(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 107241352 A
(43)申请公布日 2017.10.10

(21)申请号 201710579846.9

(22)申请日 2017.07.17

(71)申请人 浙江鹏信信息科技股份有限公司
地址 311100 浙江省杭州市余杭区仓前街道向往街1008号14幢9-10层

(72)发明人 陈晓莉 徐菁 丁一帆 刘亭 林建洪

(74)专利代理机构 杭州千克知识产权代理有限公司 33246
代理人 周希良

(51)Int.Cl.
H04L 29/06(2006.01)

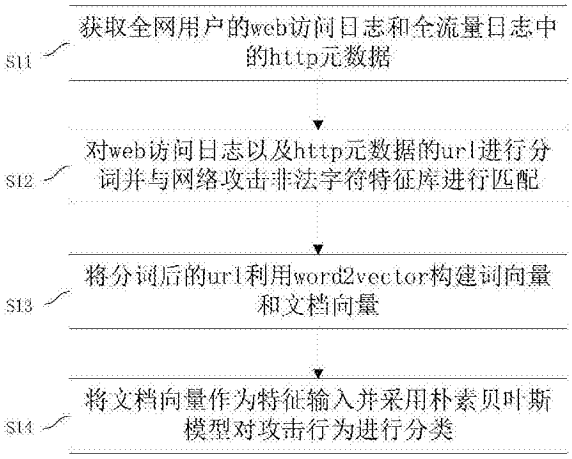
权利要求书2页 说明书10页 附图7页

(54)发明名称

一种网络安全事件分类与预测方法及系统

(57)摘要

本发明公开了一种网络安全事件分类与预测方法及系统，用以解决现有技术缺少及时发现攻击行为特征，对攻击行为进行准确分类的能力。该方法包括：S1、获取全网用户的web访问日志和全流量日志中的http元数据；S2、对所述web访问日志和所述http元数据的url进行分词并与网络攻击非法字符特征库进行匹配；S3、将分词后的url利用word2vector构建词向量和文档向量；S4、将所述文档向量作为特征输入并采用朴素贝叶斯模型对所述攻击行为进行分类。本发明实现关键点的实时监测，依靠机器学习发现带有主流攻击特征的异常行为，改善了网络攻击行为分类的效率，降低了人工审核的时间成本，能够适应不断变化的攻击行为，提高了分类检测准确率，为网络安全提供了保障。



CN 107241352 A

1.一种网络安全事件分类与预测方法,其特征在于,包括步骤:

S1、获取全网用户的web访问日志和全流量日志中的http元数据;

S2、对所述web访问日志和所述http元数据的url进行分词并与网络攻击非法字符特征库进行匹配;

S3、将分词后的url利用word2vector构建词向量和文档向量;

S4、将所述文档向量作为特征输入并采用朴素贝叶斯模型对所述攻击行为进行分类。

2.根据权利要求1所述的一种网络安全事件分类与预测方法,其特征在于,还包括步骤:

S5、识别不同种类的网络攻击行为;

S6、对所述各类网络攻击行为采取不同的处置与防范措施;

S7、对已识别的攻击行为的url进一步分词以优化所述非法字符特征库。

3.根据权利要求1所述的一种网络安全事件分类与预测方法,其特征在于,步骤S2中所述构建网络攻击非法字符特征库的步骤具体包括:

采集各种攻击行为的web访问日志和全流量http元数据样本;

对所述攻击行为的web访问日志和全流量http元数据样本进行分词;

统计频率大于预设频率的字符;

根据所述字符构建网络攻击非法字符特征库。

4.根据权利要求1所述的一种网络安全事件分类与预测方法,其特征在于,步骤S3具体包括:

统计所述网络攻击非法字符库的非法关键词;

利用one-hot-vector将所述关键词转换成n维向量;

将n维向量的输入层与隐藏层全连接;

通过反向传递得到最终向量并通过与最初词向量相乘得到最终词向量;

将每条url出现的攻击关键词对应的词向量相加以得到文档向量。

5.根据权利要求1所述的一种网络安全事件分类与预测方法,其特征在于,步骤S4具体包括:

统计当前攻击类型的数量;

将所述文档向量作为贝叶斯的特征输入得到类别集合;

统计各类别集合的特征属性的条件概率;

计算每类攻击的后验概率;

将最大后验概率的类别设为当前url的攻击类别。

6.一种网络安全事件分类与预测系统,其特征在于,包括:

获取模块,用于获取全网用户的web访问日志和全流量日志中的http元数据;

匹配模块,用于对所述web访问日志和所述http元数据的url进行分词并与网络攻击非法字符特征库进行匹配;

构建模块,用于将分词后的url利用word2vector构建词向量和文档向量;

分类模块,用于将所述文档向量作为特征输入并采用朴素贝叶斯模型对所述攻击行为进行分类。

7.根据权利要求6所述的一种网络安全事件分类与预测系统,其特征在于,还包括:

识别模块，用于识别不同种类的网络攻击行为；

处理模块，用于对所述各类网络攻击行为采取不同的处置与防范措施；

优化模块，用于对已识别的攻击行为的url进一步分词以优化所述非法字符特征库。

8.根据权利要求6所述的一种网络安全事件分类与预测系统，其特征在于，所述匹配模块具体包括：

采集单元，用于采集各种攻击行为的web访问日志和全流量http元数据样本；

分词单元，用于对所述攻击行为的web访问日志和全流量http元数据样本进行分词；

第一统计单元，用于统计频率大于预设频率的字符；

特征库构建单元，用于根据所述字符构建网络攻击非法字符特征库。

9.根据权利要求6所述的一种网络安全事件分类与预测系统，其特征在于，所述构建模块具体包括：

第二统计单元，用于统计所述网络攻击非法字符库的非法关键词；

转换单元，用于利用one-hot-vector将所述关键词转换成n维向量；

连接单元，用于将n维向量的输入层与隐藏层全连接；

相乘单元，用于通过反向传递得到最终向量并通过与最初词向量相乘得到最终词向量；

相加单元，用于将每条url出现的攻击关键词对应的词向量相加以得到文档向量。

10.根据权利要求6所述的一种网络安全事件分类与预测系统，其特征在于，所述分类模块具体包括：

第三统计单元，用于统计当前攻击类型的数量；

输入单元，用于将所述文档向量作为贝叶斯的特征输入得到类别集合；

第四统计单元，用于统计各类别集合的特征属性的条件概率；

计算单元，用于计算每类攻击的后验概率；

设置单元，用于将最大后验概率的类别设为当前url的攻击类别。

一种网络安全事件分类与预测方法及系统

技术领域

[0001] 本发明涉及计算机网络领域，尤其涉及一种网络安全事件分类与预测方法及系统。

背景技术

[0002] 近年来，随着web应用的不断普及，针对web服务应用的攻击成为网络上广泛传播的攻击方式。由于许多网络应用服务开发者缺乏安全意识，致使网络服务程序中存在大量的安全漏洞，这使得web服务器成为黑客攻击的主要目标之一。

[0003] 互联网上最主要的攻击方式主要有跨站脚本攻击(XSS)、SQL注入攻击(SQL-inject)、远程文件包含(RFI)等给予http协议的网络攻击。为了防御web攻击，各种安全防御技术已被提出并得以应用。主要包括数据加密、安全路由、访问控制、报文鉴别方法的以防范和自我保护为主的被动保护方式，其在其有效防范网络攻击上虽有重要作用，但缺少及时发现攻击行为特征，对攻击进行准确分类的能力。

