DOI:10.19322/j.cnki.issn.1006-4710.2021.03.013

基于区块链的大型社交类网游敏感信息数据挖掘框架

白 杰[1,2]，杜彦辉[1]

(1.中国人民公安大学 信息网络安全学院，北京 100038；2.温州大学 国际教育学院，浙江 温州 325035)

摘要：本文针对社交类网游中敏感信息识别处理体系展开研究，提出了区块链模式下网游敏感信息即时数据挖掘框架。选取某大型社交网游聊天室数据库进行测试，采用基于Python的SKLearn库进行数据预处理，通过TensorFlow实现模型训练和验证。结果表明：针对网游语境中的短文本识别，TextCNN的准确率高于朴素贝叶斯、CNN两种模型5%以上，因此在模型数据层中引入TextCNN模型能够满足大型网游中敏感信息识别高效、精准的要求。结论证明，区块链模式下的网游敏感信息挖掘框架具有联盟链的层级管理优势、分布式账本对信息传播全程留痕的特性，并能通过智能合约和共识机制提升合约执行力。

关键词：网络敏感信息；社交类网游；区块链模型；深度学习

中图分类号：TP391.1 **文献标志码：**A **文章编号：**1006-4710(2021)03-0397-06

Data mining framework for sensitive information of large-scale social online games based on blockchain

BAI Jie[1,2], DU Yanhui[1]

(1. College of Information Network Security, People's Public Security University of China, Beijing 100038, China; 2. College of International Education, Wenzhou University, Wenzhou 325035, China)

Abstract: This paper studies the sensitive information recognition and processing system in social online games. A real-time data mining framework for sensitive information on online games in the blockchain mode is proposed. A large-scale social online game chat room database is selected for testing, with SKLearn library based on Python is used for data preprocessing. The model training and verification are implemented through Tensorflow. The results show that the accuracy of TextCNN is over 5% higher than that of Naive Bayes and CNN models for short text recognition in online game context, so TextCNN model can meet the requirements for high efficiency and accuracy of sensitive information recognition in large-scale online games. The conclusion proves that the blockchain-based online game sensitive information mining framework has the advantage of alliance chain hierarchical management, the characteristics of the distributed ledgers leaving traces in the whole process of information dissemination, and enhanced contract enforcement through the smart contracts and consensus mechanisms.

Key words: network sensitive information; social online games; blockchain model; deep learning

2020年9月29日，中国互联网络信息中心发布的第46次《中国互联网络发展状况统计报告》显示，中国网民中网络游戏类用户超过5.3亿[1]。社交型网游占网游总数的85%以上，网络游戏社区的虚拟身份特征，使得参与者会更随意地发表未经求证的观点，进而成为网络舆情的参与者及传播者。针对业务量大、受众广的社交类网络游戏舆情，人工智能方法模型为网络敏感信息的发掘提供了工具，

收稿日期：2021-01-22； **网络出版日期：**2021-04-14

网络出版地址：https://kns.cnki.net/kcms/detail/61.1294.N.20210414.0853.002.html

基金项目：国家重点研发计划重点专项项目(2016YFB0801105)

第一作者：白杰，女，博士后，讲师，研究方向为网络安全防控及大数据建模。E-mail：wxbaijie@163.com

通信作者：杜彦辉，男，博士，教授，博导，研究方向为网络安全执法技术。E-mail：dyh6889@126.com

例如深度学习被广泛应用于自然语言处理领域中的文本分类[2-4]。区块链以其分布式数据库技术以及去中心化、共识机制等优势,逐渐被应用到舆情管控及电子存证领域[5-7],但前人的研究多侧重于事后的数据分析,缺少重要的事前防控和事中监管对策[8-9]。如何利用区块链优势,建立敏感信息的即时监控处理系统,从海量大数据中抓取敏感词汇,对抓取的数据运用高效的算法加以分析,并进行在线监测、预警、溯源,成为亟待解决的问题。

本文的主要创新点:

