(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111159588 B
(45)授权公告日 2022.12.13

(21)申请号 201911314312.9
(22)申请日 2019.12.19
(65)同一申请的已公布的文献号
申请公布号 CN 111159588 A
(43)申请公布日 2020.05.15
(73)专利权人 电子科技大学
地址 610000 四川省成都市高新区(西区)西源大道2006号
专利权人 赛尔网络有限公司
(72)发明人 刘瑶 鲁俊良 李佳洲 娄云 秦臻
(74)专利代理机构 成都正德明志知识产权代理有限公司 51360
专利代理师 陈瑶
(51)Int.Cl.
G06F 16/955(2019.01)
G06N 3/04(2006.01)
(56)对比文件
CN 101211341 A,2008.07.02
CN 103685308 A,2014.03.26
CN 103685307 A,2014.03.26
EP 3416068 A2,2018.12.19
CN 109450845 A,2019.03.08
US 2015172311 A1,2015.06.18
CN 109101552 A,2018.12.28
张慧等.基于CNN和多分类器的恶意URLs检测.《计算机工程与设计》.2019,第40卷(第10期),2991-2995+30.
Le Hung等.urlnet:learning a url representation with deep learning for malicious url detection.《arXiv preprint arXiv》.2018,1-13.
审查员 沈婷婷

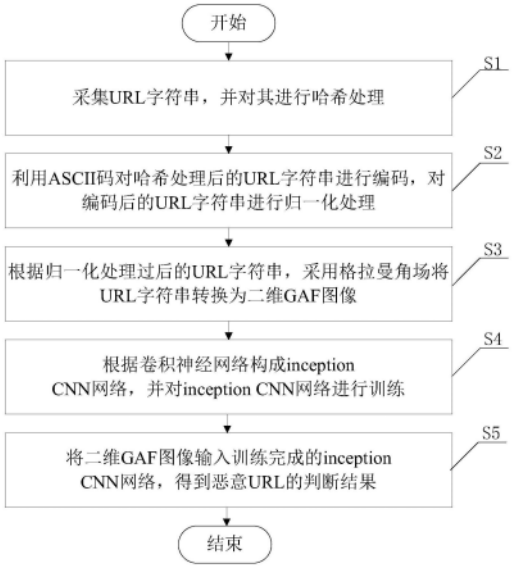
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种基于URL成像技术的恶意URL检测方法

(57)摘要

本发明公开了一种基于URL成像技术的恶意URL检测方法,包括以下步骤:采集URL字符串,并对其进行哈希处理;利用ASCII码对哈希处理后的URL字符串进行编码,对编码后的URL字符串进行归一化处理;根据归一化处理过后的URL字符串,采用格拉曼角场将URL字符串转换为二维图像;根据卷积神经网络构成inception CNN网络,并对其进行训练;将二维图像输入训练完成的inception CNN网络,得到恶意URL的判断结果。本发明通过将URL转换为二维图像,能够准确的识别恶意URL。



CN 111159588 B

1.一种基于URL成像技术的恶意URL检测方法,其特征在于,包括以下步骤:

S1、采集URL字符串,并对其进行哈希处理;

S2、利用ASCII码对哈希处理后的URL字符串进行编码,对编码后的URL字符串进行归一化处理;

S3、根据归一化处理过后的URL字符串,采用格拉曼角场将URL字符串转换为二维GAF图像;

S4、根据卷积神经网络构成inception CNN网络,并对inception CNN网络进行训练;

S5、将二维GAF图像输入训练完成的inception CNN网络,得到恶意URL的判断结果;

所述步骤S3包括以下分步骤:

S3.1、根据归一化处理过后的URL字符串,将其笛卡尔坐标系转变为极坐标系;

S3.2、将极坐标系的数据分别放入格拉曼角差场和格拉曼角和场中,得到新的一维数据;

S3.3、将新的一维数据按照URL字符顺序对应排布,得到二维GAF图像;

