈值，则报警。

[0005] 优选地，所述步骤A1包括：A11.确定风险要素，对全网段的网络空间资产风险样本数据进行采集；A12.将采集到的风险样本数据进行漏洞扫描，并划分安全级别。

[0006] 进一步地优选，所述风险要素包括：目标IP、开放端口、服务器系统类型及版本、服务器应用类型及版本、存在的漏洞、数据库类型及版本、弱口令、是否采用CDN加速和防火墙中的一种或多种。

[0007] 进一步地优选，所述安全级别划分为：高危、中危、低危、安全四个安全级别，其比例为1:1:1:1，每种安全级别的数量≥5000。

[0008] 进一步地优选，所述步骤A1还包括：A13.将采集后的网络空间资产风险样本数据转化为深度学习可识别的二进制样本数据。

[0009] 更进一步地优选，所述步骤A13包括：A131.将样本进行图片化处理，裁剪为统一大小；A132.对裁剪后的图片进行白化处理。

[0010] 优选地，所述步骤A2的所述分布式训练学习采用梯度递减的方式，其初始梯度为10^{-4}。

[0011] 优选地，所述步骤A2包括：A21.准备训练环境，训练环境采用Tensorflow GPU模式进行；A22.从数据库中提取训练样本数据，结合卷积神经网络进行模型训练，得到风险预测模型；A23.从数据库中提取测试样本数据，对风险预测模型进行评估测试。

[0012] 更进一步地优选，所述步骤A22包括：A221.模型网络结构，采用3个卷积层，第一个用3*3的卷积核，后面两个使用2*2的卷积核，每个卷积层后边都跟最大池化层，之后再跟两个隐藏层和一个输出层，每个卷积层的特征图分别用32、64、128；A222.使用softmax函数进行回归，最后的输出层不需要softmax回归；A223.利用训练样本数据进行训练，得到初始风

险预测模型。

[0013] 本发明还提供一种包含计算机程序的计算机可读存储介质，所述计算机程序被计算机执行以实现如上所述的方法。

[0014] 本发明的有益效果：对全网段网络空间资产风险样本进行采集，并结合卷积神经网络(CNN)进行分布式训练学习，通过综合所有的局部结果，并结合神经网络分析进行自我学习和调整，得到的一个全面而综合的风险预测模型。该风险预测模型可对多个目标网络或不存在明显漏洞的目标进行安全风险评估与预警，能从整体上评估一个网络的安全状态；并提升了响应速度，快速发现风险点，提高了网络安全态势分析预测的处理效率和准确性；同时降低了维护成本，节省人力。

[0015] 在进一步的优选方案中还能获得更多的优点：利用CNN进行网络安全评估与预警的最大阻力是：应用场景学习样本的构建。本发明通过将风险样本的风险要素限定为：目标IP、开放端口、服务器系统类型及版本、服务器应用类型及版本、存在的漏洞、数据库类型及版本、弱口令、是否采用CDN加速、是否采用防火墙中的一种或几种，从而既节省CNN分布式训练的时间，又提高了安全评估与预警结果的准确性。

附图说明

[0016] 图1为本发明具体实施方式的基于深度学习的网络风险预警方法流程示意图。

[0017] 图2为本本发明具体实施方式中卷积神经网络分布式训练学习流程示意图。

具体实施方式

[0018] 下面结合具体实施方式并对照附图对本发明作进一步详细说明，应该强调的是，下述说明仅仅是示例性的，而不是为了限制本发明的范围及其应用。

[0019] 如图1所示，本实施例提供一种基于深度学习的网络风险预警方法，其包括如下步骤：

[0020] 步骤1.采集全网段网络空间资产风险样本数据。

[0021] 步骤1-1，对网络空间资产风险样本数据建库，通过对资产的风险点进行识别，确定风险要素，风险要素包括：目标IP、开放端口，服务器系统类型及版本，服务器应用类型及版本，存在的漏洞，数据库类型及版本，弱口令，是否采用CDN加速，是否采用防火墙。根据风险要素，对全网段的网络空间资产风险样本数据进行采集。

[0022] 通过提炼出如上所述对网络安全可能造成严重后果的风险要素，形成样本数据，可以保证后期深度学习预测结果的真实可靠性。有些风险要素看起来没有危险，但是组合到一起，就可能造成致命的漏洞。

