(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 113010895 A
(43)申请公布日 2021.06.22

(21)申请号 202011423335.6

(22)申请日 2020.12.08

(71)申请人 四川大学
地址 610065 四川省成都市一环路南一段24号

(72)发明人 刘嘉勇 贾鹏 王炎

(51)Int.Cl.
G06F 21/57(2013.01)
G06N 3/04(2006.01)
G06N 3/08(2006.01)

权利要求书2页 说明书4页 附图3页

(54)发明名称

一种基于深度学习的漏洞危害评估指标技术

(57)摘要

本发明涉及安全漏洞危害评估技术领域和深度学习神经网络领域,旨在提供一种更加完善的多维度安全漏洞危害性评估技术。该技术的核心是将安全漏洞的评估指标值转化为特征向量,利用DNN神经网络学习漏洞的特征向量,以生成漏洞的类别词典。该技术的工作流程为将安全漏洞的包括危害性、通用度、漏洞生命周期及利用开销等多项评估指标值转换为数值特征向量,接着提取各个特征向量中的数值特征,利用全连接神经网络DNN学习漏洞的评估指标值特征,最后生成漏洞的类别词典。其中在生成类别词典时利用了softmax激活函数实现多分类任务。最后利用生成的深度学习模型进行漏洞危害评估。本技术为安全漏洞的危害性评估提供了一种新的解决方案。

CN 113010895 A

1.一种基于深度学习的漏洞危害评估指标技术,其特征在于,所述方法包括以下步骤:

A、对安全漏洞进行统计划分,依照多维度评估指标体系提出的评估准则构建每一个安全漏洞的评估指标值;

B、将安全漏洞的多项评估指标值转化为效能系数,从而为每个安全漏洞构成一个数值特征向量;

C、构建一个全连接神经网络DNN,利用DNN来提取各个向量中的数值特征,并通过学习漏洞的评估指标值特征来训练深度学习模型;

D、利用softmax激活函数实现多分类任务,并以此生成安全漏洞的类别词典;

E、基于生成的深度学习模型及漏洞类别词典,进行安全漏洞危害评估 。

2.根据权利要求1所述的一种基于深度学习的漏洞危害评估指标技术,其特征在于,所述的步骤A进一步包括如下步骤:

A1、多维度评估指标体系从危害性、通用度、漏洞生命周期、利用开销等4个评估维度,通过22个评估指标来综合衡量漏洞的危害程度,评估指标的选取参考了CVSS、CWSS、CNNVD、CVRS等指标体系的指标,并结合漏洞评估的特点新增了部分评估指标;

A2、评估指标值对于不同的评估维度并不相同,大体上可分为五类:无、低、高、默认、未知。

3.根据权利要求2所述的一种基于深度学习的漏洞危害评估指标技术,所述的步骤A1中的四个评价维度还可做如下细分:

A11、危害性指标集主要对漏洞产生的危害进行评估,分为目标影响和环境影响两个方面,从机密性影响、完整性影响、可用性影响等方面分别对漏洞对目标和目标环境产生的影响进行描述,漏洞对目标和环境机密性、完整性、可用性的影响越大,则漏洞的危害性越大;

A12、通用度指标集主要从漏洞影响范围的维度来衡量漏洞危害性,该指标集包括了操作系统范围、应用程序范围、威胁对象类型、支持的硬件架构范围、目标的规模等几个方面的指标,漏洞适用的操作系统、应用程序、硬件架构、目标群体越多,则漏洞的危害性越大;

A13、漏洞生命周期指标集主要从动态变化的角度来度量漏洞的危害性,在漏洞从出现到消亡的整个声明周期中,漏洞对应的利用代码成熟度、修复方案、来源可信度、利用代码扩散度、被检测率等指标都是不断变化的,漏洞的危害程度也随着这些指标的改变而不断变化;