1) 本研究提出了一种区块链架构下网游平台敏感信息的发掘、判断及处理框架;在敏感信息挖掘过程中,结合区块链的分布式记账系统提高敏感信息挖掘效率,利用区块链的可溯性实现敏感信息源的快速追溯,有效提高网游中敏感信息的处理精度;

2) 在区块链模式下改进数据模型层,应用优化后的深度学习算法提高文本分类标注的精准性和效率,通过数据库测试取得较高的效率,为后续多款网游的网络安全监控提供理论基础。

1 敏感信息处理过程及方法综述

网络敏感信息包含文字、图片及语音视频等多种媒体形式,在大型网游中,中/英文短文本是其主要的交流方式。网游中的敏感文本信息可分为主题性文本和带情感倾向的文本[10]。敏感信息中具有明显主题词语(如暴力、色情、诈骗、垃圾信息等)的文本,被判定为主题性文本,技术上常用 Web 爬虫程序抓取特定关键词,并对抓取到的消息进行屏蔽处理。具有情感倾向性的不良文本,则包含了信息发布者的观点、态度、立场等信息。而网游端的国外玩家占有相当一部分比例,使得网游成为政治经济类敏感言论的集中地。这类信息变化度较大,很难及时识别,给控制不良舆情的发酵带来了极大的挑战,游戏研发公司往往通过人工识别来标记,耗费大量人力的同时又很难兼顾效率,因此需要溯源并挖掘其传播路径,采用智能化的方法及时处理。单一点对点的输入—输出往往效率较低,舆情处理通常是依从游戏玩家→信息端→网络总控制中心→公安网络安全部门→网络总控制中心→游戏端→玩家的反馈处理顺序,很难满足舆情控制时间紧、任务重的需要,且需要占用大量警力进行排查溯源。

目前 Web 挖掘标志性算法有决策树、规则归纳、贝叶斯方法、支持向量机、神经元网络等[11-13]。作为当前的研究热点,深度学习算法利用多个处理层,逐步强化机器学习,对数据集进行抽象处理,替代手工获取特征,提高了抓取的效率[14],最大程度地简化了特征工程和预处理。根据实际情况,复杂的网络文本需要更多的训练数据,预训练的词向量可以为分类结果带来提升,更能体现深度学习在敏感信息挖掘方面的优势。

随着区块链 3.0 时代的到来,在网游舆情防控过程中,联盟链的构建能更好地解决网络安全管理部门和互联网企业在应对舆情管理时的层级问题,分布式账本不可篡改的特性能充分保障信息传播全程留痕,智能合约和共识机制确保了舆情挖掘中数据的真实性和合约的执行力。区块链独有的技术特征能够充分提高网络舆情管理的准确度和效率,加大信息安全和隐私保护力度。

2 区块链模式下的网游网络敏感信息模型

2.1 区块链模式下网络敏感信息挖掘系统

图 1 为区块链模式下网络敏感信息挖掘系统架构。

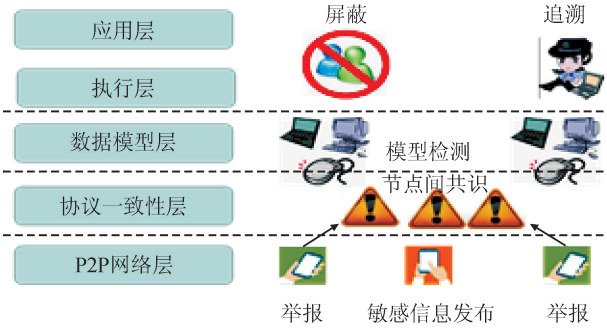

图 1 区块链模式下网络敏感信息挖掘系统架构

Fig. 1 Network sensitive information mining system architecture in blockchain mode