所述步骤S4中的inception CNN网络包括输入层,所述输入层分别与第一卷积层的输入端、第二卷积层的输入端、第三池化层的输入端和第四卷积层的输入端连接;

所述第一卷积层的输出端通过第一池化层和第一展平层与拼接层的输入端连接,所述第二卷积层的输出端通过第二池化层和第二展平层与拼接层的输入端连接,所述第三池化层的输出端通过第三卷积层和第三展平层与拼接层的输入端连接,所述第四卷积层的输出端与拼接层的输入端连接;

所述拼接层的输出端通过依次连接的第一连接层、失活层、第二全连接层、第三全连接层和sigmoid激活层与输出层连接。

2.根据权利要求1所述的一种基于URL成像技术的恶意URL检测方法,其特征在于,所述步骤S1中采集的URL字符串为$\vec{d}=[d_1,d_2,...,d_i,...,d_n]$,所述$d_i$表示URL的字符,i=1,2,...,n,n表示URL的长度。

3.根据权利要求2所述的一种基于URL成像技术的恶意URL检测方法,其特征在于,所述步骤S2中利用ASCII码对URL字符串进行编码的具体方法为:通过ASCII码对URL字符串进行编码,得到ASCII字符串;所述ASCII字符串为$A(\vec{d})=[A(d_1),A(d_2),...,A(d_i),...,A(d_n)]$,$A(d_i)$表示URL的字符$d_i$的ASCII码;

所述步骤S2中对编码后的URL字符串进行归一化处理的公式如下:

$$A^*(d_i)=\frac{A(d_i)-\min A(d_i)}{\max A(d_i)-\min A(d_i)}$$

所述编码后的URL字符串进行归一化处理后,得到归一化字符串为

$$A^*(\vec{d})=[A^*(d_1),A^*(d_2),...,A^*(d_i),...,A^*(d_n)];$$

其中,$A^*(d_i)$表示归一化处理过后的$A(d_i)$,$\min A(d_i)$表示$A(d_i)$中最小的值,$\max A(d_i)$表示$A(d_i)$中最大的值。

4.根据权利要求1所述的一种基于URL成像技术的恶意URL检测方法,其特征在于,所述

步骤S3.1包括以下分步骤：

S3.1.1、根据归一化后的字符串$A^*(d_i)$，获取距离r和反余弦ϕ，具体计算公式如下：

$$\begin{cases} r=\dfrac{t_i}{N} & t_i \in N \\ \phi=\arccos(A^*(d_i)) & -1 \le A^*(d_i) \le 1 \end{cases}$$

S3.1.2、根据距离r和反余弦ϕ，将归一化后的字符串$A^*(d_i)$用极坐标表示；

其中，r表示URL字符用极坐标表示时的点到原点的距离，t_i表示时间步长，N表示正则化极坐标系统扩张成空间的常数因子。

5.根据权利要求1所述的一种基于URL成像技术的恶意URL检测方法，其特征在于，所述步骤S3.2中格拉曼角差场GADF为：

$$GADF=\sqrt{I-\overline{X}^2}^{'}\bullet\overline{X}-\overline{X}^{'}\bullet\sqrt{I-\overline{X}^2}$$

所述步骤S3.2中格拉曼角和场GASF为：

$$GASF=\overline{X}^{'}\bullet\overline{X}-\sqrt{I-\overline{X}^2}^{'}\bullet\sqrt{I-\overline{X}^2}$$

其中，$\overline{X}$表示使用极坐标表示的URL字符串，I表示单位行向量，$\overline{X}^{'}$表示$\overline{X}$的导数，$\sqrt{I-\overline{X}^2}^{'}$表示$\sqrt{I-\overline{X}^2}$的导数。

