(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118540075 A
(43)申请公布日 2024.08.23

(21)申请号 202310154406.4

(22)申请日 2023.02.22

(71)申请人 中国科学院计算机网络信息中心
地址 100190 北京市海淀区中关村南四街4号院内2号楼

(72)发明人 宫良一 龙春 付豪 黄潘 王跃达 付豪豪

(74)专利代理机构 北京知舟专利事务所(普通合伙) 11550
专利代理师 郭韫

(51)Int.Cl.
H04L 9/40(2022.01)
G06N 3/0464(2023.01)
G06N 3/0442(2023.01)
H04L 61/4511(2022.01)
G06N 3/045(2023.01)

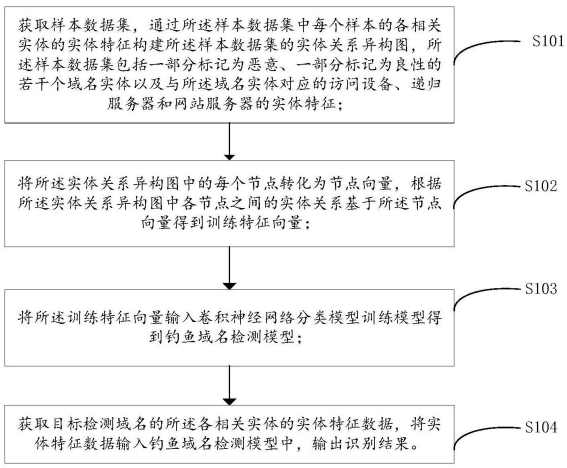
权利要求书2页 说明书11页 附图3页

(54)发明名称

基于实体关系挖掘的钓鱼攻击域名识别方法、系统和装置

(57)摘要

本申请公开了一种基于实体关系挖掘的钓鱼攻击域名识别方法、系统和装置，该方法通过获取样本数据集，通过所述样本数据集中每个样本的各相关实体的实体特征构建所述样本数据集的实体关系异构图；将所述实体关系异构图中的每个节点转化为节点向量，根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量；将所述训练特征向量输入卷积神经网络分类模型训练模型得到钓鱼域名检测模型；获取目标检测域名的所述各相关实体的实体特征数据，将实体特征数据输入钓鱼域名检测模型中，输出识别结果。实现对钓鱼网站域名进行及时检查，不依赖黑白名单，能够避免视觉上的逃逸检测，能够对抗攻击者精心设计的逃逸技术。



CN 118540075 A

1.一种基于实体关系挖掘的钓鱼攻击域名识别方法,其特征在于,包括:

获取样本数据集,通过所述样本数据集中每个样本的各相关实体的实体特征构建所述样本数据集的实体关系异构图,所述样本数据集包括一部分标记为恶意、一部分标记为良性的若干个域名实体以及与所述域名实体对应的访问设备、递归服务器和网站服务器的实体特征;

将所述实体关系异构图中的每个节点转化为节点向量,根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量;

将所述训练特征向量输入卷积神经网络分类模型训练模型得到钓鱼域名检测模型;

获取目标检测域名的所述各相关实体的实体特征数据,将实体特征数据输入钓鱼域名检测模型中,输出识别结果。

2.根据权利要求1所述的基于实体关系挖掘的钓鱼攻击域名识别方法,其特征在于,在获取样本集之前,还包括:捕获网络流量中每个访问请求对应的域名系统的流量数据得到每个样本;根据所述流量数据获取访问请求对应的源IP地址、目的IP地址、域名以及域名系统提供的解析访问请求的解析IP地址;基于预设的黑名单与白名单确定获取到的所述域名的标签属性;响应于得到所述域名的标签属性,根据所述源IP地址、目的IP地址、域名和解析IP地址获取所述各相关实体的实体特征;根据所述标签属性和所述实体特征构建带有标签的钓鱼域名实体关系和正常域名实体关系的数据集得到所述样本数据集。

3.根据权利要求2所述的基于实体关系挖掘的钓鱼攻击域名识别方法,其特征在于,所述各相关实体包括访问设备、域名实体、递归服务器和网站服务器;所述根据所述源IP地址、目的IP地址、域名和解析IP地址获取所述各相关实体的实体特征,包括:根据所述标签属性确定所述域名实体的实体特征;根据所述源IP地址确定所述源IP对应的访问设备的实体特征;根据所述目的IP地址确定所述网站服务器的实体特征;根据所述解析IP地址确定所述递归服务器的实体特征。

4.根据权利要求3所述的基于实体关系挖掘的钓鱼攻击域名识别方法,其特征在于,所述基于预设的黑名单与白名单确定获取到的所述域名的标签属性,包括:将获取到的所述域名与预设的黑名单中的钓鱼域名和白名单中的正常域名进行匹配,如果匹配到钓鱼域名,则将所述域名标记钓鱼域名标签,如果匹配到正常域名,则将所述域名标记正常域名标签,如果未匹配到,则丢弃所述域名。

5.根据权利要求4所述的基于实体关系挖掘的钓鱼攻击域名识别方法,其特征在于,所述根据所述标签属性和所述实体特征构建带有标签的钓鱼域名实体关系和正常域名实体关系的数据集得到所述样本数据集,包括:建立每个样本的所述访问设备、域名实体、递归服务器和网站服务器的实体特征的关系,并根据域名标签对所述域名对应的所述访问设备、域名实体、递归服务器和网站服务器的实体特征打上与域名标签相同的标签;将所述实体特征输入二维数据表进行存储得到所述样本数据集。

6.根据权利要求1-5任一项所述的基于实体关系挖掘的钓鱼攻击域名识别方法,其特征在于,所述将所述实体关系异构图中的每个节点转化为节点向量,根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量,包括:利用自编码器对所述实体关系异构图中每一个节点的特征进行特征向量编码得到每一个节点的节点向量;将每个相关实体的所有节点向量进行聚合得到每个相关实体的聚合向量,将所述聚合

向量输入LSTM模型中，将LSTM模型的最后一层作为所述聚合向量的输出向量；根据所述实体关系异构图中所有相关实体之间的异构实体关系，按照每个实体关系将对应的所述输出向量输入基于注意力机制的LSTM模型中，得到所述训练特征向量。

7.根据权利要求6所述的基于实体关系挖掘的钓鱼攻击域名识别方法，其特征在于，在将每个相关实体的所有节点向量进行聚合得到每个相关实体的聚合向量时，使用随机游走技术确定异构图中的采样节点。

8.根据权利要求6所述的基于实体关系挖掘的钓鱼攻击域名识别方法，其特征在于，所述将实体特征数据输入钓鱼域名检测模型中，输出识别结果，包括：利用自编码器将实体特征数据进行特征向量编码得到目标检测域名的各相关实体的实体特征数据的特征向量，将特征向量输入钓鱼域名检测模型中，根据特征向量得到识别结果并输出。