A14、利用开销指标集主要从攻击者成功利用漏洞的复杂度和所需付出的代价等角度来衡量漏洞的危害性,该维度包括了权限要求、隐蔽性、攻击途径、用户交互、攻击复杂度、是否需要其他漏洞配合等指标,漏洞利用需要的权限越高、漏洞的隐蔽性越低、不能远程攻击且需要用户交互、漏洞利用的复杂度越高、漏洞对其他漏洞的依赖越高则漏洞的危害性越小。

4.根据权利要求1所述的一种基于深度学习的漏洞危害评估指标技术,其特征在于,所述的步骤B进一步包括如下步骤:

结合网络安全保护等级和国际危机管理的分级惯例,将漏洞危害性评价评语等级分为5级,即很高、高、中、低和很低;评价指标是定性指标,将其转换为定量指标可通过制定评价指标评分等级标准予以实现;按照5分制原则确定各等级的赋值,则其评价系数对应为5、4、3、2、1,评价指标等级介于两者之间的相应的评分为4.5、3.5、2.5、1.5、0.5,从而为漏洞构

成一个数值特征向量。

5.根据权利要求1所述的一种基于深度学习的漏洞危害评估指标技术,其特征在于,所述的步骤C中的全连接神经网络DNN具体结构如下:

我们搭建的DNN由输入层、隐藏层、输出层和softmax函数组成,其中输入层由22个神经元组成,对应安全漏洞数据集中的22个特征,作为输入向量,隐藏层有两层,每层分别有7和8个神经元,之后就是输出层,由100个神经元组成,对应安全漏洞数据集的目标变量的类别个数,最后使用一个softmax函数,用于解决多分类问题而创建。

6.根据权利要求5所述的一种基于深度学习的漏洞危害评估指标技术,其特征在于,所述的全连接神经网络DNN具体参数如下:

在这个模型中,我们选择的神经元激活函数为ReLU函数,损失函数为交叉熵(cross entropy),迭代的优化器(optimizer)选择Adam,最初各个层的连接权重(weights)和偏重(biases)是随机生成的。

7.根据权利要求1所述的一种基于深度学习的漏洞危害评估指标技术,其特征在于,所述的步骤E具体如下所示:

E1、加载训练好的DNN深度学习模型以及漏洞类别词典,类别词典中有100类漏洞评分,输入为一个带有22个评估指标的未知漏洞;

E2、利用深度学习模型预测输入的未知漏洞的危害性。

一种基于深度学习的漏洞危害评估指标技术

技术领域

[0001] 本发明涉及安全漏洞危害评估技术领域和深度学习神经网络领域。该技术的核心是以危害性、通用度、漏洞生命周期及利用开销等4个评估维度，总共22项评估指标来度量漏洞的危害层度，然后将每项评估指标的值转换为数值特征向量，接着提取各个特征向量中的数值特征，利用全连接神经网络DNN学习漏洞的评估指标值特征，使用softmax激活函数生成漏洞的类别词典。最后利用生成的深度学习模型及类别词典进行漏洞危害评估。

背景技术

[0002] 软件安全漏洞是指在软件设计或代码实现过程中留下的弱点或缺陷。攻击者针对这些漏洞，能够产生特定的外部输入触发漏洞，从而窃取系统信息或进行恶意破坏。然而，随着软件规模与复杂度的增加，以及计算机系统或底层软件存在设计上的缺陷，编程人员很难完全杜绝漏洞的产生。部分软件公司甚至可能留存后门或保留隐藏功能导致软件漏洞更加严重。

[0003] 海量的安全漏洞数量以及漏洞产生原因的多样化导致对安全漏洞的危害性进行准确评估，难度较大。为了解决这一问题，需要进一步对漏洞危害评估技术进行研究。通过完善的指标体系，从不同的维度刻画漏洞的危害程度，能够方便用户了解软件、系统的安全性，为研究人员提供更全面的漏洞信息，为网络管理人员提供决策信息，从而采取适当安全措施，保证网络的安全状况。