[0023] 网络空间风险样本数据获取方法：使用“目标网络主机运行的服务类型及版本信息”侦测技术，“操作系统与设备类型等信息”侦测技术，“目标主机安全脆弱性”识别技术，“CDN、防火墙”识别技术来完成样本数据的收集工作，使用分布式技术来确保采集的样本具有实时性。

[0024] 步骤1-2.将采集到的风险样本数据进行漏洞扫描，并划分为四个安全级别：高危、中危、低危、安全。其中高危、中危、低危、安全四个安全级别的比例为1:1:1:1，每种安全级别的数量≥5000。

[0025] 通过安全等级的划分，每一种安全危险等级都包含有指定的不安全因素以及此漏洞可能带来的最大的损失程度，用户可以初步掌握漏洞的所属分类以及可能造成的损失，进行特定防御措施的制定，以此来减低用户面临网络危险的风险。

[0026] 步骤1-3.将网络空间资产风险样本数据转化为深度学习可识别的二进制样本数据。采集节点数据汇总于控制服务器，数据经过数据清洗后入库。

[0027] 数据清洗的任务是过滤掉不符合要求的数据，主要为不完整的数据、错误的数据以及重复的数据等。

[0028] 鉴于该数据库中的结果数据大多数为文本或数字，且组合情况繁多，在量化样本参数上存在很大的困难，难以形成深度学习的学习模型，因此将样本数据制作成图片。

[0029] 1)样本图片处理:将样本图片统一裁剪到100x100像素大小，裁剪中央区域用于评估或随机裁剪用于训练。

[0030] 2)对图片进行近似的白化处理，使模型对于图片的动态范围变化不敏感。步骤2.从数据库中提取数据，进行卷积神经网络分布式训练学习，形成风险预测模型。

[0031] 好的学习模型，不仅可以提高学习的速度，更能提高学习结果的准确性，同时要考虑到样本的数量，综合而言，CNN模型是当前最理想的深度学习模型。此步骤采用图片训练方式结合卷积神经网络擅长解决图片识别的特点进行训练。

[0032] 将学习模型划分两类样本:训练样本和测试样本。训练样本为调试、训练阶段所需的样本数据，用作调整深度学习所用的函数、方法，引导最终结果通往正确方向;测试样本作为验证准确性是否满足网络风险评估与预警的作用，用于评估阶段。训练样本为训练模型阶段使用的样本数据;测试样本为评估模型阶段所使用的样本数据。两类样本皆已知自变量和因变量。

[0033] 根据划分的样本，将训练机器形成风险预测模型，其过程如图2所示。

[0034] 步骤2-1.准备训练环境。训练环境采用Tensorflow GPU模式进行，GPU的计算速度比CPU快，能减少训练过程的时间成本。

[0035] 步骤2-2.训练模型阶段。在训练环境中使用步骤2准备好的训练样本结合卷积神经网络进行模型训练。训练过程如下：

[0036] 1)定义的模型网络结构，采用3个卷积层，第一个用3*3的卷积核，后面两个使用2*2的卷积核，每个卷积层后边都跟最大池化层，之后再跟两个隐藏层和一个输出层，每个卷积层的特征图分别用32、64、128。

[0037] 2)使用softmax函数进行回归，最后的输出层不需要softmax函数回归。

[0038] 3)模型网络结构定义好之后，进行训练，训练得到初始风险预测模型。

[0039] 以梯度递减方式进行准确度优化，其初始梯度为10^{-4};采用CNN分布式训练，通过梯度递减的方式使训练数据进行线性回归，达到平衡状态，从而找出对训练结果影响较大的因素，再将数据作为CNN输入进行分布式训练。数据并行化式的分布式训练在GPU的每个工作节点上都存储一个模型的备份，在各节点上处理数据的不同部分，再组合各个工作节点的结果，并且在节点之间同步模型参数;其能加快数据训练以及模型成立效率。

[0040] 步骤2-3.评估模型阶段。在训练环境中使用步骤2准备好的测试样本，对步骤2-2得到的初始风险预测模型进行评估测试，确认准确性是否合格。测试方法:输入测试样本到初始风险预测模型中，待输出结果后看是否与预期相匹配。匹配则投入生产流程，用于网络

风险的预警。不合格则回到步骤2-2进行算法优化，直至输出结果与预期相匹配。输出结果有四种:安全、低风险、中风险、高风险。

[0041] 通过如上方法建立的风险预测模型，根据形成样本数据的风险要素的不同，其风险预测模型的准确率不同。根据样本数据中所选取的风险要素，其形成风险预测模型的时间不同，且风险预测模型的准确率也不同，其结果如下表：