9.一种基于实体关系挖掘的钓鱼攻击域名识别系统，其特征在于，包括：

异构图生成单元，用于获取样本数据集，通过所述样本数据集中每个样本的各相关实体的实体特征构建所述样本数据集的实体关系异构图，所述样本数据集包括一部分标记为恶意、一部分标记为良性的若干个域名实体以及与所述域名实体对应的访问设备、递归服务器和网站服务器的实体特征；

特征处理单元，用于将所述实体关系异构图中的每个节点转化为节点向量，根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量；

模型训练单元，用于将所述训练特征向量输入卷积神经网络分类模型训练模型得到钓鱼域名检测模型；

检测单元，用于获取目标检测域名的所述各相关实体的实体特征数据，将实体特征数据输入钓鱼域名检测模型中，输出识别结果。

10.一种电子设备，其特征在于，包括存储器和处理器，所述存储器中存储有计算机程序，所述计算机程序被所述处理器执行时，使得所述处理器执行权利要求1至8中任一项所述的基于实体关系挖掘的钓鱼攻击域名识别方法的步骤。

基于实体关系挖掘的钓鱼攻击域名识别方法、系统和装置

技术领域

[0001] 本申请属于计算机技术领域，具体而言，涉及一种基于实体关系挖掘的钓鱼攻击域名识别方法、系统和装置。

背景技术

[0002] 网络钓鱼是当今最严重的网络攻击之一。攻击者利用各种手段来仿冒真实网站的网络地址以及网页内容来构建钓鱼网站。攻击者能够利用钓鱼网站来诱骗获取用户的个人账户信息，进而实施电信诈骗、渗透攻击等恶意行为，给用户的财产安全和业务安全造成巨大的威胁。攻击者往往会利用钓鱼邮件或者DNS劫持将用户访问引导到钓鱼网站，而用户很难察觉到这个攻击过程。不同于其他主动攻击，网络钓鱼的请求是由用户发起，防火墙无法对用户请求进行细致分析。随着Web加密技术的普及，传统的基于URL和网页内容的钓鱼网站检测技术难以奏效，通过钓鱼域名来发现钓鱼网站成为当前钓鱼检测的重要技术。然而钓鱼网站往往采用与正常网站近似的域名，导致基于字符特征的域名识别技术准确率低。因此，钓鱼网站识别成为目前亟待解决的关键技术。

[0003] 现有技术对于钓鱼网站的检测方法包括用户举报、黑白名单、网页内容识别以及网站特征分析等技术；用户举报主要依赖于有安全意识的用户积极上报安全防护软件以及遭受到损失的用户反馈；黑白名单技术则是在入侵检测系统中植入大量的已知钓鱼网络URL，一旦发现钓鱼网站则进行流量阻断；网页内容识别主要是利用视觉技术来对比分析钓鱼网站和正常网站的视觉差异性；近些年随着人工智能技术的发展，有工作利用机器学习或深度学习来识别钓鱼网站，通过提取网站上相关元素来构建检测特征，利用已标记的钓鱼网站数据来训练人工智能检测模型。

[0004] 目前用来检测钓鱼网站的三种自动化方法：1)基于黑白名单的检测方法，钓鱼网站黑名单的有效性取决于其名单范围、更新速度和频率以及其他特征，无法检测出未列入黑名单的钓鱼网站，具有一定的滞后性；2)基于视觉相似性检测技术，对于高仿真的钓鱼网站漏报率较高，并且对于未知的网站无法跟踪检测；3)基于机器学习算法的检测方法，对于已知的钓鱼网站具有很好的检测能力，但是对于高级的钓鱼网站往往漏报率较高，因为攻击者往往会采用URL混淆或扰乱技巧逃逸机器学习检测，而且有的钓鱼网站已经采用二维码技术来躲避URL检测。

发明内容

[0005] 因此，本申请实施例在于提供一种基于实体关系挖掘的钓鱼攻击域名识别方法、系统和装置，旨在解决上述现有技术存在的至少一个问题。

[0006] 为实现上述目的，第一方面，本申请提供了一种基于实体关系挖掘的钓鱼攻击域名识别方法，包括：

[0007] 获取样本数据集，通过所述样本数据集中每个样本的各相关实体的实体特征构建所述样本数据集的实体关系异构图，所述样本数据集包括一部分标记为恶意、一部分标记

为良性的若干个域名实体以及与所述域名实体对应的访问设备、递归服务器和网站服务器的实体特征；

[0008] 将所述实体关系异构图中的每个节点转化为节点向量，根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量；

[0009] 将所述训练特征向量输入卷积神经网络分类模型训练模型得到钓鱼域名检测模型；

[0010] 获取目标检测域名的所述各相关实体的实体特征数据，将实体特征数据输入钓鱼域名检测模型中，输出识别结果。

[0011] 在一个实施例中，在获取样本集之前，还包括：捕获网络流量中每个访问请求对应的域名系统的流量数据得到每个样本；根据所述流量数据获取访问请求对应的源IP地址、目的IP地址、域名以及域名系统提供的解析访问请求的解析IP地址；基于预设的黑名单与白名单确定获取到的所述域名的标签属性；响应于得到所述域名的标签属性，根据所述源IP地址、目的IP地址、域名和解析IP地址获取所述各相关实体的实体特征；根据所述标签属性和所述实体特征构建带有标签的钓鱼域名实体关系和正常域名实体关系的数据集得到所述样本数据集。

[0012] 在一个实施例中，所述各相关实体包括访问设备、域名实体、递归服务器和网站服务器；所述根据所述源IP地址、目的IP地址、域名和解析IP地址获取所述各相关实体的实体特征，包括：根据所述标签属性确定所述域名实体的实体特征；根据所述源IP地址确定所述源IP对应的访问设备的实体特征；根据所述目的IP地址确定所述网站服务器的实体特征；根据所述解析IP地址确定所述递归服务器的实体特征。

[0013] 在一个实施例中，所述基于预设的黑名单与白名单确定获取到的所述域名的标签属性，包括：将获取到的所述域名与预设的黑名单中的钓鱼域名和白名单中的正常域名进行匹配，如果匹配到钓鱼域名，则将所述域名标记钓鱼域名标签，如果匹配到正常域名，则将所述域名标记正常域名标签，如果未匹配到，则丢弃所述域名。

[0014] 在一个实施例中，所述根据所述标签属性和所述实体特征构建带有标签的钓鱼域名实体关系和正常域名实体关系的数据集得到所述样本数据集，包括：建立每个样本的所述访问设备、域名实体、递归服务器和网站服务器的实体特征的关系，并根据域名标签对所述域名对应的所述访问设备、域名实体、递归服务器和网站服务器的实体特征打上与域名标签相同的标签；将所述实体特征输入二维数据表进行存储得到所述样本数据集。