[0004] 在评估指标体系方面，目前主流的指标体系有CVSS、CWSS、CVRS、CNNVD等，虽然一定程度上解决了现在漏洞危害性评估困难的问题，但依然存在以下这些问题。

[0005] 一、现有指标体系没有考虑漏洞危害性的动态性，漏洞的危害程度与网络中与该漏洞相关的资料和工具的丰富程度有很大关系，资料和工具越多，漏洞利用的难度就越低，危害性也越大。

[0006] 二、现有指标体系没有考虑漏洞被主流查毒软件查杀的情况，能检测到该漏洞的杀毒软件的数量越多，漏洞的危害性自然也越低。

[0007] 三、现有指标体系没有考虑目标漏洞与其他漏洞的依赖关系，目前许多漏洞的触发都需要其他漏洞的支撑，现有指标体系没有考虑该方面的影响。

[0008] 四、现有指标体系没有考虑漏洞通用度对评估漏洞危害性产生的影响，漏洞的通用性是评估漏洞危害的一个重要维度，漏洞影响的操作系统版本越多，影响的软件类型越多，漏洞所影响的目标(系统或软件)的应用范围越广，显然漏洞的危害性越大。

[0009] 本评估方法的主要目标是解决上文描述的目前漏洞危害评估领域依然存在的这些问题，分析典型漏洞引发的危害性类型，研究典型危害性的机理，研究漏洞危害性相关的评估维度及各维度之间的关系，研究漏洞危害性量化标准，建立漏洞危害性评估指标体系。

发明内容

[0010] “一种基于深度学习的漏洞危害评估指标技术”是在安全漏洞危害性评估过程中

针对现有技术存在的问题所提出来的发明。本发明的主要目标是解决目前漏洞危害评估领域依然存在的各种问题，如没有考虑漏洞的危害性的动态性、没有考虑漏洞被主流查毒软件查杀的情况以及没有考虑目标漏洞与其他漏洞的依赖关系等。提供一种基于深度学习神经网络的漏洞危害评估指标技术，以有效地考虑到各种因素的影响，提高评估精度。本发明中的评估方法提供了一种新的评估思路，通过考虑安全漏洞的多维度的评估指标，构建一种新的数值特征向量生成模型，利用全连接神经网络技术保留漏洞更多的向量隐藏信息，从而充分考虑到各种影响因素对预测的准确性造成的影响。该方法可以广泛地用于各种安全漏洞危害性评估场景，相比与传统方法，其评估结果更加客观。

[0011] 为了实现上述目标，本发明提出了一种基于深度学习的漏洞危害评估指标技术，该技术对安全漏洞进行统计划分，依照多维度评估指标体系提出的评估准则来构建每一个安全漏洞的评估指标值，然后将安全漏洞的多项评估指标值转化为效能指数，从而为每个安全漏洞构成一个数值特征向量；接着构建一个全连接神经网络DNN，利用DNN来提取各个向量中的数值特征，并通过学习漏洞的评估指标值特征来训练深度学习模型；另外利用softmax激活函数实现多分类任务，以此生成安全漏洞的类别词典；基于生成的深度学习模型及漏洞的类别词典，进行安全漏洞危害评估。其中多维度评估指标体系从危害性、通用度、漏洞生命周期、利用开销等4个评估维度，通过22个评估指标来综合衡量漏洞的危害程度，评估指标的选取参考了CVSS、CWSS、CNNVD、CVRS等指标体系的指标，并结合漏洞评估的特点新增了部分评估指标。危害性分为目标影响和环境影响，从机密性、完整性、可用性等方面进行描述；通用度则包括了操作系统、应用程序、威胁对象类型、支持的硬件架构范围、目标规模等方面的指标；漏洞生命周期主要从生态变化的角度度量漏洞的危害性；利用开销包括了权限要求、隐蔽性、攻击途径、用户交互、攻击复杂度、是否需要其他漏洞配合等指标。该技术框架包含了评估指标提取模块、数值特征向量生成模型、DNN神经网络、漏洞评估模型等四个模块。评估指标提取模块主要是提取上述提及的各维度的22个评估指标，并生成一个指标向量；数值特征向量生成模型将指标向量作为输入，并对其进行one-hot编码生成数值特征向量；DNN神经网络通过一个三层神经网络架构学习各漏洞的数值向量训练漏洞危害性评估模型并生成漏洞的类别词典；漏洞评估模块则是基于训练好的深度学习模型及生成的类别词典对漏洞进行危害性评估。