[0004] 公开号为CN106209826A的专利提供了一种安全事件分析方法，包括如下步骤：根据日志报文中某个关键字，辨别该日志报文是应用日志、系统日志、还是安全日志，将上述日志分成普通事件、异常事件和安全事件，从普通事件的集合中通过异常识别方法寻找出异常事件，从异常事件的集合中通过识别违规操作行为和威胁行为寻找出安全事件。该发明通过识别网络环境中各类设备产生的日志，用事件详细分类解释网络状况，针对所有事件集合，明确地给出了事件的详细分类情况，便于管理人员理解网络中实时发生的事件状态。但是该发明缺少及时发现攻击行为特征，对攻击行为准确分类的能力。

发明内容

[0005] 本发明要解决的技术问题目的在于提供一种网络安全事件分类与预测方法及系统，用以解决现有技术缺少及时发现攻击行为特征，对攻击行为进行准确分类的能力。

[0006] 为了实现上述目的，本发明采用的技术方案为：

[0007] 一种网络安全事件分类与预测方法，包括步骤：

[0008] S1、获取全网用户的web访问日志和全流量日志中的http元数据；

[0009] S2、对所述web访问日志和所述http元数据的url进行分词并与网络攻击非法字符特征库进行匹配；

[0010] S3、将分词后的url利用word2vector构建词向量和文档向量；

[0011] S4、将所述文档向量作为特征输入并采用朴素贝叶斯模型对所述攻击行为进行分类。

[0012] 进一步地，还包括步骤：

[0013] S5、识别不同种类的网络攻击行为；

[0014] S6、对所述各类网络攻击行为采取不同的处置与防范措施；

[0015] S7、对已识别的攻击行为的url进一步分词以优化所述非法字符特征库。

[0016] 进一步地,步骤S2中所述构建网络攻击非法字符特征库的步骤具体包括:

[0017] 采集各种攻击行为的web访问日志和全流量http元数据样本;

[0018] 对所述攻击行为的web访问日志和全流量http元数据样本进行分词;

[0019] 统计频率大于预设频率的字符;

[0020] 根据所述字符构建网络攻击非法字符特征库。

[0021] 进一步地,步骤S3具体包括:

[0022] 统计所述网络攻击非法字符库的非法关键词;

[0023] 利用one-hot-vector将所述关键词转换成n维向量;

[0024] 将n维向量的输入层与隐藏层全连接;

[0025] 通过反向传递得到最终向量并通过与最初词向量相乘得到最终词向量;

[0026] 将每条url出现的攻击关键词对应的词向量相加以得到文档向量。

[0027] 进一步地,步骤S4具体包括:

[0028] 统计当前攻击类型的数量;

[0029] 将所述文档向量作为贝叶斯的特征输入得到类别集合;

[0030] 统计各类别集合的特征属性的条件概率;

[0031] 计算每类攻击的后验概率;

[0032] 将最大后验概率的类别设为当前url的攻击类别。

[0033] 一种网络安全事件分类与预测系统,包括:

[0034] 获取模块,用于获取全网用户的web访问日志和全流量日志中的http元数据;

[0035] 匹配模块,用于对所述web访问日志和所述http元数据的url进行分词并与网络攻击非法字符特征库进行匹配;

[0036] 构建模块,用于将分词后的url利用word2vector构建词向量和文档向量;

[0037] 分类模块,用于将所述文档向量作为特征输入并采用朴素贝叶斯模型对所述攻击行为进行分类。

[0038] 进一步地,还包括:

[0039] 识别模块,用于识别不同种类的网络攻击行为;

[0040] 处理模块,用于对所述各类网络攻击行为采取不同的处置与防范措施;

[0041] 优化模块,用于对已识别的攻击行为的url进一步分词以优化所述非法字符特征库。

[0042] 进一步地,所述匹配模块具体包括:

[0043] 采集单元,用于采集各种攻击行为的web访问日志和全流量http元数据样本;

[0044] 分词单元,用于对所述攻击行为的web访问日志和全流量http元数据样本进行分词;

[0045] 第一统计单元,用于统计频率大于预设频率的字符;

[0046] 特征库构建单元,用于根据所述字符构建网络攻击非法字符特征库。

[0047] 进一步地,所述构建模块具体包括:

[0048] 第二统计单元,用于统计所述网络攻击非法字符库的非法关键词;

[0049] 转换单元,用于利用one-hot-vector将所述关键词转换成n维向量;

[0050] 连接单元,用于将n维向量的输入层与隐藏层全连接;

[0051] 相乘单元，用于通过反向传递得到最终向量并通过与最初词向量相乘得到最终词向量；

[0052] 相加单元，用于将每条url出现的攻击关键词对应的词向量相加以得到文档向量。

[0053] 进一步地，所述分类模块具体包括：

[0054] 第三统计单元，用于统计当前攻击类型的数量；

[0055] 输入单元，用于将所述文档向量作为贝叶斯的特征输入得到类别集合；

[0056] 第四统计单元，用于统计各类别集合的特征属性的条件概率；

[0057] 计算单元，用于计算每类攻击的后验概率；

[0058] 设置单元，用于将最大后验概率的类别设为当前url的攻击类别。

[0059] 本发明与传统的技术相比，有如下优点：

[0060] 本发明实现关键点的实时监测，依靠机器学习发现带有主流攻击特征的异常行为，改善了网络攻击行为分类的效率，降低了人工审核的时间成本，能够适应不断变化的攻击行为，提高了分类检测准确率，为网络安全提供了保障。

附图说明

[0061] 图1是实施例一提供的一种网络安全事件分类与预测方法流程图；

[0062] 图2是实施例二提供的一种网络安全事件分类与预测方法流程图；

[0063] 图3是实施例三提供的一种网络安全事件分类与预测方法流程图；

[0064] 图4是实施例四提供的一种网络安全事件分类与预测方法流程图；

[0065] 图5是实施例五提供的一种网络安全事件分类与预测方法流程图；

[0066] 图6是实施例一至实施例四提供的一种网络安全事件分类与预测系统结构图；

[0067] 图7是实施例五提供的一种网络安全事件分类与预测系统结构图。

具体实施方式

[0068] 以下是本发明的具体实施例并结合附图，对本发明的技术方案作进一步的描述，但本发明并不限于这些实施例。

[0069] 实施例一

[0070] 本实施例提供了一种网络安全事件分类与预测方法，如图1所示，包括步骤：

[0071] S11:获取全网用户的web访问日志和全流量日志中的http元数据；

[0072] S12:对web访问日志和http元数据的url进行分词并与网络攻击非法字符特征库进行匹配；

[0073] S13:将分词后的url利用word2vector构建词向量和文档向量；

[0074] S14:将文档向量作为特征输入并采用朴素贝叶斯模型对攻击行为进行分类。

[0075] 本实施例的分析对象为用户的web访问日志和全局流量日志中的http元数据。通过对数据进行解析、分析后发现，主流网络攻击的关键特征主要体现在url中，由于url通常包含大量的字符，因此需要对web日志和http元数据中的url进行自然语言处理，对其进行分词，提取每一类攻击高频出现的非法字符构建特征库，再利用word2vector构建词向量和文档向量，将文档向量作为特征输入到朴素贝叶斯模型中，对网络攻击行为进行分类。