[0015] 在一个实施例中，所述将所述实体关系异构图中的每个节点转化为节点向量，根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量，包括：利用自编码器对所述实体关系异构图中每一个节点的特征进行特征向量编码得到每一个节点的节点向量；将每个相关实体的所有节点向量进行聚合得到每个相关实体的聚合向量，将所述聚合向量输入LSTM模型中，将LSTM模型的最后一层作为所述聚合向量的输出向量；根据所述实体关系异构图中所有相关实体之间的异构实体关系，按照每个实体关系将对应的所述输出向量输入基于注意力机制的LSTM模型中，得到所述训练特征向量。

[0016] 在一个实施例中，在将每个相关实体的所有节点向量进行聚合得到每个相关实体的聚合向量时，使用随机游走技术确定异构图中的采样节点。

[0017] 在一个实施例中，所述将实体特征数据输入钓鱼域名检测模型中，输出识别结果，

包括:利用自编码器将实体特征数据进行特征向量编码得到目标检测域名的各相关实体的实体特征数据的特征向量,将特征向量输入钓鱼域名检测模型中,根据特征向量得到识别结果并输出。

[0018] 第二方面,本申请还提供了一种基于实体关系挖掘的钓鱼攻击域名识别系统,包括:

[0019] 异构图生成单元,用于获取样本数据集,通过所述样本数据集中每个样本的各相关实体的实体特征构建所述样本数据集的实体关系异构图,所述样本数据集包括一部分标记为恶意、一部分标记为良性的若干个域名实体以及与所述域名实体对应的访问设备、递归服务器和网站服务器的实体特征;

[0020] 特征处理单元,用于将所述实体关系异构图中的每个节点转化为节点向量,根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量;

[0021] 模型训练单元,用于将所述训练特征向量输入卷积神经网络分类模型训练模型得到钓鱼域名检测模型;

[0022] 检测单元,用于获取目标检测域名的所述各相关实体的实体特征数据,将实体特征数据输入钓鱼域名检测模型中,输出识别结果。

[0023] 第三方面,本申请还提供了一种电子设备,包括存储器和处理器,所述存储器中存储有计算机程序,所述计算机程序被所述处理器执行时,使得所述处理器执行所述基于实体关系挖掘的钓鱼攻击域名识别方法的步骤。

[0024] 第四方面,本申请还提供了一种计算机可读存储介质,所述计算机可读存储介质上存储有计算机程序,所述计算机程序被处理器执行时,使得所述处理器执行所述基于实体关系挖掘的钓鱼攻击域名识别方法的步骤。

[0025] 本申请实施例提供的一种基于实体关系挖掘的钓鱼攻击域名识别方法、系统、电子设备及存储介质,通过获取样本数据集,通过所述样本数据集中每个样本的各相关实体的实体特征构建所述样本数据集的实体关系异构图,所述样本数据集包括一部分标记为恶意、一部分标记为良性的若干个域名实体以及与所述域名实体对应的访问设备、递归服务器和网站服务器的实体特征;将所述实体关系异构图中的每个节点转化为节点向量,根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量;将所述训练特征向量输入卷积神经网络分类模型训练模型得到钓鱼域名检测模型;获取目标检测域名的所述各相关实体的实体特征数据,将实体特征数据输入钓鱼域名检测模型中,输出识别结果。本申请提供的钓鱼攻击域名识别方法,采用的是基于域名实体关系的钓鱼网站检测;首先,能够对钓鱼网站域名进行及时检查,不依赖黑白名单;其次,是对域名访问IP、域名、递归解析器、服务器IP等多个实体关系挖掘,能够避免视觉上的逃逸检测;另外,不依赖URL特定的特征,而是挖掘钓鱼网站的实体关系结构,能够对抗攻击者精心设计的逃逸技术。

附图说明

[0026] 图1为本发明实施例提供的基于实体关系挖掘的钓鱼攻击域名识别方法的流程图;

[0027] 图2为本发明实施例提供的基于实体关系挖掘的钓鱼攻击域名识别方法的实体关

系异构图；

[0028] 图3为本发明实施例提供的基于实体关系挖掘的钓鱼攻击域名识别方法的架构示意图；

[0029] 图4为本发明实施例提供的基于实体关系挖掘的钓鱼攻击域名识别系统的主要模块图；

[0030] 图5为本申请实施例提供的可以应用于其中的示例性系统架构图；

[0031] 图6为适于用来实现本申请实施例的终端设备或服务器的计算机系统的结构示意图。

具体实施方式

[0032] 为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分的实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护的范围。

[0033] 需要说明的是，本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0034] 并且，上述部分术语除了可以用于表示方位或位置关系以外，还可能用于表示其他含义，例如术语“上”在某些情况下也可能用于表示某种依附关系或连接关系。对于本领域普通技术人员而言，可以根据具体情况理解这些术语在本申请中的具体含义。

[0035] 另外，术语“多个”的含义应为两个以及两个以上。

[0036] 需要说明的是，目前用来检测钓鱼网站主要有三种自动化方法：1)基于黑白名单的检测方法：将待检测的网站URL与黑白名单中的URL进行对比，来判断是否为钓鱼网站。这种方法实现简单、易于部署，但钓鱼网站黑名单的有效性取决于其名单范围、更新速度和频率以及其他特征，所以这种方法无法检测出未列入黑名单的钓鱼网站，具有一定的滞后性。2)基于视觉相似性检测技术：提取钓鱼网页的视觉特征，与目标网页特征之间进行差异对比，达到某个阈值则认为是一个钓鱼网站。然而这种技术对于高仿真的钓鱼网站漏报率较高，并且对于未知的网站无法跟踪检测。3)基于机器学习算法的检测方法：使用机器学习的方法提取URL和网站的相关特征，输入分类器得到最终结果。基于机器学习或深度学习算法的方法对于已知的钓鱼网站具有很好的检测能力，但是对于高级的钓鱼网站往往漏报率较高，因为攻击者往往会采用URL混淆或扰乱技巧逃逸机器学习检测，而且有的钓鱼网站已经采用二维码技术来躲避URL检测。

[0037] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0038] 图1示出了本申请实施例提供的一种基于实体关系挖掘的钓鱼攻击域名识别方法

的实现流程，为了便于说明，仅示出与本申请实施例相关的部分，详述如下：

[0039] 一种基于实体关系挖掘的钓鱼攻击域名识别方法，包括：

[0040] S101：获取样本数据集，通过所述样本数据集中每个样本的各相关实体的实体特征构建所述样本数据集的实体关系异构图，所述样本数据集包括一部分标记为恶意、一部分标记为良性的若干个域名实体以及与所述域名实体对应的访问设备、递归服务器和网站服务器的实体特征；

[0041] S102：将所述实体关系异构图中的每个节点转化为节点向量，根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量；