[0042]

参考因素	是否包含该因素									
目标IP	√	√	√	√	√	√	√	√	√	×
开放端口	√	√	√	√	√	√	√	√	×	×
服务器系统类型及版本	√	√	√	√	√	√	√	×	×	×
服务器应用类型及版本	√	√	√	√	√	√	×	×	×	×
存在漏洞	√	√	√	√	√	×	×	×	×	×
数据库类型及版本	√	√	√	√	×	×	×	×	×	×
弱口令	√	√	√	×	×	×	×	×	×	×
是否采用CDN加速	√	√	×	×	×	×	×	×	×	×
是否采用防火墙	√	×	×	×	×	×	×	×	×	×
准确率	95%	92%	83%	72%	43%	26%	7%	6%	1%	0
花费时间	5min	4.6min	4.2min	3.6min	3min	2min	1.3min	0.8min	80ms	5ms

[0043] 从上表中可知:当风险要素包括“目标IP,开放端口,服务器系统类型及版本,服务器应用类型及版本,存在的漏洞,数据库类型及版本,弱口令,是否采用CDN加速,是否采用防火墙”时，其风险预测模型的准确率高，且学习时间短，而当风险要素缺少其中的某一个时，其结果缺乏准确性。

[0044] 当风险要素多余这些时，实验结果表明:其学习时间长，形成风险预测模型的时间长，耗费的成本高。通过选取适当的风险要素:“目标IP,开放端口,服务器系统类型及版本,服务器应用类型及版本,存在的漏洞,数据库类型及版本,弱口令,是否采用CDN加速,是否采用防火墙”，使得学习时间短，且形成的风险预测模型的准确率高，即又快又准。

[0045] 步骤3.将生产数据输入风险预测模型，评估其风险值，如达到预警阈值，则报警。

[0046] 以上内容是结合具体/优选的实施方式对本发明所作的进一步详细说明，不能认定本发明的具体实施只局限于这些说明。对于本发明所属技术领域的普通技术人员来说，在不脱离本发明构思的前提下，其还可以对这些已描述的实施方式做出若干替代或变型，而这些替代或变型方式都应当视为属于本发明的保护范围。