6.根据权利要求1所述的一种基于URL成像技术的恶意URL检测方法，其特征在于，所述步骤S4中对inception CNN网络进行训练的具体方法为：

A1、根据步骤S1至步骤S3，生成正负样本比例为1.5:1的若干训练数据；

A2、将训练数据中正样本和负样本各随机抽取百分之十作为验证数据集，随机初始化inception CNN网络；

A3、将训练数据批大小分别设置为32、64和128，并将其输入inception CNN网络；

A4、将二元交叉熵函数作为损失函数，以损失值最小为目标，使用Sigmoid算法对神经网络的参数进行优化，并使用梯度下降法对神经网络进行参数更新；

A5、利用验证数据集对损失值进行验证，当损失值不再减小，此时的网络参数保存为最终参数，得到训练完成的inception CNN网络。

一种基于URL成像技术的恶意URL检测方法

技术领域

[0001] 本发明属于URL识别领域,具体涉及一种基于URL成像技术的恶意URL检测方法。

背景技术

[0002] 信息技术的普及极大促进了在线银行、电子商务和社交网络的发展,人们越来越多地通过互联网完成社交、购物、资讯获取等行为,政府也在通过互联网推行电子政务,增强政府的透明性,改进公共决策质量。但同时,互联网也成为不法分子的活跃平台,涌现出大量的网络犯罪行为。网络攻击者通过钓鱼网站、垃圾广告和恶意软件推广等方式非法牟利。在这些攻击行为中,有相当大的一部分是以恶意URL为主要手段实现的。URL即统一资源定位符,是对互联网上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。而恶意URL是指欺骗用户访问,达到“执行恶意行为”或“非法窃取用户数据”目的URL。攻击者通过恶意URL构建攻击操作,诱导不知情的用户访问攻击者提供的URL,达到其窃取用户的个人隐私信息目的,例如用户的银行帐号及密码信息,或者下载和执行恶意程序或脚本。因此,及时精确地检测恶意URL,从而有效应对大量多类型的网络安全攻击,是构建网络安全解决方案中的重要一环。但现有恶意URL检测的深度学习模型中存在三个基本问题:(1)无法有效地捕获语义或顺序模式:现有的方法依赖于使用单词包特性,但它们不能有效地捕捉单词或字符出现在URL字符串中的顺序;(2)无法处理不可见的特征:在预测过程中,测试URL很可能包含训练数据中不存在的新单词。在这种情况下,经过训练的模型无法从这些单词中提取关于URL的任何有用信息。(3)URL中唯一的单词数量可能非常大,这在训练模型时造成了严重的内存限制。

发明内容

[0003] 针对现有技术中的上述不足,本发明提供的一种基于URL成像技术的恶意URL检测方法解决了现有恶意URL检测存在的问题。

[0004] 为了达到上述发明目的,本发明采用的技术方案为:一种基于URL成像技术的恶意URL检测方法,包括以下步骤:

[0005] S1、采集URL字符串,并对其进行哈希处理;

[0006] S2、利用ASCII码对哈希处理后的URL字符串进行编码,对编码后的URL字符串进行归一化处理;

[0007] S3、根据归一化处理过后的URL字符串,采用格拉曼角场将URL字符串转换为二维GAF图像;

[0008] S4、根据卷积神经网络构成inception CNN网络,并对inception CNN网络进行训练;

[0009] S5、将二维GAF图像输入训练完成的inception CNN网络,得到恶意URL的判断结果。

[0010] 进一步地,所述步骤S1中采集的URL字符串为$\vec{d}=[d_1,d_2,...,d_i,...,d_n]$,所述$d_i$表示

URL的字符，i＝1,2,...,n,n表示URL的长度。

[0011] 进一步地，所述步骤S2中利用ASCII码对URL字符串进行编码的具体方法为：通过ASCII码对URL字符串进行编码，得到ASCII字符串；所述ASCII字符串为