[0042] S103：将所述训练特征向量输入卷积神经网络分类模型训练模型得到钓鱼域名检测模型；

[0043] S104：获取目标检测域名的所述各相关实体的实体特征数据，将实体特征数据输入钓鱼域名检测模型中，输出识别结果。

[0044] 即本申请实施例提供的基于实体关系挖掘的钓鱼攻击域名识别方法，通过挖掘并构建域名相关实体的实体关系异构图，并基于挖掘的实体关系异构图训练识别模型得到域名检测模型，在域名检测时先将域名的各相关实体进行识别获取，基于域名检测模型对相关实体进行识别判断后得到域名的识别结果。首先，该技术能够对钓鱼网站域名进行及时检查，不依赖黑白名单；其次，该技术是对域名访问IP、域名、递归解析器、服务器IP等多个实体关系挖掘，能够避免视觉上的逃逸检测；另外，该技术不依赖URL特定的特征，而是挖掘钓鱼网站的实体关系结构，能够对抗攻击者精心设计的逃逸技术。

[0045] 在步骤S101中，获取样本数据集，通过所述样本数据集中每个样本的各相关实体的实体特征构建所述样本数据集的实体关系异构图，所述样本数据集包括一部分标记为恶意、一部分标记为良性的若干个域名实体以及与所述域名实体对应的访问设备、递归服务器和网站服务器的实体特征。在这里，样本数据集中有部分样本是恶意域名，有部分样本是非恶意样本，即良性样本；通过对样本数据集中的样本预先打标，并挖掘构建每个样本的各相关实体的实体特征之间的实体关系，然后根据实体关系构建每个样本的各相关实体的实体关系异构图，由此，每个恶意样本或者良性样本均有对应的实体关系异构图，通过实体关系异构图便可以得知恶意样本或者良性样本的各相关实体的对应实体特征，进而可以通过每个相关实体特征判断出域名是属于恶意或良性。需要说明的是，各相关实体指的是每个域名相关的域名实体以及与所述域名实体对应的访问设备、递归服务器和网站服务器的实体特征，即各相关实体包括了域名实体、访问设备、递归服务器和网站服务器等实体，通过获取每个样本(即每个样本域名)的各实体的实体特征，便可以构建每个样本的实体关系异构图，以此根据每个样本的实体关系异构图训练检测模型，进而可以根据域名的相关实体检测域名是否恶意或者良性，实现以下效果：首先，提高域名的检测精度，能够对钓鱼网站域名进行及时检查，不依赖黑白名单；其次，该技术是对域名访问IP、域名、递归解析器、服务器IP等多个实体关系挖掘，能够避免视觉上的逃逸检测；另外，该技术不依赖URL特定的特征，而是挖掘钓鱼网站的实体关系结构，能够对抗攻击者精心设计的逃逸技术。

[0046] 如图2所示，为本发明实施例提供的基于实体关系挖掘的钓鱼攻击域名识别方法的实体关系异构图。从图2中可以看出，可以通过样本数据集构建样本数据集的相关实体“访问设备、域名、递归服务器和网站服务器”之间的实体关系异构图，作为后续模型训练的

数据准备。在实体关系异构图中，异构节点可以分布是由访问设备、域名、递归服务器和网站服务器构成，每相邻两个异构节点之间通过元路径(边)连接，每个访问设备节点可以对应多个域名节点，每个域名节点可以对应多个递归服务器节点，每个递归服务器节点有也可以对应多个网站服务器节点。由此构成样本数据集的各相关实体的实体关系异构图，作为后续的模型训练的数据输入。

[0047] 具体的，访问设备(域名访问设备)的实体特征具体包括操作系统类型(Windows XP、Windows 7/8/10/11、Android 4～12、MacOS 6～12、Linux等)、设备资产类型(PC机、服务器、手机、物联网设备、专用设备)等。域名实体特征指域名本身的字符特征，具体包括域名的熵值、域名字符和数字比例、域名的n-gram信息、域名的长度，以及域名的注册特征，具体包括注册商域名注册商信息等；递归服务器的实体特征指域名请求解析的递归服务器地址、递归服务器所在网络的运营商、递归服务器是否为公开递归服务器、递归服务器所在的地理位置等；域名对应的网站服务器的实体特征指网站服务器的IP地址、网站服务器开放端口、网站服务器的运营商、网站服务器所在的地理位置、网站服务器开放的端口、网站服务器的IP地址是否为恶意IP等。

[0048] 在一个实施例中，在获取样本集之前，还包括：捕获网络流量中每个访问请求对应的域名系统的流量数据得到每个样本；根据所述流量数据获取访问请求对应的源IP地址、目的IP地址、域名以及域名系统提供的解析访问请求的解析IP地址；基于预设的黑名单与白名单确定获取到的所述域名的标签属性；响应于得到所述域名的标签属性，根据所述源IP地址、目的IP地址、域名和解析IP地址获取所述各相关实体的实体特征；根据所述标签属性和所述实体特征构建带有标签的钓鱼域名实体关系和正常域名实体关系的数据集得到所述样本数据集。即，在本申请的实施例提供的基于实体关系挖掘的钓鱼攻击域名识别方法实施过程中，不断获取网络流量中的每个访问请求对应的域名系统的流量数据，以不断收集样本数据得到样本数据集。通过对流量中的域名进行提取，提取后回对域名相关的实体进行提取以构建样本数据集。在这里，可以通过访问请求提取网络流量中的访问域名，再通过域名对相关的实体进行提取。具体的，提取到域名后，根据对应的访问源IP地址、目的IP地址提取得到访问设备和网站服务器的实体特征，根据域名系统的解析IP地址提取得到递归服务器的实体特征。同时，根据预设的域名黑名单和白名单，确定获取到的所述域名的标签属性，即域名是恶意或良性的标签，再将跟该域名相关的其他实体的实体特征对应进行相应的标签，最终构建带有标签的钓鱼域名实体关系和正常域名实体关系的数据集得到所述样本数据集。以便基于样本数据集构建实体关系异构图。

[0049] 进一步的，所述各相关实体包括访问设备、域名实体、递归服务器和网站服务器；所述根据所述源IP地址、目的IP地址、域名和解析IP地址获取所述各相关实体的实体特征，包括：根据所述标签属性确定所述域名实体的实体特征；根据所述源IP地址确定所述源IP对应的访问设备的实体特征；根据所述目的IP地址确定所述网站服务器的实体特征；根据所述解析IP地址确定所述递归服务器的实体特征。

[0050] 进一步的，所述基于预设的黑名单与白名单确定获取到的所述域名的标签属性，包括：将获取到的所述域名与预设的黑名单中的钓鱼域名和白名单中的正常域名进行匹配，如果匹配到钓鱼域名，则将所述域名标记钓鱼域名标签(或恶意标签)，如果匹配到正常域名，则将所述域名标记正常域名标签(或者良性标签)，如果未匹配到，则丢弃所述域名。