[0076] 其中，url即统一资源定位符，是对可以从互联网上得到的资源的位置和访问方法

的一种简洁的表示，是互联网上标准资源的地址。互联网上的每个文件都有一个唯一的URL，它包含的信息指出文件的位置和浏览器应该怎么处理它。

[0077] 在因特网的历史上，url的发明是一个非常基础的步骤。url的语法是一般的，可扩展的，它使用ASCII代码的一部分来表示互联网的地址。一般统一资源定位符的开始标志着一个计算机网络所使用的网络协议。

[0078] 统一资源定位符是统一资源标志符的一个下种。统一资源标志符确定一个资源，而统一资源定位符不但确定一个资源，而且还表示出它在哪里。

[0079] 朴素贝叶斯法是基于贝叶斯定理与特征条件独立假设的分类方法。最为广泛的两种分类模型是决策树模型和朴素贝叶斯模型。

[0080] 和决策树模型相比，朴素贝叶斯分类发源于古典数学理论，有着坚实的数学基础，和稳定的分类效率。同时，朴素贝叶斯模型所需的参数很少，对缺失数据不太敏感，算法也比较简单。理论上，朴素贝叶斯模型与其他分类方法相比具有最小的误差率。

[0081] 通过采集用户web访问日志和网络全局流量来实现关键点的实时监控，依靠机器学习发现带有主流攻击特征的异常行为，与现有的安全设备可有效互补，共同维护网络安全。机器学习的应用可从训练数据集中自动提取攻击模式，生成分类模型，有效改善了网络攻击行为分类的效率，降低了人工审核的时间成本，并能够适应不断变化的攻击者的行为，提高了分类检测准确率，为网络安全提供了保障。

[0082] 本实施例还提供了一种网络安全事件分类与预测系统，如图6所示，包括：

[0083] 获取模块61，用于获取全网用户的web访问日志和全流量日志中的http元数据；

[0084] 匹配模块62，用于对web访问日志和http元数据的url进行分词并与网络攻击非法字符特征库进行匹配；

[0085] 构建模块63，用于将分词后的url利用word2vector构建词向量和文档向量；

[0086] 分类模块64，用于将文档向量作为特征输入并采用朴素贝叶斯模型对攻击行为进行分类。

[0087] 具体的，本实施例的分析对象为用户的web访问日志和全局流量日志中的http元数据。获取模块61在获取了全网用户的web访问日志和全流量日志中的http元数据后，通过对数据进行解析、分析后发现，主流网络攻击的关键特征主要体现在url中，由于url通常包含大量的字符，因此需要对web日志和http元数据中的url进行自然语言处理，匹配模块62对其进行分词，提取每一类攻击高频出现的非法字符构建特征库，构建模块63再利用word2vector构建词向量和文档向量，将文档向量作为特征输入到朴素贝叶斯模型中，分类模块64对网络攻击行为进行分类。

[0088] 本实施例提供的系统中，机器学习的应用可从训练数据集中自动提取攻击模式，生成分类模型，有效改善了网络攻击行为分类的效率，降低了人工审核的时间成本，并能够适应不断变化的攻击者的行为，提高了分类检测准确率，为网络安全提供了保障。

[0089] 实施例二

[0090] 本实施例提供了一种网络安全事件分类与预测方法，如图2所示，包括步骤：

[0091] S21：获取全网用户的web访问日志和全流量日志中的http元数据；

[0092] S22：采集各种攻击行为的web访问日志和全流量http元数据样本；

[0093] S23：对攻击行为的web访问日志和全流量http元数据样本进行分词；

[0094] S24:统计频率大于预设频率的字符;

[0095] S25:根据字符构建网络攻击非法字符特征库;

[0096] S26:对web访问日志和http元数据的url进行分词并与网络攻击非法字符特征库进行匹配;

[0097] S27:将分词后的url利用word2vector构建词向量和文档向量;

[0098] S28:将文档向量作为特征输入并采用朴素贝叶斯模型对攻击行为进行分类。

[0099] 与实施例一不同之处在于,步骤S12包括步骤S22～步骤S25。

[0100] 通过对现网web访问日志和http元数据中的url进行分析发现,目前该网络主要存在的攻击有以下几种:

[0101] (1)SQL注入攻击:web应用程序对用户输入数据的合法性没有判断,攻击者可以在web应用程序中事先定义好的查询语句的结尾上添加额外的SQL语句,以此来实现欺骗数据库服务器执行非授权的任意查询,从而进一步得到相应的数据信息。经统计发现,SQL注入攻击的高频非法字符为:select、union、and、or等常用SQL字符。

[0102] (2)XSS(Cross Site Script)跨站脚本攻击:攻击者往web页面里插入恶意html代码,当用户浏览该网页时,嵌入web里面的html代码会被执行,从而达到恶意用户的特殊目的。经统计发现,XSS攻击的高频非法字符为:script、svg、eval、expression等字符。

[0103] (3)OS命令注入:系统提供命令执行类函数处理相关应用场景的功能,而当不合理的使用这类函数并且调用的变量未考虑安全因素时,就会执行恶意的命令调用,被攻击利用。经统计发现,QS命令注入的高频非法字符为:exec、css等字符。

[0104] (4)目录遍历:由于web服务器或web应用程序对用户输入文件名称的安全性验证不足而导致的一种安全漏洞,攻击者通过http请求和利用一些特殊字符就可以绕过服务器的安全限制,访问任意受限的文件甚至执行系统命令。经统计发现,目录遍历的高频非法字符为:../、etc/passwd、svn/entries等字符。

[0105] 表1 主要攻击类型与高频非法字符

[0106]

攻击类型	高频非法字符
SQL 注入攻击	select, union, and, or, hex, unhex, xor, from, insert……
XSS 跨站脚本攻击	script, svg, eval, expression, javascript, alert……
OS 命令注入	exec, css, methodAccessor, Runtime@getRuntime……
目录遍历	../, etc/passwd, svn/entries……
……	……

[0107] 具体的,构建非法字符特征库包括以下步骤:采集各种攻击行为的web日志和全流量http元数据样本,对采集数据的url进行分词,统计出高频出现的字符,从而构建网络攻击非法字符特征库。

[0108] 本实施例还提供了一种网络安全事件分类与预测系统,如图6所示,包括:

[0109] 获取模块61,用于获取全网用户的web访问日志和全流量日志中的http元数据;

[0110] 匹配模块62,用于对web访问日志和http元数据的url进行分词并与网络攻击非法字符特征库进行匹配;

[0111] 构建模块63,用于将分词后的url利用word2vector构建词向量和文档向量;

[0112] 分类模块64,用于将文档向量作为特征输入并采用朴素贝叶斯模型对攻击行为进行分类。

[0113] 与实施例一不同之处在于,匹配模块62具体包括:

[0114] 采集单元,用于采集各种攻击行为的web访问日志和全流量http元数据样本;

[0115] 分词单元,用于对攻击行为的web访问日志和全流量http元数据样本进行分词;

[0116] 第一统计单元,用于统计频率大于预设频率的字符;

[0117] 特征库构建单元,用于根据字符构建网络攻击非法字符特征库;

[0118] 具体的,采集单元采集各种攻击行为的web日志和全流量http元数据样本,分词单元对采集数据的url进行分词,第一统计单元统计出高频出现的字符,特征库构建单元构建网络攻击非法字符特征库。

[0119] 实施例三

[0120] 本实施例提供了一种网络安全事件分类与预测方法,如图3所示,包括步骤:

[0121] S31:获取全网用户的web访问日志和全流量日志中的http元数据;

[0122] S32:对web访问日志和http元数据的url进行分词并与网络攻击非法字符特征库进行匹配;

[0123] S33:统计网络攻击非法字符库的非法关键词;