$\vec{A(d)}=[A(d_1),A(d_2),...,A(d_i),...,A(d_n)]$，$A(d_i)$表示URL的字符$d_i$的ASCII码；

[0012] 所述步骤S2中对编码后的URL字符串进行归一化处理的公式如下：

[0013] $$A^*(d_i)=\frac{A(d_i)-\min A(d_i)}{\max A(d_i)-\min A(d_i)}$$

[0014] 所述编码后的URL字符串进行归一化处理后，得到归一化字符串为

[0015] $$\vec{A^*(d)}=[A^*(d_1),A^*(d_2),...,A^*(d_i),...,A^*(d_n)];$$

[0016] 其中，$A^*(d_i)$表示归一化处理过后的$A(d_i)$，$\min A(d_i)$表示$A(d_i)$中最小的值，$\max A(d_i)$表示$A(d_i)$中最大的值。

[0017] 进一步地，所述步骤S3包括以下分步骤：

[0018] S3.1、根据归一化处理过后的URL字符串，将其笛卡尔坐标系转变为极坐标系；

[0019] S3.2、将极坐标系的数据分别放入格拉曼角差场和格拉曼角和场中，得到新的一维数据；

[0020] S3.3、将新的一维数据按照URL字符顺序对应排布，得到二维GAF图像。

[0021] 进一步地，所述步骤S3.1包括以下分步骤：

[0022] S3.1.1、根据归一化后的字符串$A^*(d_i)$，获取距离r和反余弦φ，具体计算公式如下：

[0023] $$\begin{cases} r=\frac{t_i}{N} & t_i \in N \\ \phi=\arccos(A^*(d_i)) & -1 \le A^*(d_i) \le 1 \end{cases}$$

[0024] S3.1.2、根据距离r和反余弦φ，将归一化后的字符串$A^*(d_i)$用极坐标表示；

[0025] 其中，r表示URL字符用极坐标表示时的点到原点的距离，t_i表示时间步长，N表示正则化极坐标系统扩张成空间的常数因子。

[0026] 进一步地，所述步骤S3.2中格拉曼角差场GADF为：

[0027] $$GADF=\sqrt{I-\overline{X}^2}'\cdot\overline{X}-\overline{X}'\cdot\sqrt{I-\overline{X}^2}$$

[0028] 所述步骤S3.2中格拉曼角和场GASF为：

[0029] $$GASF=\overline{X}'\cdot\overline{X}-\sqrt{I-\overline{X}^2}'\cdot\sqrt{I-\overline{X}^2}$$

[0030] 其中，$\overline{X}$表示使用极坐标表示的URL字符串，I表示单位行向量，$\overline{X}'$表示$\overline{X}$的导数，$\sqrt{I-\overline{X}^2}'$表示$\sqrt{I-\overline{X}^2}$的导数。

[0031] 进一步地，所述步骤S4中的inception CNN网络包括输入层，所述输入层分别与第一卷积层的输入端、第二卷积层的输入端、第三池化层的输入端和第四卷积层的输入端连接；

[0032] 所述第一卷积层的输出端通过第一池化层和第一展平层与拼接层的输入端连接，所述第二卷积层的输出端通过第二池化层和第二展平层与拼接层的输入端连接，所述第三池化层的输出端通过第三卷积层和第三展平层与拼接层的输入端连接，所述第四卷积层的输出端与拼接层的输入端连接；