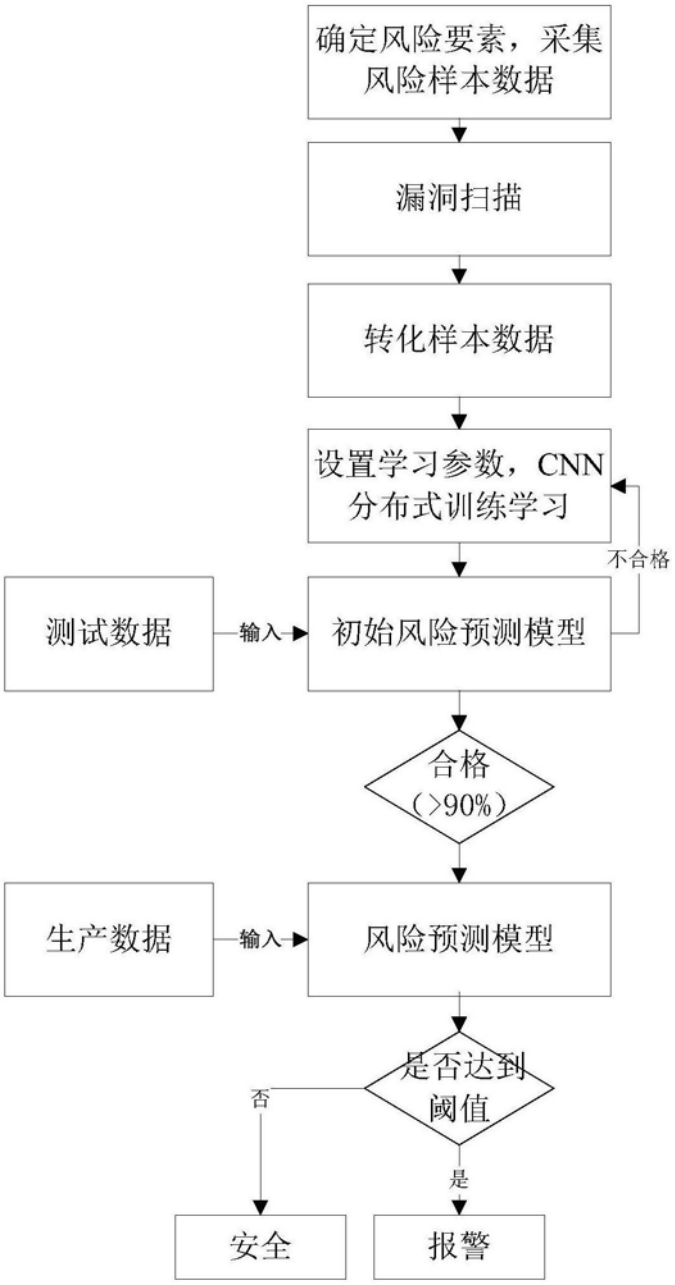

确定风险要素，采集风险样本数据
漏洞扫描
转化样本数据
设置学习参数，CNN分布式训练学习
不合格
测试数据
输入
初始风险预测模型
合格（>90%）
生产数据
输入
风险预测模型
是否达到阈值
否
是
安全
报警

图1

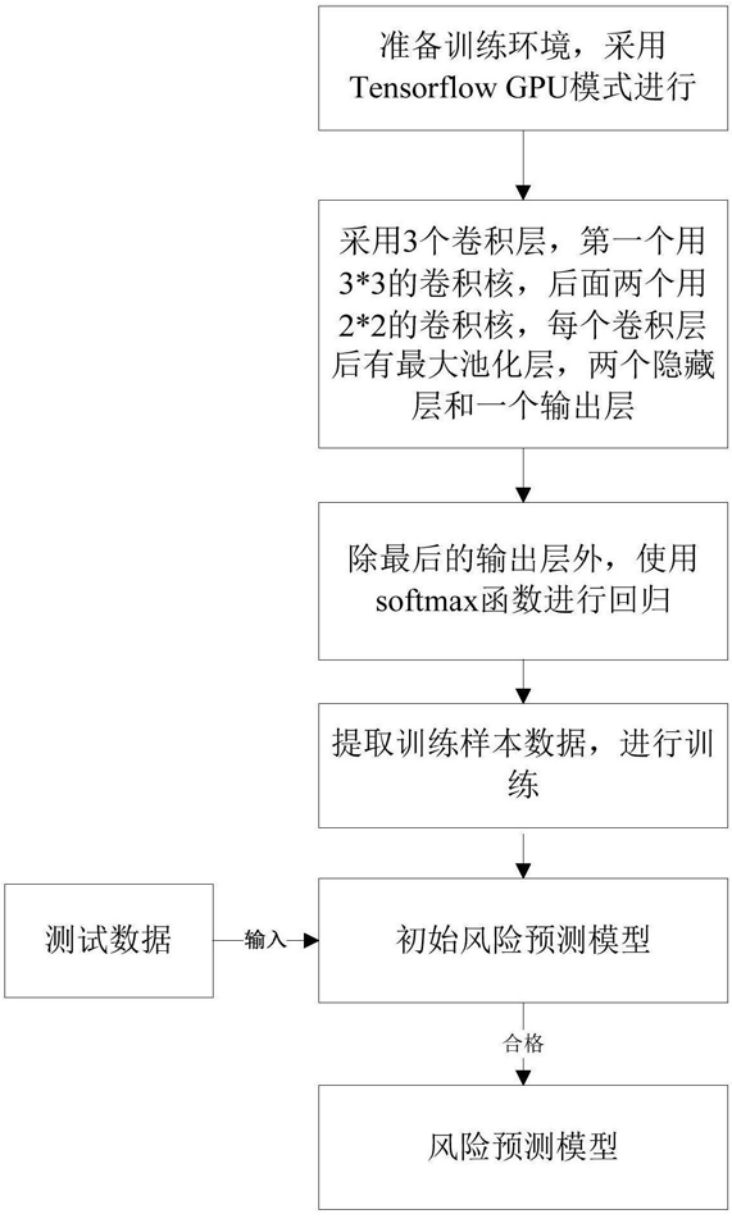

准备训练环境，采用Tensorflow GPU模式进行
采用3个卷积层，第一个用3*3的卷积核，后面两个用2*2的卷积核，每个卷积层后有最大池化层，两个隐藏层和一个输出层
除最后的输出层外，使用softmax函数进行回归
提取训练样本数据，进行训练
测试数据
输入
初始风险预测模型
合格
风险预测模型

图2