[0051] 进一步的,所述根据所述标签属性和所述实体特征构建带有标签的钓鱼域名实体关系和正常域名实体关系的数据集得到所述样本数据集,包括:建立每个样本的所述访问设备、域名实体、递归服务器和网站服务器的实体特征的关系,并根据域名标签对所述域名对应的所述访问设备、域名实体、递归服务器和网站服务器的实体特征打上与域名标签相同的标签;将所述实体特征输入二维数据表进行存储得到所述样本数据集。

[0052] 例如,通过预先在网络网关设备处采集大量的钓鱼域名相关的实体特征数据,建立从访问设备-域名-递归服务器-网站服务器四者之间的关联关系,并根据黑白名单对每个实体特征打上对应的标签,由此,在获取了实体特征的基础上构建带有标签的钓鱼域名实体关系和正常域名实体关系的样本数据集。

[0053] 示例性的,每个样本的各相关实体的实体特征获取技术可以为:1)捕获网络流量中的DNS流量数据;2)从DNS请求解析流量中提取源IP、目的IP和域名;3)从DNS响应流量中提取解析IP;4)将提取的域名与黑名单中钓鱼域名以及白名单中正常域名进行匹配;5)一旦匹配到则利用nslookup和whois查询域名实体特征(域名类型、注册商信息、SOA信息),利用nmap开源工具来查询源IP对应的访问设备实体特征(开放端口、操作系统类型、应用服务类型)、递归DNS对应的实体特征(IP地址、开放端口、BIND版本、运营商)以及网站服务器的实体特征(IP地址、开放端口、操作系统类型、应用服务版本)。最后,在获取了实体特征基础上构建带有标签的钓鱼域名实体关系和正常域名实体关系的数据集。这里的关系是指从访问设备-域名-递归服务器-网站服务器四者之间的关联关系。由此,将利用流量中DNS数据包请求和响应的对应关系来构建四者实体的关系矩阵,完成数据项序列构建,并基于数据项序列来构建异构图。

[0054] 在步骤S102中:将所述实体关系异构图中的每个节点转化为节点向量,根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量。实体关系异构图是由多个异构节点和路径边组成,每个异构节点的数据特征不相同,因此先将每个节点的特征进行向量化得到每个节点的节点向量,以便于进行数据处理和模型训练。将每个节点的特征向量化得到每个节点的节点向量后,根据实体异构图中的各异构节点之间的实体特征关系,将每个节点向量进行处理后得到一个总的输出向量作为训练特征向量。

[0055] 进一步的,所述将所述实体关系异构图中的每个节点转化为节点向量,根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量,包括:利用自编码器对所述实体关系异构图中每一个节点的特征进行特征向量编码得到每一个节点的节点向量;将每个相关实体的所有节点向量进行聚合得到每个相关实体的聚合向量,将所述聚合向量输入LSTM模型中,将LSTM模型的最后一层作为所述聚合向量的输出向量;根据所述实体关系异构图中所有相关实体之间的异构实体关系,按照每个实体关系将对应的所述输出向量输入基于注意力机制的LSTM模型中,得到所述训练特征向量。在这里,在将每个相关实体的所有节点向量进行聚合得到每个相关实体的聚合向量时,使用随机游走技术确定异构图中的采样节点。由此,本申请中采用的是随机游走技术来生成节点序列,其中包括节点和边的组合。由于节点之间是异构的,本实施例中使用基于元路径的随机游走。每个节点都采用概率性采样方式,获取的采样序列反映了该节点的特征。本申请实施例中元路径包括访问设备-域名-递归服务器、域名-递归服务器-网站服务器、访问设备-域名-网站服务器,设置路径中各节点的转移概率为0或者1;当采样一个节点时,按照某类元路径会

有不同的邻居节点,这里按照概率获取邻居节点加入采样序列中,之后再从该采样节点按照相同方式采样。为了避免某类样本采样过度,本申请实施例对每类样本都限制获取一定个数的采样节点。此外当采样到某一节点时,设置一定概率返回到初始采样节点,确保可以采集到相差较远的路径上的节点。

[0056] 在步骤S103中:将所述训练特征向量输入卷积神经网络分类模型训练模型得到钓鱼域名检测模型。在这里,卷积神经网络分类模型可以为卷积神经网络(CNN)分类模型。

[0057] 具体的,如图3为本发明实施例提供的基于实体关系挖掘的钓鱼攻击域名识别方法的架构示意图,示出了从异构图到模型训练的过程。在本实施例中,由于异构图节点特征类型不同需要映射到相同的特征空间,本申请实施例将利用自编码器技术来对异构图中每一个节点的特征进行特征向量编码,获得每一个节点的向量化表达方式。自编码器是一种无监督训练方法,本申请实施例在输入模型前使用大量的样本训练异构图中每类实体的自编码器,各个自编码器可以将不同实体不同维度的特征映射到相同大小的中间层上。本申请实施例中为了加快训练速度,中间层编码向量编码大小设定为16维大小。同时,本申请实施例中,对随机游走获得的同类型的邻居节点进行聚合,采用LSTM方法对输入的编码向量按照顺序采样对得到的相同类型邻居进行特征表达,将LSTM最后一层作为这一类型邻居的输出向量(Mean Pooling);其次,由于不同类型节点的重要程度不同,对于一个节点不同类型的异构邻居节点,本申请实施例采用基于注意力机制的LSTM技术来开展联合学习不同类型的邻居,获得一个预测节点统一的向量表达;最后,将统一的向量表达输入到一个卷积神经网络(CNN)分类模型,从而获得训练结果得到域名检测模型。在这里,模型训练过程中的损失函数为真实标签与预测标签的交叉熵损失函数,最后使用两层线性全连接层以及softmax激活函数输出良性和恶意的概率值,以得到域名的预测标签。由此,通过上述的流程和训练将得到基于异构图的钓鱼域名检测模型。

[0058] 在步骤S104中:获取目标检测域名的所述各相关实体的实体特征数据,将实体特征数据输入钓鱼域名检测模型中,输出识别结果。由此,实现在线域名的实时检测。首先,能够对钓鱼网站域名进行及时检查,不依赖黑白名单;其次,是对域名访问IP、域名、递归解析器、服务器IP等多个实体关系挖掘,能够避免视觉上的逃逸检测;另外,不依赖URL特定的特征,而是挖掘钓鱼网站的实体关系结构,能够对抗攻击者精心设计的逃逸技术。