[0033] 所述拼接层的输出端通过依次连接的第一连接层、失活层、第二全连接层、第三全连接层和sigmoid激活层与输出层连接。

[0034] 进一步地，所述步骤S4中对inception CNN网络进行训练的具体方法为：

[0035] A1、根据步骤S1至步骤S3，生成正负样本比例为1.5:1的若干训练数据；

[0036] A2、将训练数据中正样本和负样本各随机抽取百分之十作为验证数据集，随机初始化inception CNN网络；

[0037] A3、将训练数据批大小分别设置为32、64和128，并将其输入inception CNN网络；

[0038] A4、将二元交叉熵函数作为损失函数，以损失值最小为目标，使用Sigmoid算法对神经网络的参数进行优化，并使用梯度下降法对神经网络进行参数更新；

[0039] A5、利用验证数据集对损失值进行验证，当损失值不再减小，此时的网络参数保存为最终参数，得到训练完成的inception CNN网络。

[0040] 本发明的有益效果为：

[0041] (1)本发明通过构建字符向量，并将字符向量经过一系列操作转化为二维图像，有效地捕捉了URL中字符的顺序，使恶意URL的识别结果更加准确。

[0042] (2)本发明通过构建inception CNN网络，获得了更好的图像表征，inception CNN网络避免了网络过拟合的问题，加快整个网络传输梯度更新，避免了简单地叠加一个较大的卷积层导致消耗大量计算资源的问题。

[0043] (3)本发明通过将URL转换为二维图像，能够准确的识别恶意URL。

附图说明

[0044] 图1为本发明提出的一种基于URL成像技术的恶意URL检测方法流程图。

[0045] 图2为本发明提出的inception CNN网络的结构示意图。

具体实施方式

[0046] 下面对本发明的具体实施方式进行描述，以便于本技术领域的技术人员理解本发明，但应该清楚，本发明不限于具体实施方式的范围，对本技术领域的普通技术人员来讲，只要各种变化在所附的权利要求限定和确定的本发明的精神和范围内，这些变化是显而易见的，一切利用本发明构思的发明创造均在保护之列。

[0047] 下面结合附图详细说明本发明的实施例。

[0048] 如图1所示，一种基于URL成像技术的恶意URL检测方法，包括以下步骤：

[0049] S1、采集URL字符串，并对其进行哈希处理；

[0050] S2、利用ASCII码对哈希处理后的URL字符串进行编码，对编码后的URL字符串进行归一化处理；

[0051] S3、根据归一化处理过后的URL字符串，采用格拉曼角场将URL字符串转换为二维GAF图像；

[0052] S4、根据卷积神经网络构成inception CNN网络，并对inception CNN网络进行训练；

[0053] S5、将二维GAF图像输入训练完成的inception CNN网络，得到恶意URL的判断结果。

[0054] 步骤S1中采集的URL字符串为$\vec{d}=[d_1,d_2,...,d_i,...,d_n]$，所述$d_i$表示URL的字符，i＝1,2,...,n,n表示URL的长度。

[0055] 步骤S2中利用ASCII码对URL字符串进行编码的具体方法为：通过ASCII码对URL字符串进行编码，得到ASCII字符串；所述ASCII字符串为

$A(\vec{d})=[A(d_1),A(d_2),...,A(d_i),...,A(d_n)]$，$A(d_i)$表示URL的字符$d_i$的ASCII码。

[0056] 所述步骤S2中对编码后的URL字符串进行归一化处理的公式如下：

[0057] $$A^*(d_i)=\frac{A(d_i)-\min A(d_i)}{\max A(d_i)-\min A(d_i)}$$

[0058] 所述编码后的URL字符串进行归一化处理后，得到归一化字符串为

$A^*(\vec{d})=[A^*(d_1),A^*(d_2),...,A^*(d_i),...,A^*(d_n)]$；

[0059] 其中，$A^*(d_i)$表示归一化处理过后的$A(d_i)$，$\min A(d_i)$表示$A(d_i)$中最小的值，$\max A(d_i)$表示$A(d_i)$中最大的值。

[0060] 步骤S3包括以下分步骤：

[0061] S3.1、根据归一化处理过后的URL字符串，将其笛卡尔坐标系转变为极坐标系；

[0062] S3.2、将极坐标系的数据分别放入格拉曼角差场和格拉曼角和场中，得到新的一维数据；

[0063] S3.3、将新的一维数据按照URL字符顺序对应排布，得到二维GAF图像。

[0064] 步骤S3.1包括以下分步骤：

[0065] S3.1.1、根据归一化后的字符串$A^*(d_i)$，获取距离r和反余弦φ，具体计算公式如下：

[0066] $$\begin{cases} r=\frac{t_i}{N} & t_i\in N \\ \phi=\arccos(A^*(d_i)) & -1\le A^*(d_i)\le 1 \end{cases}$$