[0124] S34:利用one-hot-vector将非法关键词转换成n维向量;

[0125] S35:将n维向量的输入层与隐藏层全连接;

[0126] S36:通过反向传递得到最终向量并通过与最初词向量相乘得到最终词向量;

[0127] S37:将每条url出现的攻击关键词对应的词向量相加以得到文档向量;

[0128] S38:将文档向量作为特征输入并采用朴素贝叶斯模型对攻击行为进行分类。

[0129] 与实施例一不同之处在于,步骤S13具体包括步骤S33～步骤S37。

[0130] word2vector于2013年由Google的研究员发布,是一种用于深度学习的词向量生成工具。word2vector本质上是利用了神经网络语言模型并对其进行了简化,既保证了效果又提高了计算复杂度。该模型常用的算法有两种:CBOW和Skip-gram。其中CBOW模型利用词W(t)前后各k个词去预测当前词;而Skip-gram模型恰好相反,它利用词W(t)去预测它前后各k个词,本发明采用Skip-gram模型。以“I think hypercar is expensive”为例,给定“hpyercar”,算法的目的是根据“hypercar”预测前后文中出现“I”,“think”,“is”,“expensive”的概率。Skip-gram的数学表达式:$P(W_i|W_t)$,$t-k\leqslant i\leqslant t+k$。

[0131] 在训练该模型之前,首先需要将非法特征库中的词进行量化转换为词向量。特征词库中非法字符的个数就是向量的维度,利用one-hot-vector赋予每一个词一个编码,该词所在的位置标记为“1”,其他位置标记为“0”。如“select”的词向量为[0,0,0,0,1...,0,0],“script”的词向量为[0,1,0,0,0...,0,0]。

[0132] word2vector是具有一个隐含层的神经元网络(如下图)。它的输入和输出都是词向量,在训练的神经元网络收敛之后,将从输入层到隐含层的权重赋给每个词向量,因此每

个词能得到具有语义意义的新的向量。

[0133] 本实施例的具体实现过程为：

[0134] 步骤S33对非法字符特征库中的攻击关键词进行统计，假设有有m个攻击关键词；

[0135] 步骤S34：先利用one-hot-vector将一个词转换成一个n维的向量x，以“select”为例：

[0136] "select"→[0,0,0,0,1...,0,0]

[0137] 步骤S34：隐藏层中有m个神经元，已知输入层是一个n维向量且与隐藏层全连接，所以需要一个n*m的权重矩阵w把n维的向量映射到纬度为1*m的隐藏神经元中；

[0138] $$w=\begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1m} \\ w_{21} & w_{21} & \cdots & w_{3m} \\ \cdots & \cdots & \cdots & \cdots \\ w_{n1} & w_{n1} & \cdots & w_{nm} \end{bmatrix}$$

[0139] 步骤S35：从隐藏层到输出层同样利用全连接，在计算输出单元的时候加入softmax分类器，通过反向传递可以求得最终的向量w；

[0140] 步骤S36：通过与最初的词向量相乘即x*w可以求得最终的词向量，也就是1*m的向量W(i)；

[0141] $x*w=W(i)=[W_{i1}\ W_{i2}\ \cdots\ W_{im}]$

[0142] 步骤S36：将每一条url出现的攻击关键词对应的词向量进行相加，得到属于该条url的文档向量d。

[0143] 本实施例还提供了一种网络安全事件分类与预测系统，如图6所示，包括：

[0144] 获取模块61，用于获取全网用户的web访问日志和全流量日志中的http元数据；

[0145] 匹配模块62，用于对web访问日志和http元数据的url进行分词并与网络攻击非法字符特征库进行匹配；

[0146] 构建模块63，用于将分词后的url利用word2vector构建词向量和文档向量；

[0147] 分类模块64，用于将文档向量作为特征输入并采用朴素贝叶斯模型对攻击行为进行分类。

[0148] 与实施例一不同之处在于，构建模块63具体包括：

[0149] 第二统计单元，用于统计网络攻击非法字符库的非法关键词；

[0150] 转换单元，用于利用one-hot-vector将非法关键词转换成n维向量；

[0151] 连接单元，用于将n维向量的输入层与隐藏层全连接；

[0152] 相乘单元，用于通过反向传递得到最终向量并通过与最初词向量相乘得到最终词向量；

[0153] 相加单元，用于将每条url出现的攻击关键词对应的词向量相加以得到文档向量。

[0154] 实施例四

[0155] 本实施例提供了一种网络安全事件分类与预测方法，如图4所示，包括步骤：

[0156] S41：获取全网用户的web访问日志和全流量日志中的http元数据；

[0157] S42：对web访问日志和http元数据的url进行分词并与网络攻击非法字符特征库进行匹配；

[0158] S43：将分词后的url利用word2vector构建词向量和文档向量；

[0159] S44：统计当前攻击类型的数量；

[0160] S45:将文档向量作为贝叶斯的特征输入得到类别集合;

[0161] S46:统计各类别集合的特征属性的条件概率;

[0162] S47:计算每类攻击的后延概率;

[0163] S48:将最大后验概率的类别设为当前url的攻击类别。

[0164] 与实施例一不同之处在于,步骤S14包括步骤S44～步骤S48。

[0165] 朴素贝叶斯分类器为贝叶斯分类的一种,其基于统计学原理,通过事件的先验概率,来获得事件可能所属每类的后验概率,选最大后验概率的对应类作为该事件的所属类。贝叶斯定理的公式为:

[0166] $$P(A|B)=\frac{P(B|A)P(A)}{P(B)}$$

[0167] P(A|B)表示事件B已经发生的前提下,事件A发生的概率,叫做事件B发生下事件A的条件概率。其基本求解公式为:

[0168] $$P(A|B)=\frac{P(AB)}{P(B)}$$

[0169] P(A)是A的先验概率或边缘概率。之所以称为"先验"是因为它不考虑任何B方面的因素;

[0170] P(B|A)是已知A发生后B的条件概率,也由于得自A的取值而被称作B的后验概率;

[0171] P(B)是B的先验概率或边缘概率,也作标准化常量。

[0172] 朴素贝叶斯在网络安全攻击行为分类中的应用过程如下:

[0173] 步骤S44:已知当前数据集中存在z种攻击类型;

[0174] 步骤S45:设d=$\{a_1,a_2,a_3,\cdots,a_m\}$为一个待分类项,而每个a为d的一个特征属性。其中d是由上述特征库中的非法关键词通过word2vector转换生成的关键词向量通过相加得到的文档向量;

[0175] 已知有z种攻击类别,类别集合

[0176] C=$\{y_1,y_2,y_3,\cdots,y_z\}$;

[0177] 步骤S46:统计得到在各类别下各个特征属性的条件概率,即

[0178] $P(a_1|y_1)$,$P(a_2|y_1)$,$\cdots P(a_m|y_1)$;$P(a_1|y_2)$,$P(a_2|y_2)$,$\cdots P(a_m|y2)$,$\cdots$,$P(a_1|y_z)$,$P(a_2|y_z)$,$\cdots P(a_m|y_z$

[0179] 步骤S47:假设各个特征属性是条件独立的,则根据贝叶斯定理有如下推导:

[0180] $$P(y_i|d)=\frac{P(d|y_i)P(y_i)}{P(d)}$$

[0181] 因为分母对于所有类别为常数,因为我们只要将分子最大化皆可,又因为各特征属性是条件独立的,所以有:

[0182] $$P(d|y_i)P(y_i)=P(a_1|y_i)P(a_2|y_i)\cdots P(a_m|y_i)P(y_i)=P(y_i)\prod_{j=1}^{m}P(a_j|y_i)$$

[0183] 分别计算$P(y_1|d)$,$P(y_2|d)$,$\cdots P(y_z|d)$;

[0184] 如果$P(y_j|d)=\max\{P(y_1|d),P(y_2|d)\cdots P(y_z|d)\}$,则d对应的分类是$y_j$;

[0185] 步骤S48:根据得到的最大后验概率的得到每一条url对应的攻击类别。

[0186] 本实施例还提供了一种网络安全事件分类与预测系统，如图6所示，包括：

[0187] 获取模块61，用于获取全网用户的web访问日志和全流量日志中的http元数据；

[0188] 匹配模块62，用于对web访问日志和http元数据的url进行分词并与网络攻击非法字符特征库进行匹配；

[0189] 构建模块63，用于将分词后的url利用word2vector构建词向量和文档向量；

[0190] 分类模块64，用于将文档向量作为特征输入并采用朴素贝叶斯模型对攻击行为进行分类。

[0191] 与实施例一不同之处在于，分类模块64具体包括：

[0192] 第三统计单元，用于统计当前攻击类型的数量；

[0193] 输入单元，用于将文档向量作为贝叶斯的特征输入得到类别集合；

[0194] 第四统计单元，用于统计各类别集合的特征属性的条件概率；

[0195] 计算单元，用于计算每类攻击的后延概率；

[0196] 设置单元，用于将最大后验概率的类别设为当前url的攻击类别。

[0197] 实施例五

[0198] 本实施例提供了一种网络安全事件分类与预测方法，如图5所示，包括步骤：

[0199] S51：获取全网用户的web访问日志和全流量日志中的http元数据；

[0200] S52：对web访问日志和http元数据的url进行分词并与网络攻击非法字符特征库进行匹配；

[0201] S53：将分词后的url利用word2vector构建词向量和文档向量；

[0202] S54：将文档向量作为特征输入并采用朴素贝叶斯模型对攻击行为进行分类；

[0203] S55：识别不同种类的网络攻击行为；

[0204] S56：对各类网络攻击行为采集不同的处置与防范措施；

[0205] S57：对已识别的攻击行为的url进一步分词以优化非法字符特征库。

[0206] 本实施例与实施例一不同之处在于，还包括步骤S15～步骤S17。

[0207] 在朴素贝叶斯分类器进行分类后，将预测为各位攻击的url进一步分析，提取出现频率高但未在特征库内的非法字符，完善数据库。

[0208] 具体的，在对现网用户访问数据进行分析后发现，目前网站中占比最高的攻击类型为SQL注入攻击与XSS跨站脚本攻击，当贝叶斯分类器对某类攻击的判断结果大于事先设定的阈值Y时，应立即采取有效的措施进行封堵与防控。对于模型判断的攻击类型可采取如下应对措施：

[0209] (1)事前预测：当贝叶斯分类器对某类攻击的判断结果小于事先设定的阈值时，对攻击者IP进行监控并且对疑似被攻击网站进行漏洞扫描，及时采取安全防护措施，避免网站遭受攻击。

[0210] (2)事中防护：当贝叶斯分类器对某类攻击的判断结果大于事先设定的阈值时，及时部署专业的防御设备、入侵防御产品，避免网站攻击行为的扩散与恶化。

[0211] (3)事后取证与分析：包括对攻击事件进行还原、对安全设备检测结果进行验证、对常见攻击行为进行深度分析三个方面。

[0212] 1)对攻击事件进行还原。根据模型输出的攻击者IP、攻击时间、攻击类型、URL关键字符等信息匹配原始日志，提取对应的攻击特征包括但不限于：攻击时间、攻击者IP，被攻

击者IP、url长度、url关键字符、请求方式等，对攻击事件进行溯源与还原并构建攻击黑名单库，便于了解当前的网络安全态势与脆弱性风险。

[0213] 2)对安全设备检测结果进行验证。将模型分析的结果与WAF等网络安全设备检测结果进行对比分析，若两者的分析、检测结果一致则可确认攻击事件的发生并进行针对性的措施，若结果不一致则可对攻击者IP进行监控与观察，避免误判，对于绕过安全设备的检测但被模型分析发现的攻击事件应提高警惕，重点观察常见攻击事件的行为是否存在变异与更新。

[0214] 3)对攻击行为进行深度分析。定期对黑名单库中的攻击行为进行分析，挖掘攻击行为之间的相关性。对于同一大类的攻击进一步分析细分的可能性，如SQL注入可细分为布尔型注入、报错型注入、可联合查询注入、可多语句查询注入等类型，攻击行为的深度分析可以为安全人员分析攻击手法并进行精准的处置提供全面的信息。

[0215] 本实施例还提供了一种网络安全事件分类与预测系统，如图7所示，包括：

[0216] 获取模块71，用于获取全网用户的web访问日志和全流量日志中的http元数据；

[0217] 匹配模块72，用于对web访问日志和http元数据的url进行分词并与网络攻击非法字符特征库进行匹配；

[0218] 构建模块73，用于将分词后的url利用word2vector构建词向量和文档向量；

[0219] 分类模块74，用于将文档向量作为特征输入并采用朴素贝叶斯模型对攻击行为进行分类；

[0220] 识别模块75，用于识别不同种类的网络攻击行为；

[0221] 处理模块76，用于对各类网络攻击行为采集不同的处置与防范措施；

[0222] 优化模块77，用于识别的攻击行为的url进一步分词以优化非法字符特征库。

[0223] 与实施例一不同之处在于，还包括识别模块75，处理模块76及优化模块77。

[0224] 具体的，在对现网用户访问数据进行分析后发现，目前网站中占比最高的攻击类型为SQL注入攻击与XSS跨站脚本攻击，当贝叶斯分类器对某类攻击的判断结果大于事先设定的阈值Y时，应立即采取有效的措施进行封堵与防控。

[0225] 将预测为各类攻击的url进行进一步分析，提取出现频率高但未在特征库内的非法字符，完善数据库。不断更新非法字符特征库，通过机器学习，能够避免因网络攻击的升级导致不能及时发现并处理的问题。

[0226] 本文中所描述的具体实施例仅仅是对本发明精神作举例说明。本发明所属技术领域的技术人员可以对所描述的具体实施例做各种各样的修改或补充或采用类似的方式替代，但并不会偏离本发明的精神或者超越所附权利要求书所定义的范围。