附图说明

[0012] 从下面结合附图的详细描述中，将会更加清楚的理解本发明的目标、实现方法、优点和特性，其中。

[0013] 图1是一个展示本发明的评估技术整体结构的架构图。

[0014] 图2是一个说明本发明的评估技术中one-hot编码处理举例的示意图。

[0015] 图3是一个说明本发明的评估技术中基于softmax激活函数的DNN神经网络模型的架构图。

[0016] 图4是一个说明本发明的评估技术中softmax激活函数实现多分类任务的示意图。

[0017] 图5是一个说明本发明的评估技术中安全漏洞危害性评估的流程图。

具体实施方式

[0018] 本发明的安全漏洞危害性评估技术可以广泛地用于各种安全漏洞危害性评估场景。下面结合附图对本发明做进一步说明。本发明旨在提供一种解决目前漏洞危害评估领域依然存在的各种问题。基于深度学习神经网络的漏洞危害评估指标技术主要通过安全漏洞中包含的评估指标值信息,利用DNN深度学习神经网络训练得到高精度的分类模型。训练的模型可以有效地用于安全漏洞评估等场景。

[0019] 图1是一个展示本发明的评估技术整体结构的架构图。

[0020] 如图1所示,该技术框架包含了评估指标提取模块、数值特征向量生成模型、DNN神经网络、漏洞评估模型等四个模块。评估技术首先通过评估指标提取模块对输入的带有评估指标值的已知漏洞提取上述提及的危害性、通用度、漏洞生命周期、利用开销等各维度的22个评估指标,并生成一个评估指标向量;数值特征向量生成模型将评估指标向量作为输入,在该模型中对输入进行one-hot编码来将安全漏洞的多项评估指标值转化为效能系数,从而为每个安全漏洞构成一个数值特征向量;DNN神经网络通过一个三层神经网络架构学习各漏洞的数值向量以训练漏洞危害性评估模型,并通过softmax激活函数层生成漏洞的类别词典;最后,评估技术将未知漏洞的数据进行处理后,通过训练好的深度学习模型及生成的类别词典对漏洞进行危害性评估。

[0021] 图2是一个说明one-hot编码处理举例的示意图。

[0022] One-Hot编码,又称为一位有效编码,主要是采用N位状态寄存器来对N个状态进行编码,每个状态都有独立的寄存器位,并且在任意时候只有一位有效。One-Hot编码是分类变量作为二进制向量的表示。这首先要求将分类值映射到整数值。然后,每个整数值被表示为二进制向量,除了整数的索引之外,它都是零值,它被标记为1。如图2举例所示,用图示三个特征来描述某个实体,即“属性11,属性23,属性32”,如果特征类别是有序的话,我们能够用表示顺序的数组表示即“属性11,属性23,属性32” ==> [0,2,1],但是这样的特征处理并不能直接放入机器学习或深度学习算法中,因为类别之间是无序的。这时候就可以用独热编码的形式来表示了,我们用采用N位状态寄存器来对N个状态进行编码,因此,当我们再描述该实体的时候,便可以采用[1 0 0 0 1 0 1 0 0]。