[0067] S3.1.2、根据距离r和反余弦φ，将归一化后的字符串$A^*(d_i)$用极坐标表示；

[0068] 其中，r表示URL字符用极坐标表示时的点到原点的距离，t_i表示时间步长，N表示正则化极坐标系统扩张成空间的常数因子。

[0069] 步骤S3.2中格拉曼角差场GADF为：

[0070] $$GADF=\sqrt{I-\overline{X}^2}'\cdot\overline{X}-\overline{X}'\cdot\sqrt{I-\overline{X}^2}$$

[0071] 步骤S3.2中格拉曼角和场GASF为：

[0072] $$GASF=\overline{X}'\cdot\overline{X}-\sqrt{I-\overline{X}^2}'\cdot\sqrt{I-\overline{X}^2}$$

[0073] 其中，$\overline{X}$表示使用极坐标表示的URL字符串，I表示单位行向量，$\overline{X}'$表示$\overline{X}$的导数，$\sqrt{I-\overline{X}^2}'$表示$\sqrt{I-\overline{X}^2}$的导数。

[0074] 步骤S4中的inception CNN网络包括输入层，所述输入层分别与第一卷积层的输入端、第二卷积层的输入端、第三池化层的输入端和第四卷积层的输入端连接。

[0075] 第一卷积层的输出端通过第一池化层和第一展平层与拼接层的输入端连接，所述第二卷积层的输出端通过第二池化层和第二展平层与拼接层的输入端连接，所述第三池化层的输出端通过第三卷积层和第三展平层与拼接层的输入端连接，所述第四卷积层的输出端与拼接层的输入端连接。

[0076] 拼接层的输出端通过依次连接的第一连接层、失活层、第二全连接层、第三全连接层和sigmoid激活层与输出层连接。

[0077] 步骤S4中对inception CNN网络进行训练的具体方法为：

[0078] A1、根据步骤S1至步骤S3，生成正负样本比例为1.5:1的若干训练数据；

[0079] A2、将训练数据中正样本和负样本各随机抽取百分之十作为验证数据集，随机初始化inception CNN网络；

[0080] A3、将训练数据批大小分别设置为32、64和128，并将其输入inception CNN网络；

[0081] A4、将二元交叉熵函数作为损失函数，以损失值最小为目标，使用Sigmoid算法对神经网络的参数进行优化，并使用梯度下降法对神经网络进行参数更新；

[0082] A5、利用验证数据集对损失值进行验证，当损失值不再减小，此时的网络参数保存为最终参数，得到训练完成的inception CNN网络。

[0083] 在本实施例中，使用Sigmoid算法对inception CNN网络参数进行优化时，将学习率设定为0.001，训练至损失值为0.4时，损失值不再下降，此时的网络参数为inception CNN神经网络的最终参数。

[0084] 在本实施例中，将本发明与其它方法进行实验对比，它们对恶意URL的识别准确率如表1。

[0085] 表1

[0086]

方法	LSTM	TCN	FCN	inception CNN	RF	DT	SVM
准确率	0.957	0.902	0.944	0.9732	0.9303	0.8115	0.8455

[0087] 其中，机器学习方法有RF、DT和SVM，RF表示使用随机森林得到的实验结果，DT表示使用决策树得到的实验结果，SVM表示使用支持向量机得到的实验结果，深度学习方法有LSTM、TCN和FCN，LSTM表示使用长短时记忆方法得到的实验结果，TCN表示使用时态卷积网络得到的实验结果，FCN表示使用全连接网络得到的实验结果，inception CNN表示使用本发明得到的实验结果。从表1从可以明显看出本发明对恶意URL的识别率最高，证明本发明能够高准确率的识别恶意URL。