[0059] 进一步的,所述将实体特征数据输入钓鱼域名检测模型中,输出识别结果,包括:利用自编码器将实体特征数据进行特征向量编码得到目标检测域名的各相关实体的实体特征数据的特征向量,将特征向量输入钓鱼域名检测模型中,根据特征向量得到识别结果并输出。在这里,实现对待检测域名的检测,并输出检测后的标签(即标记域名为钓鱼域名或者正常域名的标签)。由此,通过在线节点,入侵检测系统将对非白名单中的域名按照前述实施例所述的实体特征获取技术来获取域名各相关的实体特征,并利用自编码器来获得各实体的编码向量,进而将编码向量输入到钓鱼域名检测模型中进行判别。一旦识别为钓鱼域名则发出报警。本申请实施例中考虑到技术应用在高速流量的网络出入口,提出一种快速实体特征查找方法。由于访问设备、递归服务器等实体特征往往稳定,一旦查阅到相关的实体特征则将其特征存储到数据库中。在线域名实体特征获取时首先查阅本地缓存数据库中是否有实体特征关系,若有则直接提取向量特征,否则利用之前的特征获取进行来在线查阅。

[0060] 由此，本申请实施例提供的基于实体关系挖掘的钓鱼攻击域名识别方法，通过所述样本数据集中每个样本的各相关实体的实体特征构建所述样本数据集的实体关系异构图，所述样本数据集包括一部分标记为恶意、一部分标记为良性的若干个域名实体以及与所述域名实体对应的访问设备、递归服务器和网站服务器的实体特征；将所述实体关系异构图中的每个节点转化为节点向量，根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量；将所述训练特征向量输入卷积神经网络分类模型训练模型得到钓鱼域名检测模型；获取目标检测域名的所述各相关实体的实体特征数据，将实体特征数据输入钓鱼域名检测模型中，输出识别结果。本申请提供的钓鱼攻击域名识别方法，采用的是基于域名实体关系的钓鱼网站检测；首先，能够对钓鱼网站域名进行及时检查，不依赖黑白名单；其次，是对域名访问IP、域名、递归解析器、服务器IP等多个实体关系挖掘，能够避免视觉上的逃逸检测；另外，不依赖URL特定的特征，而是挖掘钓鱼网站的实体关系结构，能够对抗攻击者精心设计的逃逸技术。

[0061] 图4示出了本申请实施例提供的基于实体关系挖掘的钓鱼攻击域名识别系统的主要模块图，为了便于说明，仅示出与本申请实施例相关的部分，详述如下：

[0062] 一种基于实体关系挖掘的钓鱼攻击域名识别系统200，包括：

[0063] 异构图生成单元201，用于获取样本数据集，通过所述样本数据集中每个样本的各相关实体的实体特征构建所述样本数据集的实体关系异构图，所述样本数据集包括一部分标记为恶意、一部分标记为良性的若干个域名实体以及与所述域名实体对应的访问设备、递归服务器和网站服务器的实体特征；

[0064] 特征处理单元202，用于将所述实体关系异构图中的每个节点转化为节点向量，根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量；

[0065] 模型训练单元203，用于将所述训练特征向量输入卷积神经网络分类模型训练模型得到钓鱼域名检测模型；

[0066] 检测单元204，用于获取目标检测域名的所述各相关实体的实体特征数据，将实体特征数据输入钓鱼域名检测模型中，输出识别结果。

[0067] 需要说明的是，本申请实施例提供的基于实体关系挖掘的钓鱼攻击域名识别系统的其他实施例对应于本申请实施例提供的基于实体关系挖掘的钓鱼攻击域名识别方法的其他实施例描述，在这里不再赘述。

[0068] 由此，本申请实施例提供的基于实体关系挖掘的钓鱼攻击域名识别系统，采用的是基于域名实体关系的钓鱼网站检测；首先，能够对钓鱼网站域名进行及时检查，不依赖黑白名单；其次，是对域名访问IP、域名、递归解析器、服务器IP等多个实体关系挖掘，能够避免视觉上的逃逸检测；另外，不依赖URL特定的特征，而是挖掘钓鱼网站的实体关系结构，能够对抗攻击者精心设计的逃逸技术。

[0069] 图5示出了可以应用本申请实施例的基于实体关系挖掘的钓鱼攻击域名识别方法或系统的示例性系统架构300。

[0070] 如图5所示，系统架构300可以包括终端设备301、302、303，网络304和服务器305。网络304用以在终端设备301、302、303和服务器305之间提供通信链路的介质。网络304可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

[0071] 用户可以使用终端设备301、302、303通过网络304与服务器305交互，以接收或发

送消息等。终端设备301、302、303上可以安装有各种通讯客户端应用，例如购物类应用、网页浏览器应用、搜索类应用、即时通信工具、邮箱客户端、社交平台软件等。

[0072] 终端设备301、302、303可以是具有显示屏并且支持网页浏览的各种电子设备，包括但不限于智能手机、平板电脑、膝上型便携计算机和台式计算机等等。

[0073] 服务器305可以是提供各种服务的服务器，例如对用户利用终端设备301、302、303所发送的往来消息提供支持的后台管理服务器。后台管理服务器可以在接收到终端设备请求后进行分析等处理，并将处理结果反馈给终端设备。

[0074] 需要说明的是，本申请实施例所提供的基于实体关系挖掘的钓鱼攻击域名识别方法一般由终端设备301、302、303或服务器305执行，相应地，基于实体关系挖掘的钓鱼攻击域名识别系统一般设置于终端设备301、302、303或服务器305中。

[0075] 应该理解，图5中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和服务器。

[0076] 下面参考图6，其示出了适于用来实现本申请实施例的终端设备或服务器的计算机系统400的结构示意图。图6示出的计算机系统仅仅是一个示例，不应对本申请实施例的功能和使用范围带来任何限制。

[0077] 如图6所示，计算机系统400包括中央处理单元(CPU)401，其可以根据存储在只读存储器(ROM)402中的程序或者从存储部分408加载到随机访问存储器(RAM)403中的程序而执行各种适当的动作和处理。在RAM 403中，还存储有系统400操作所需的各种程序和数据。CPU 401、ROM 402以及RAM403通过总线404彼此相连。输入/输出(I/O)接口405也连接至总线404。

[0078] 以下部件连接至I/O接口405：包括键盘、鼠标等的输入部分406；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分407；包括硬盘等的存储部分408；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分409。通信部分409经由诸如因特网的网络执行通信处理。驱动器410也根据需要连接至I/O接口405。可拆卸介质411，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器410上，以便于从其上读出的计算机程序根据需要被安装入存储部分408。

[0079] 特别地，根据本申请公开的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本申请公开的实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信部分409从网络上被下载和安装，和/或从可拆卸介质411被安装。在该计算机程序被中央处理单元(CPU)401执行时，执行本申请的系统中限定的上述功能。

[0080] 需要说明的是，本申请所示的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本申请中，计算机可读存储介质可以是任何包含或存储程

序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本申请中，计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于：无线、电线、光缆、RF等等，或者上述的任意合适的组合。