[0023] 图3是一个描述DNN神经网络模型的架构图。

[0024] 如图3所示,我们搭建的DNN深度学习模型由输入层、隐藏层、输出层和softmax函数组成,其中输入层由22个神经元组成,对应安全漏洞数据集中的22个特征,作为输入向量,隐藏层有两层,每层分别有7和8个神经元,之后就是输出层,由100个神经元组成,对应安全漏洞数据集的目标变量的类别个数,最后,就是一个softmax函数,用于解决多分类问题而创建。在这个模型中,我们选择的神经元激活函数为ReLU函数,损失函数为交叉熵(cross entropy),迭代的优化器(optimizer)选择Adam,最初各个层的连接权重(weights)和偏重(biases)是随机生成的,每次训练的批数为64,共迭代10次。

[0025] 图4是一个描述softmax激活函数实现多分类任务的示意图。

[0026] 如图4所示,在机器学习尤其是深度学习中,softmax是个非常常用而且比较重要的函数,尤其在多分类的场景中使用广泛。他把一些输入映射为0-1之间的实数,并且归一化保证和为1,因此多分类的概率之和也刚好为1。softmax是一种形如下式的函数:

$$P(i)=\frac{exp(\theta_i^T x)}{\sum_{k=1}^{K}\theta_i^T x}$$

通过softmax函数,可以使得P(i)的范围在[0,1]之间。在回归和分类问题中,通常θ是待求参数,通过寻找使得P(i)最大的θi作为最佳参数。Softmax函数加入了e的幂函数是为了两极化:正样本的结果将趋近于1,而负样本的结果趋近于0。这样为多类别分类提供了方便(可以把P(i)看作是样本属于类别i的概率)。可以说,softmax函数是logistic函数的一种泛化。在本发明中,评估系统的训练集为1万条左右带有评估指标的CVE漏洞集,该漏洞数据集的漏洞评分是通过人工标注形成的。在经过各个模块的处理后,softmax函数将CVE漏洞的评分1~10分为100个类别,形成一个类别词典,用于漏洞危害性预测评估。

[0027] 图5是一个描述安全漏洞危害性评估的流程图。

[0028] 如图5所示,本发明采用深度学习模型进行漏洞危害性评估。评估技术首先通过评估指标提取模块对输入的带有评估指标值的未知漏洞提取上各维度的22个评估指标,并生成一个评估指标向量;数值特征向量生成模型将评估指标向量作为输入,在该模型中对输入进行one-hot编码将安全漏洞的多项评估指标值转化为效能系数,从而为每个安全漏洞构成一个数值特征向量;最后,评估技术经过漏洞评估模块即训练好的是深度学习模型及生成的类别词典对漏洞进行危害性评估。

[0029] 如上所述,本发明通过考虑安全漏洞多维度评估指标并生成其数值特征向量进行漏洞危害性评估,其优点在于:1、在详细分析了现有漏洞危害评估指标体系的基础上,提出了一个更加完善的多维度漏洞危害性评估指标体系,详细阐述了指标体系所涉及的评估维度及代表的含义,介绍了各个维度的分级方法。2、提出的对指标向量进行one-hot编码生成数值特征向量可简便地将指标值转换为数值,会让特征之间的计算更加合理。3、在进行模型训练时,在输出层引入了softmax激活函数可方便实现多分类任务。4、本发明的评估技术可以充分考虑到各种影响漏洞危害性的评估指标,并以此提高预测漏洞危害性的准确性。

[0030] 尽管出于说明的目的描述了本发明的优选实施例子,本领域人员将理解,在不脱离如附属权利要求所披露的本发明的范围和精神的情况下,各种修改、增加和替换都是可能的。