[0088] 本发明通过构建字符向量，并将字符向量经过一系列操作转化为二维图像，有效地捕捉了URL中字符的顺序，使恶意URL的识别结果更加准确。本发明通过构建inception CNN网络，获得了更好的图像表征，inception CNN网络避免了网络过拟合的问题，加快整个网络传输梯度更新，避免了简单地叠加一个较大的卷积层导致消耗大量计算资源的问题。本发明通过将URL转换为二维图像，能够准确的识别恶意URL。

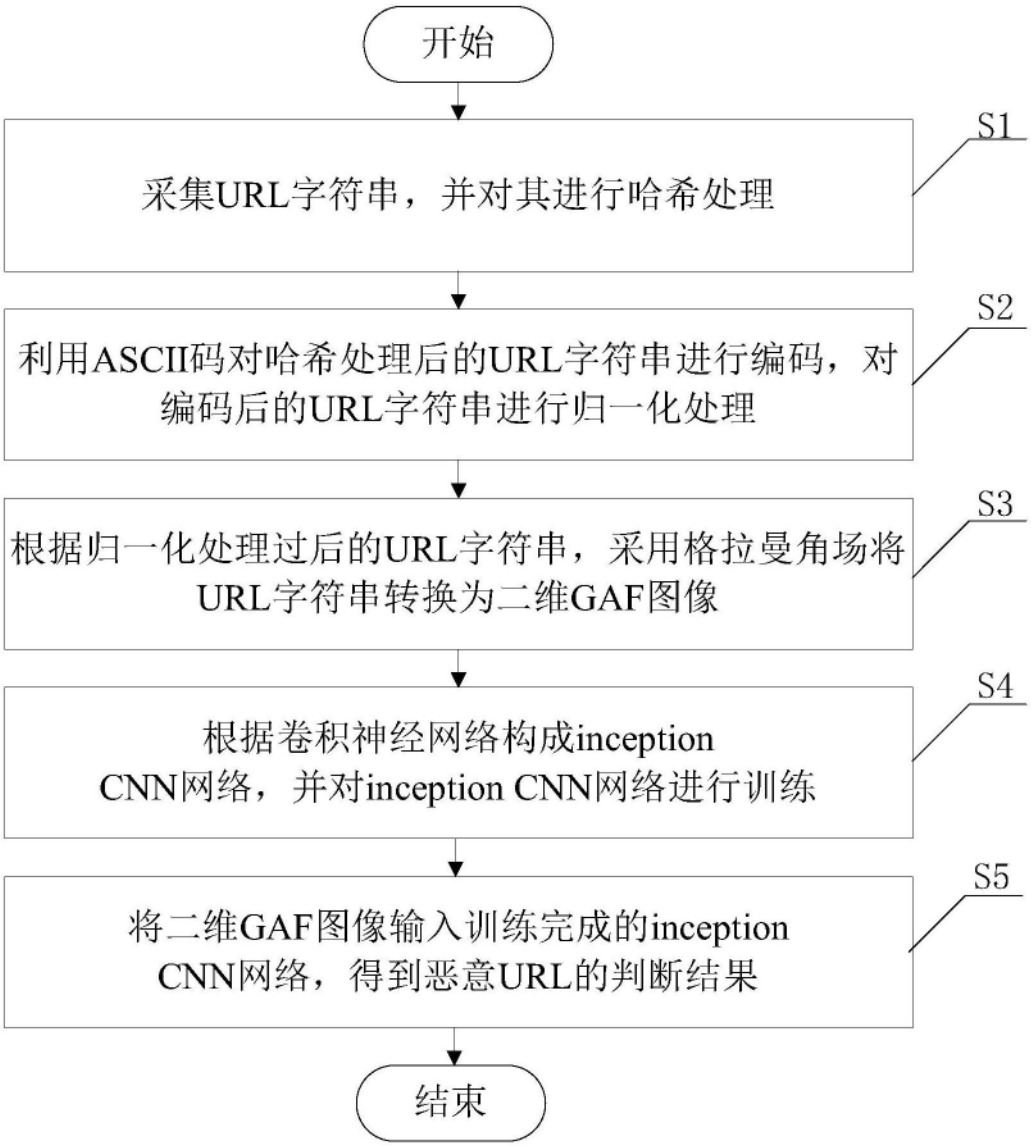

开始
S1
采集URL字符串，并对其进行哈希处理
S2
利用ASCII码对哈希处理后的URL字符串进行编码，对编码后的URL字符串进行归一化处理