[0081] 附图中的流程图和框图，图示了按照本申请各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0082] 描述于本申请实施例中所涉及到的模块可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的模块也可以设置在处理器中，例如，可以描述为：一种处理器包括确定模块、提取模块、训练模块和筛选模块。其中，这些模块的名称在某种情况下并不构成对该模块本身的限定，例如，确定模块还可以被描述为“确定候选用户集的模块”。

[0083] 以上所述实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对本申请专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。

[0084] 以上所述仅为本申请的优选实施例而已，并不用于限制本申请，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

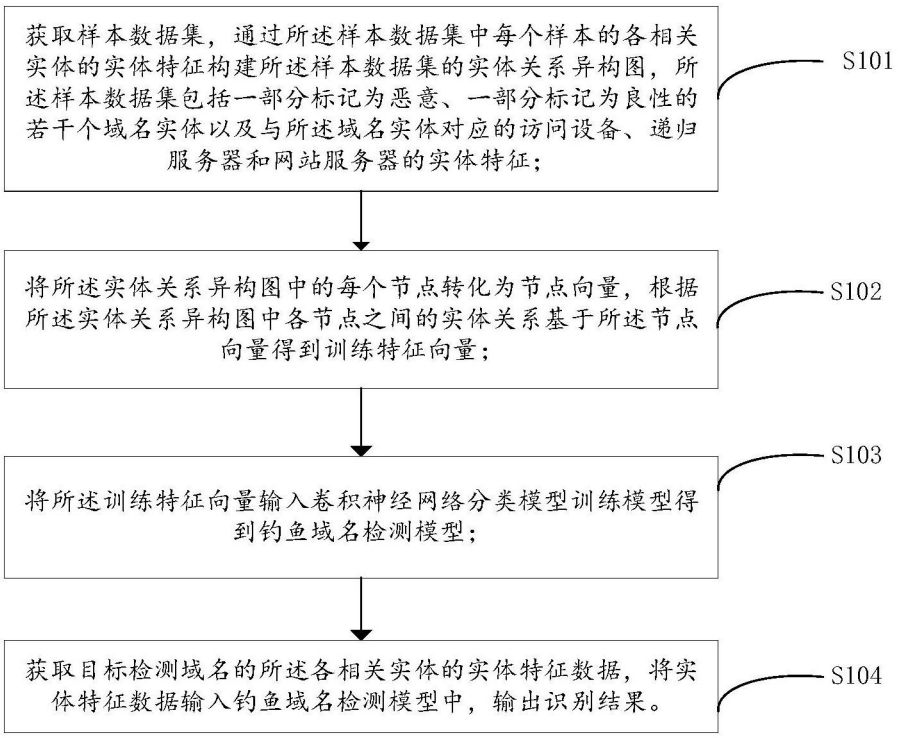

获取样本数据集，通过所述样本数据集中每个样本的各相关实体的实体特征构建所述样本数据集的实体关系异构图，所述样本数据集包括一部分标记为恶意、一部分标记为良性的若干个域名实体以及与所述域名实体对应的访问设备、递归服务器和网站服务器的实体特征；
S101
将所述实体关系异构图中的每个节点转化为节点向量，根据所述实体关系异构图中各节点之间的实体关系基于所述节点向量得到训练特征向量；
S102
将所述训练特征向量输入卷积神经网络分类模型训练模型得到钓鱼域名检测模型；
S103
获取目标检测域名的所述各相关实体的实体特征数据，将实体特征数据输入钓鱼域名检测模型中，输出识别结果。
S104