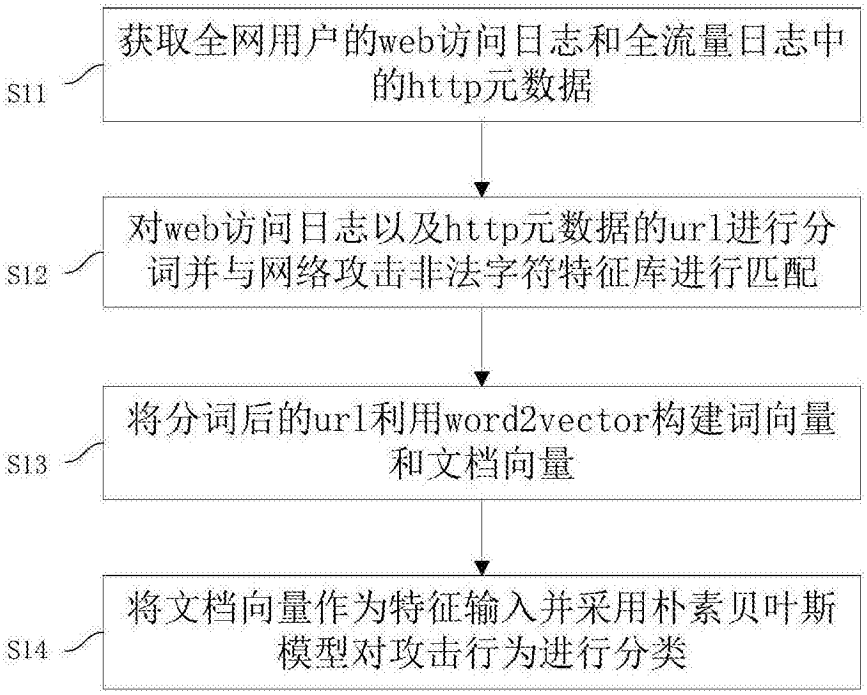

S11
获取全网用户的web访问日志和全流量日志中的http元数据
S12
对web访问日志以及http元数据的url进行分词并与网络攻击非法字符特征库进行匹配
S13
将分词后的url利用word2vector构建词向量和文档向量
S14
将文档向量作为特征输入并采用朴素贝叶斯模型对攻击行为进行分类

图1

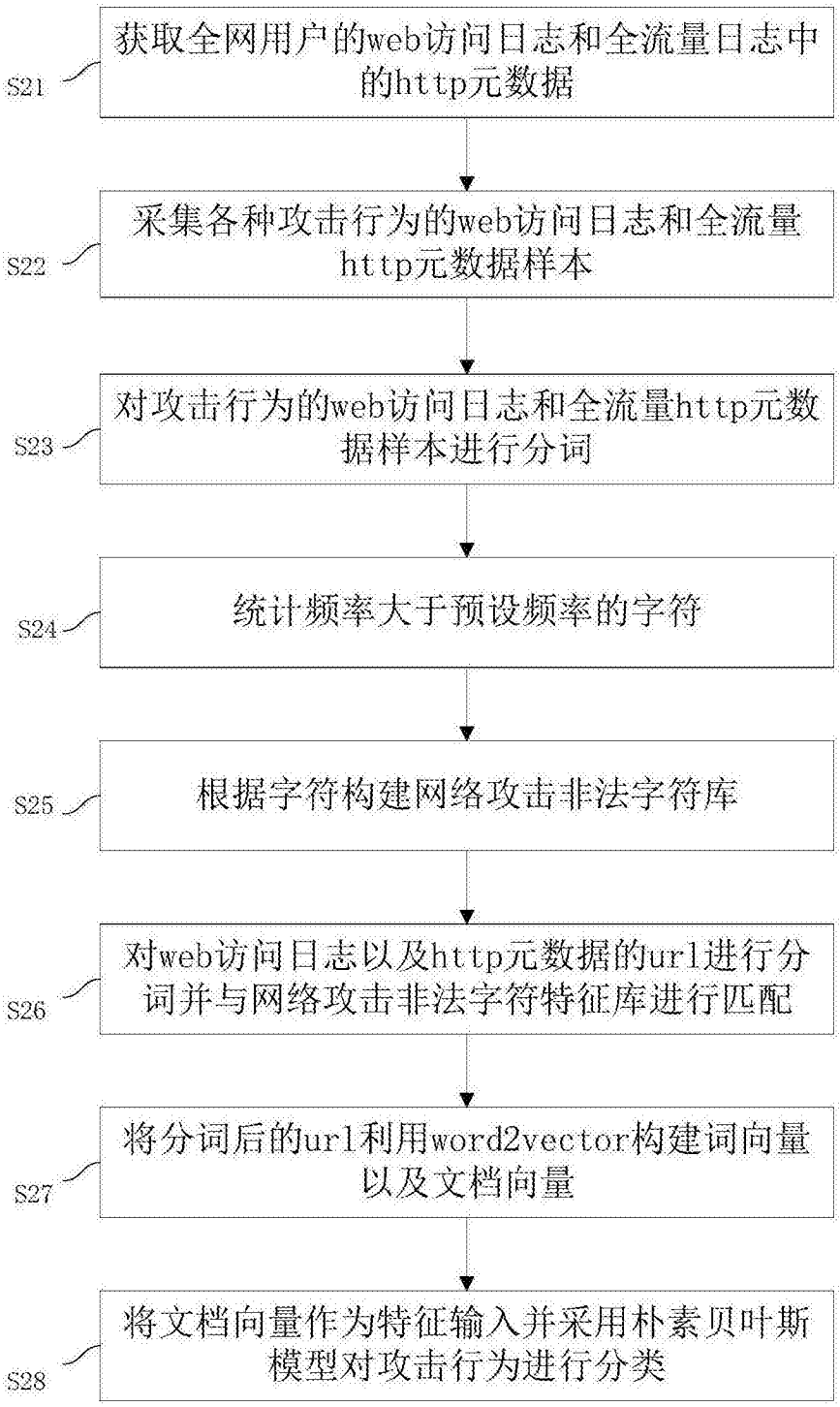

S21
获取全网用户的web访问日志和全流量日志中的http元数据
S22
采集各种攻击行为的web访问日志和全流量http元数据样本
S23
对攻击行为的web访问日志和全流量http元数据样本进行分词
S24
统计频率大于预设频率的字符
S25
根据字符构建网络攻击非法字符库
S26
对web访问日志以及http元数据的url进行分词并与网络攻击非法字符特征库进行匹配
S27
将分词后的url利用word2vector构建词向量以及文档向量
S28
将文档向量作为特征输入并采用朴素贝叶斯模型对攻击行为进行分类