S3
根据归一化处理过后的URL字符串，采用格拉曼角场将URL字符串转换为二维GAF图像
S4
根据卷积神经网络构成inception CNN网络，并对inception CNN网络进行训练
S5
将二维GAF图像输入训练完成的inception CNN网络，得到恶意URL的判断结果
结束

图1

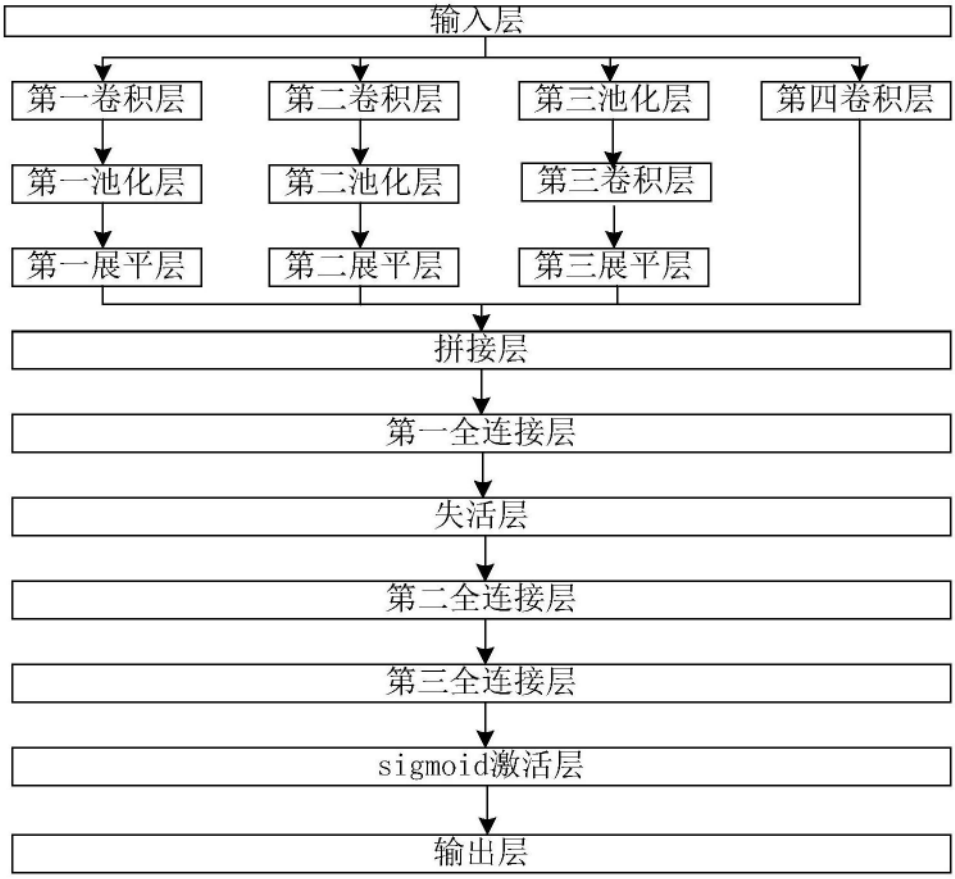

输入层
第一卷积层
第二卷积层
第三池化层
第四卷积层
第一池化层
第二池化层
第三卷积层
第一展平层
第二展平层
第三展平层
拼接层
第一全连接层
失活层
第二全连接层
第三全连接层
sigmoid激活层
输出层

图2