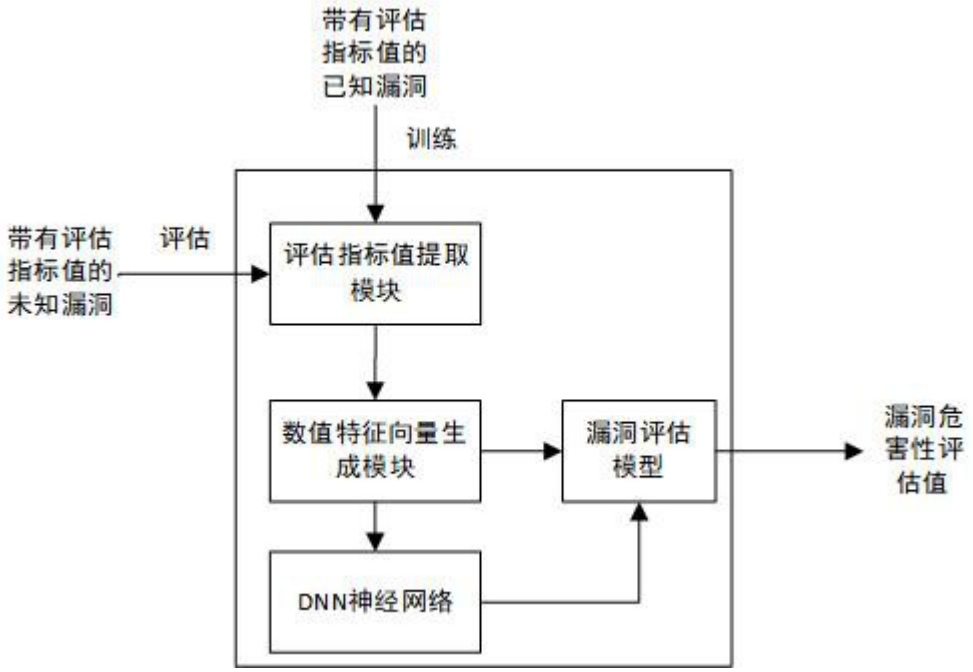

图1

特征1	特征2	特征3
[“属性11”，”属性12”]	[“属性21”，”属性22”，”属性23”]	[“属性31”，”属性32”，”属性33”，“属性34”]
N=2	N=3	N=4
属性11：10 属性12：01	属性21：100 属性22：010 属性23：001	属性31：1000 属性32：0100 属性33：0010 属性34：0001

图2

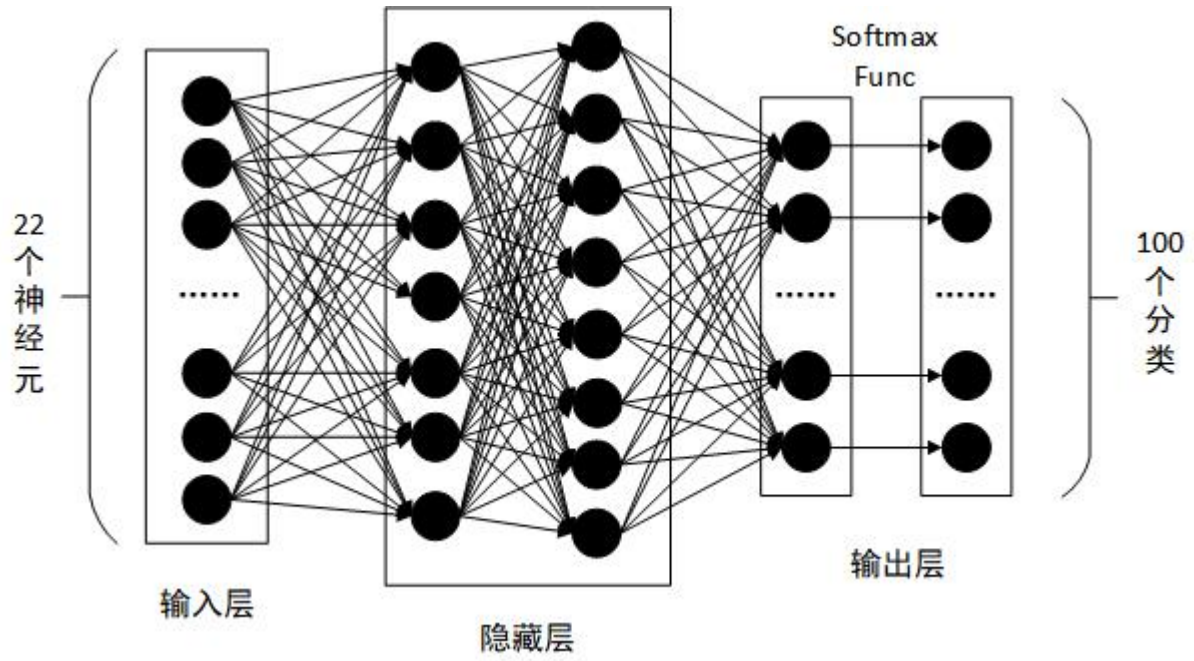
Softmax
Func
22
个
神
经
元
100
个
分
类
输入层
隐藏层
输出层