图2

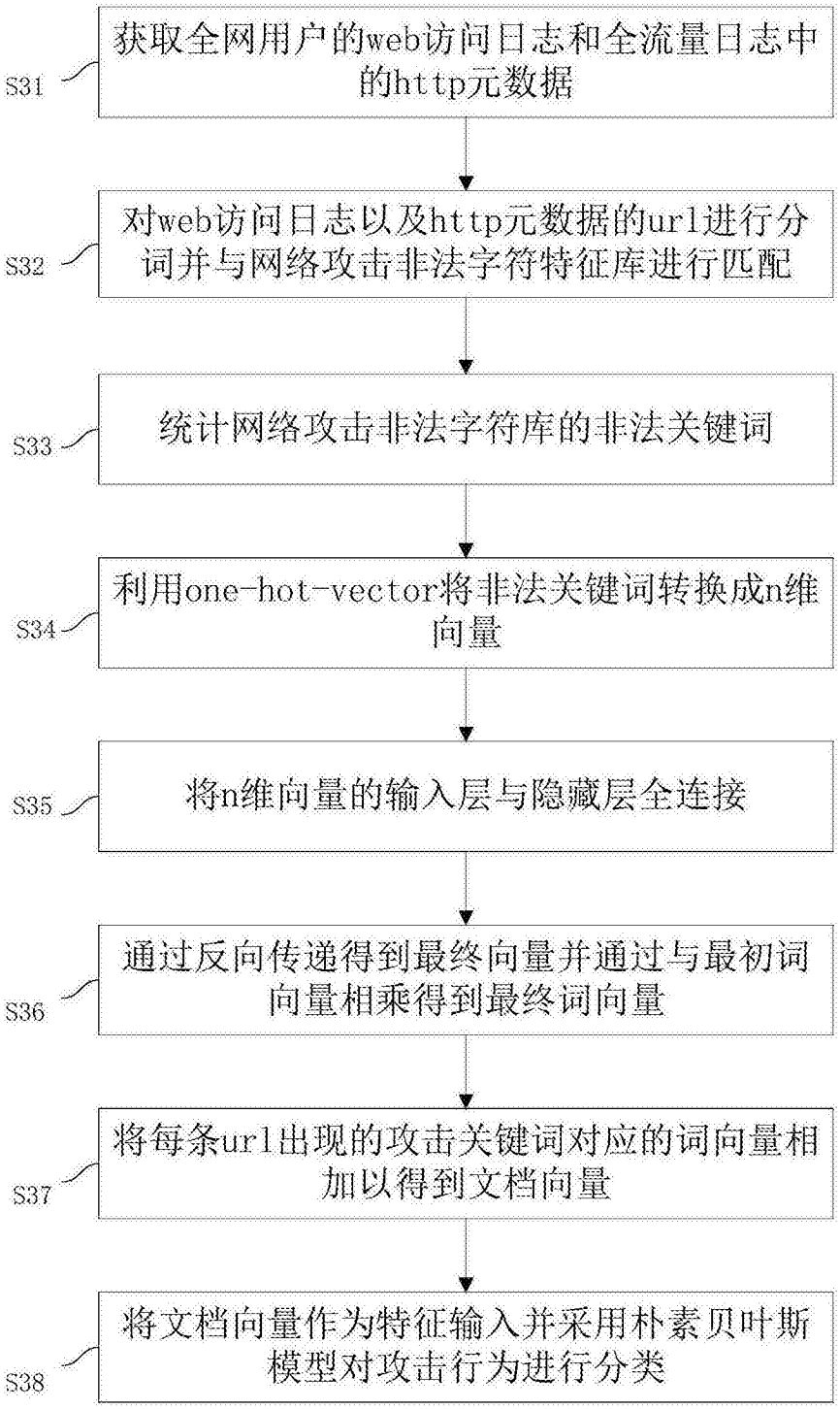

S31
获取全网用户的web访问日志和全流量日志中的http元数据
S32
对web访问日志以及http元数据的url进行分词并与网络攻击非法字符特征库进行匹配
S33
统计网络攻击非法字符库的非法关键词
S34
利用one-hot-vector将非法关键词转换成n维向量
S35
将n维向量的输入层与隐藏层全连接
S36
通过反向传递得到最终向量并通过与最初词向量相乘得到最终词向量
S37
将每条url出现的攻击关键词对应的词向量相加以得到文档向量
S38
将文档向量作为特征输入并采用朴素贝叶斯模型对攻击行为进行分类

图3

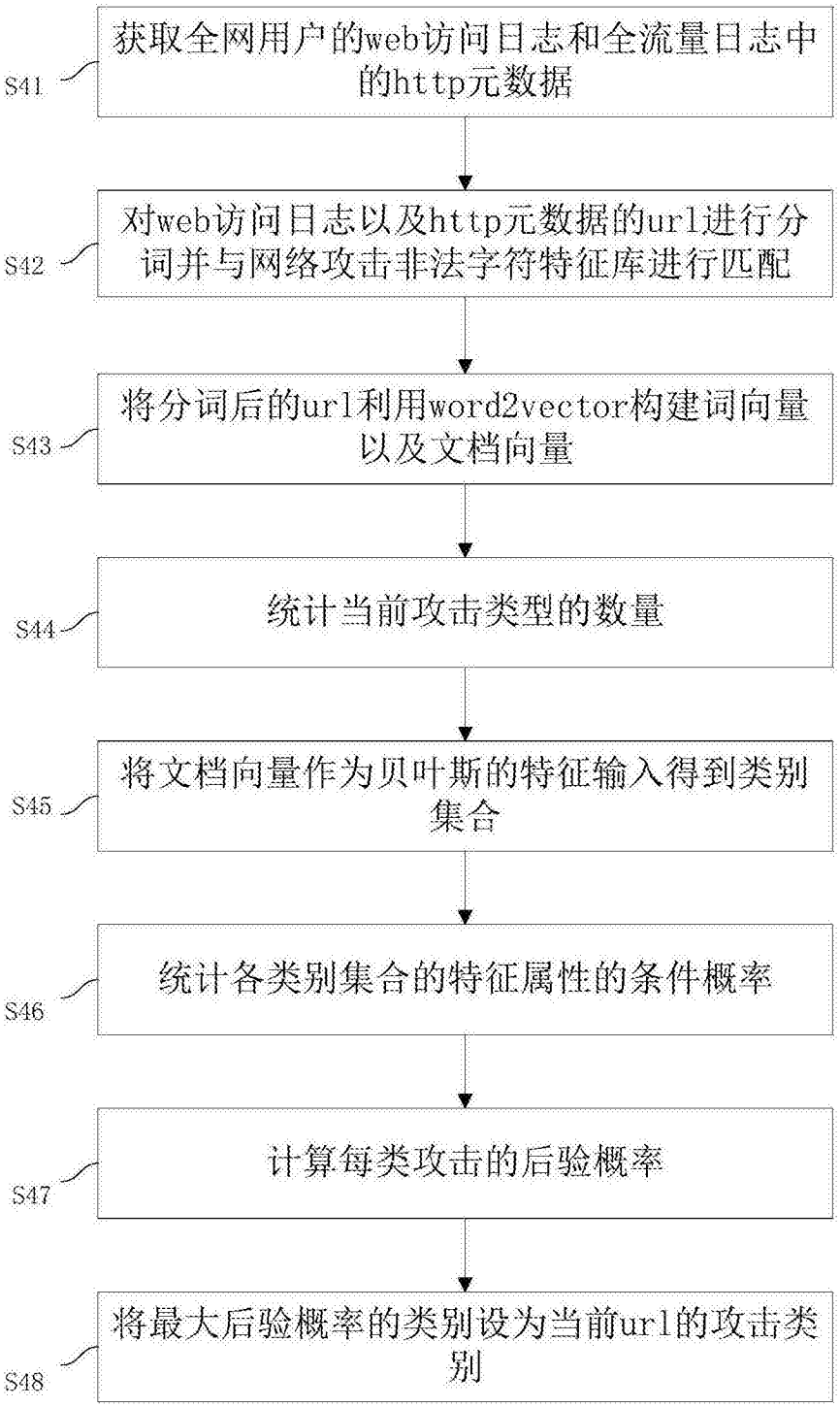

S41
获取全网用户的web访问日志和全流量日志中的http元数据
S42
对web访问日志以及http元数据的url进行分词并与网络攻击非法字符特征库进行匹配
S43
将分词后的url利用word2vector构建词向量以及文档向量
S44
统计当前攻击类型的数量
S45
将文档向量作为贝叶斯的特征输入得到类别集合
S46
统计各类别集合的特征属性的条件概率
S47
计算每类攻击的后验概率
S48
将最大后验概率的类别设为当前url的攻击类别