图1

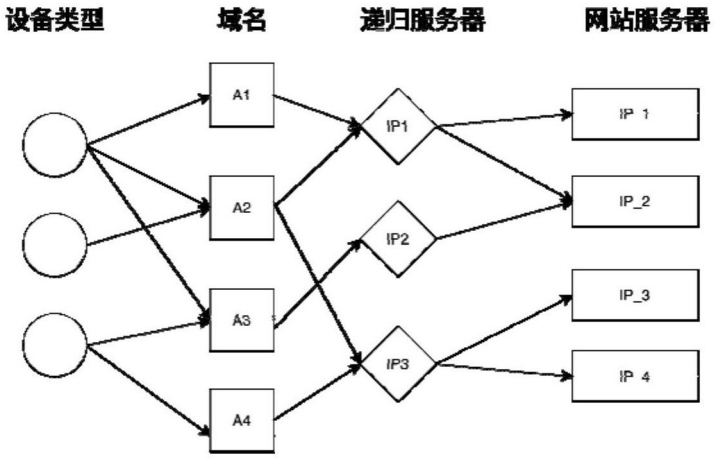

设备类型
域名
递归服务器
网站服务器
A1
A2
A3
A4
IP1
IP2
IP3
IP 1
IP_2
IP_3
IP 4

图2

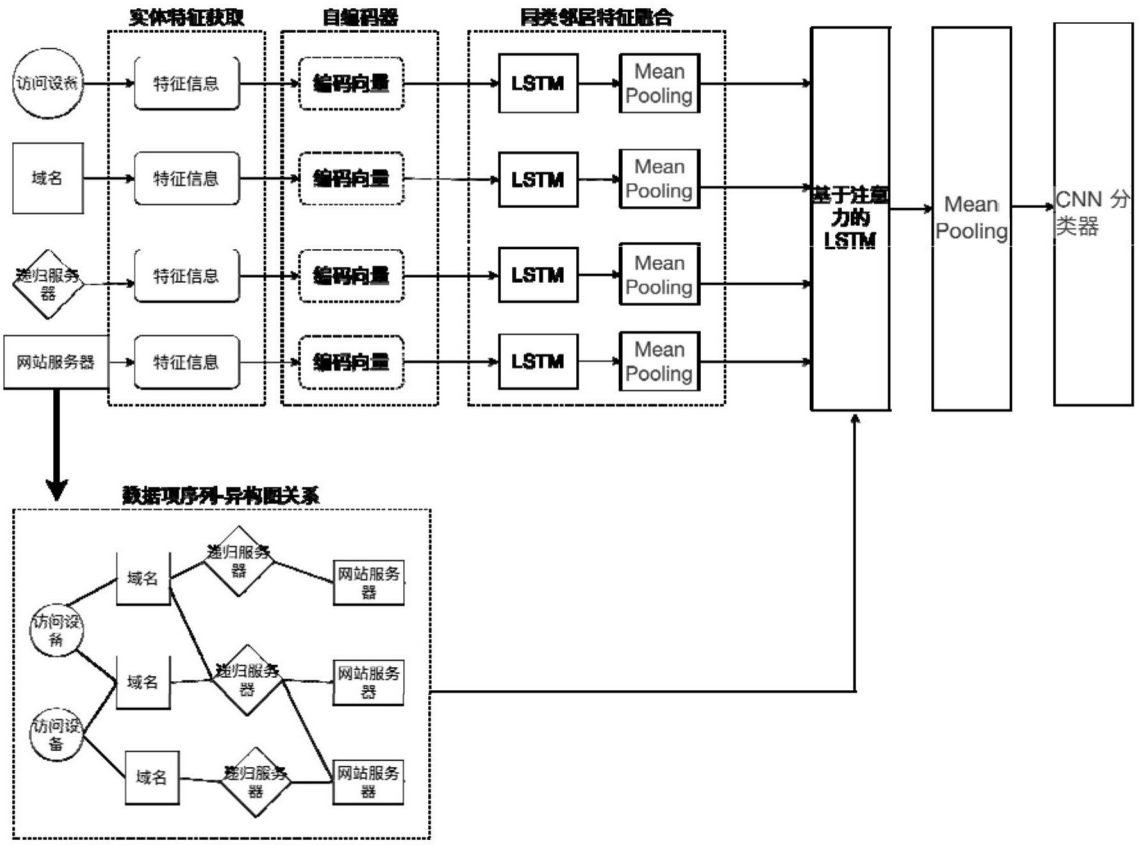

实体特征获取
自编码器
同类邻居特征融合
访问设备
域名
递归服务器
网站服务器
特征信息
编码向量
LSTM
Mean Pooling
基于注意力的LSTM
Mean Pooling
CNN 分类器
数据项序列-异构图关系

图3

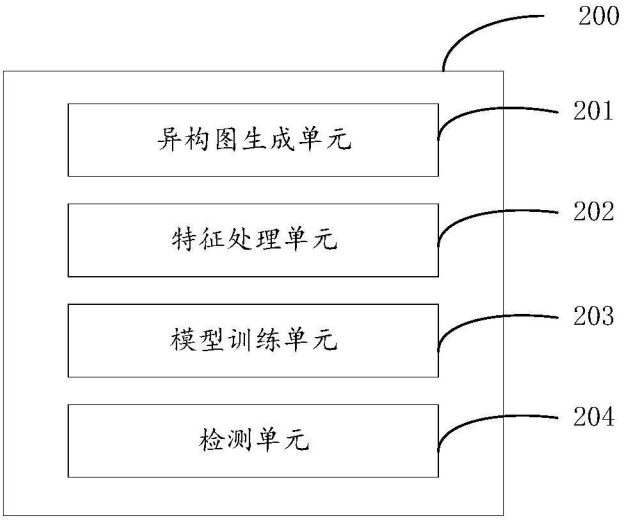

200
异构图生成单元
201
特征处理单元
202
模型训练单元
203
检测单元
204

图4

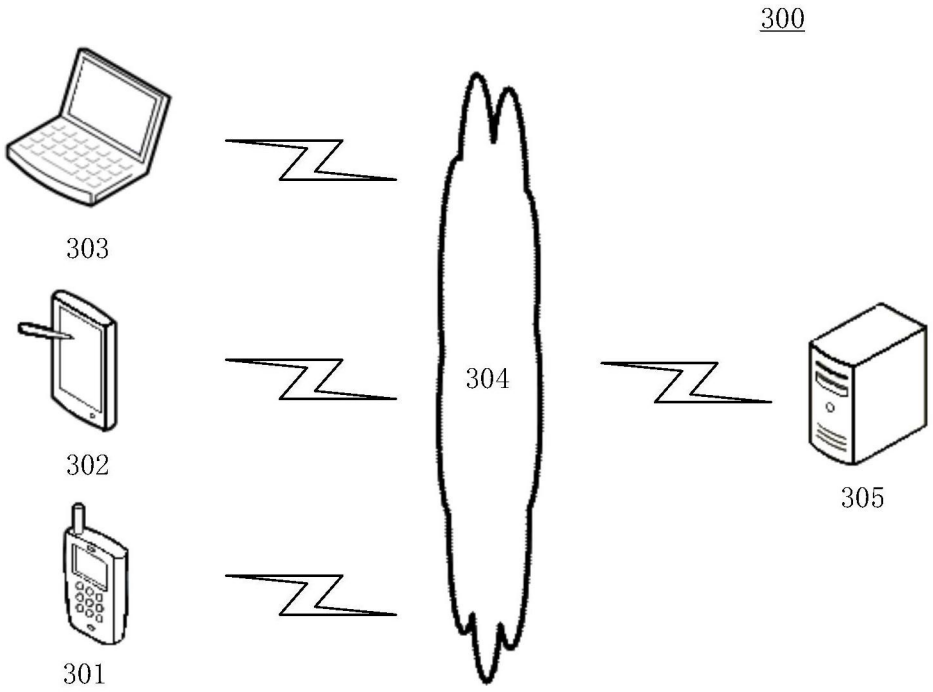

300
303
302
301
304
305

图5

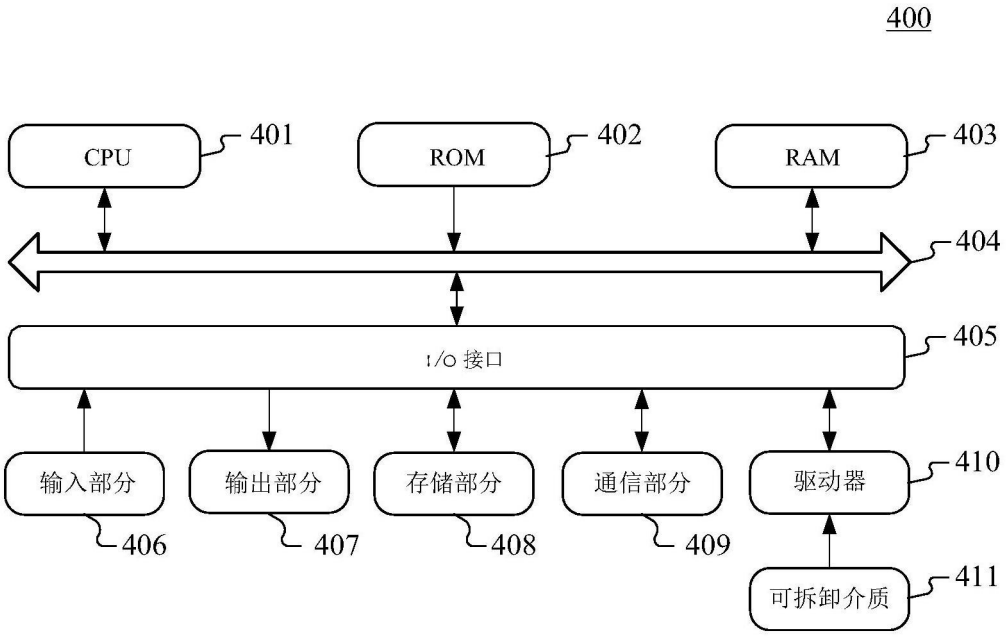

400
CPU
401
ROM
402
RAM
403
404
I/O 接口
405
输入部分
406
输出部分
407
存储部分
408
通信部分
409
驱动器
410
可拆卸介质
411

图6