图3

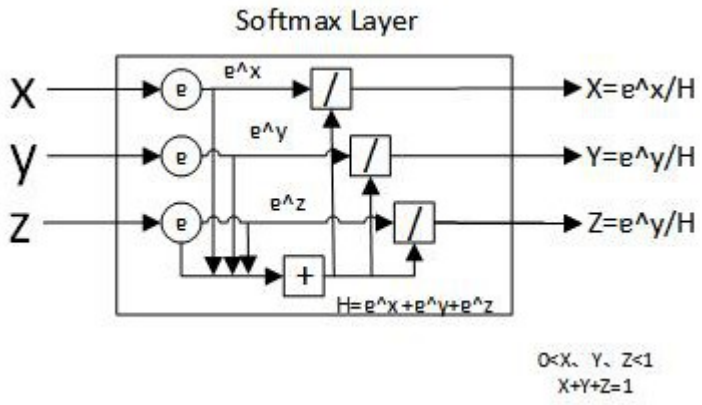
Softmax Layer
X
y
z
e
e^x
e^y
e^z
+
H=e^x+e^y+e^z
X=e^x/H
Y=e^y/H
Z=e^y/H
0<X、Y、Z<1
X+Y+Z=1

图4

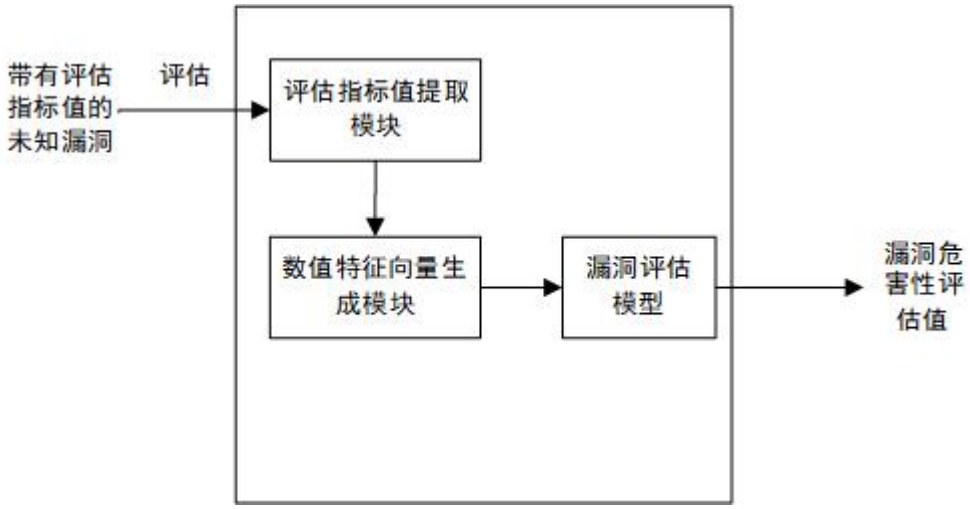

图5