图4

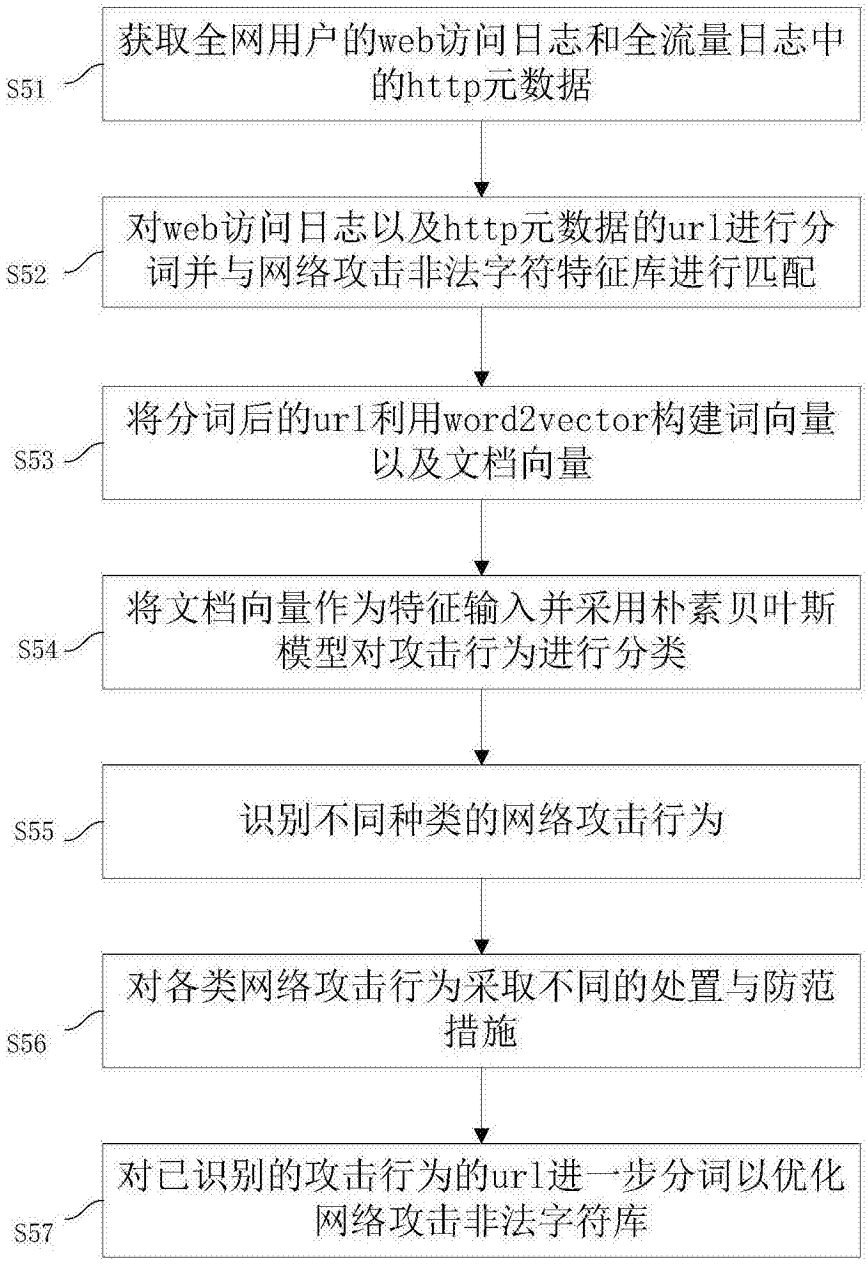

S51
获取全网用户的web访问日志和全流量日志中的http元数据
S52
对web访问日志以及http元数据的url进行分词并与网络攻击非法字符特征库进行匹配
S53
将分词后的url利用word2vector构建词向量以及文档向量
S54
将文档向量作为特征输入并采用朴素贝叶斯模型对攻击行为进行分类
S55
识别不同种类的网络攻击行为
S56
对各类网络攻击行为采取不同的处置与防范措施
S57
对已识别的攻击行为的url进一步分词以优化网络攻击非法字符库

图5

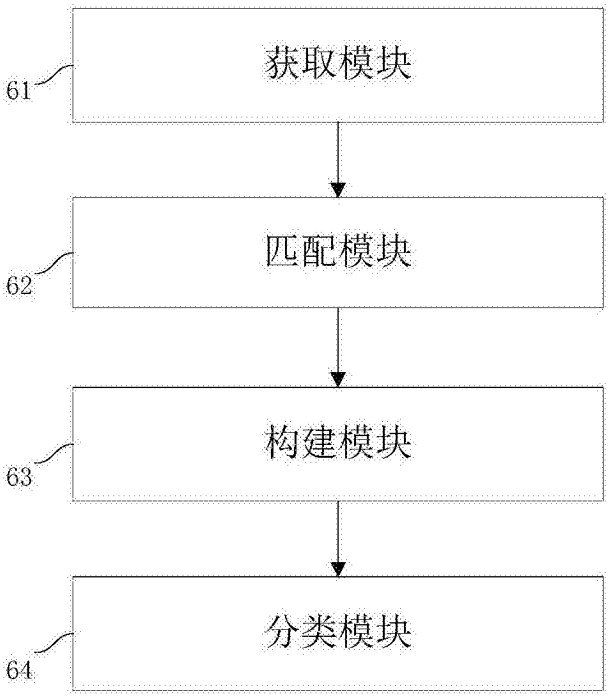


图6

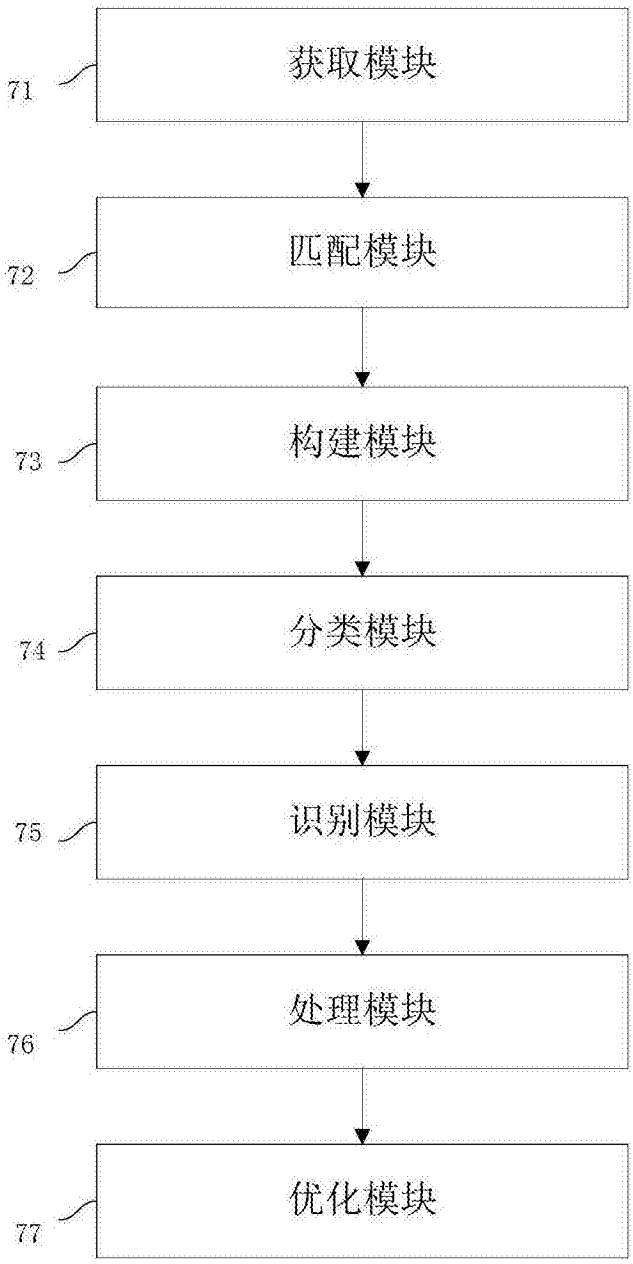


图7