2.1.1 底层 P2P 网络

游戏玩家发布文字信息的过程会采用 P2P 网络,每个节点都同时保留所有数据,这样即使其中一个节点删除了敏感信息词汇,在其他节点中也留有证据。在信息发布过程中调用区块链的发布接口,采样节点通过网络爬虫爬取敏感词汇,针对主题性文本建立敏感信息词库,从而实现敏感信息数据采集功能。每区服定时将所识别的数据使用非对称加密通信技术签名后发送给可信存储服务模块。

2.1.2 协议一致性层(共识机制)

区块链模式下的敏感信息挖掘系统中,各节点之间只有达成共识,确定某一信息为不良舆论,才可以进行下一步操作。共识机制的主要作用是保持底层区块链敏感数据认证的一致性,防止恶意不实举报或者玩家无意识的举报点击,避免了大量伪敏感信息,从而节约了计算空间,减少了无效计算[15]。

通过共识机制，确定敏感信息的真实性后，将当前区块生成的哈希值加入到父系区块中，并存入加密区块链中进行防篡改保护。

2.1.3 数据模型层

区块链作为一种分布式存储数据库技术，用于实时存证游戏玩家账号信息、信息发布记录等。在区块链中，单个数据区块由区块头和区块体组成。在区块头上记录当前区块的特征值，如信息生成时间、区块数据的散列值及上一区块的散列值等。在敏感信息发酵过程中，首先产生第 0 代区块（无 Hash 地址），之后的交易区块依次指向第 0 代区块，且保留了上一个区块的 Hash 地址（区块的特征标识），区块代间通过 Hash 地址（特征性）相连，形成了信息的链式结构，由此便可记录区块链中敏感信息的第一个发布者以备追查。散列值在消息挖掘区块链中起着决定性作用。每个区块个体（消息）持有唯一性的散列值，散列值随区块内容变化而改变。

2.1.4 执行及应用

敏感信息挖掘的主要过程如下。

1）哈希生成：信息检测者在本地执行深度学习改进算法，抓取文档，获得关键词集合；然后输入时间戳、文档集合以及关键词集合，由此获得确定的作为输出的哈希索引。

2）加密共识：区块链采用非对称加密算法，例如，玩家注册阶段产生一个私钥（Private Key），用 Private Key 和椭圆曲线算法 Secp256k1 生成 65 字节的随机数即公钥，当游戏玩家经由网游客户端发布信息时，系统对公钥进行 SHA256[10] 和 RIPEMD160 双哈希运算，得到 20 字节长度的摘要结果，将其作为主体信息，附加上版本前缀 0x00 及地址校验码，并对摘要结果进行两次 SHA256 运算，取生成哈希值的前四位，最后，版本前缀＋主体信息＋校验位经由 Base58 处理得到地址，将其上传给云端服务器。

3）权限授予：各区服的控制端通过算法确认发布的信息属于非敏感信息后，将密钥和相关参数发送给数据使用者，授予合法权限（发言）。

4）数据解密：数据的使用者通过执行解密算法，输入密钥和加密文档集，输出明文文档集。

5）动态更新：数据发布者向服务器提出文档更新请求，增加或删掉消息。服务器确认原有哈希并对新生成哈希分类，持续动态更新，同时进行敏感词汇判断。

2.2 区块链模式下网络敏感信息挖掘模型特性

在区块链模式下，可以把敏感信息的挖掘过程等同于节点之间的交易（举报）行为，其具体特性对网络敏感信息挖掘模型的影响如下。

2.2.1 敏感信息挖掘节点的去中心化

传统的敏感信息挖掘通常是由玩家举报或者系统检测来实现，然后上传到腾讯网络安全的总库，由游戏安全部门进行确认，再进行反馈及处理，而确认的难度随着敏感信息的变形、改写以及表达形式的多样化而逐步增加，这使得舆情发酵期间数据的处理时间很难满足及时性的要求。

对于敏感信息中的变形词汇，常用的处理方法是应用机器算法加强对敏感词汇的测试，将变形的敏感信息加入词库，以期到达更准确的效果。但是这样需要一个反馈再学习的过程。而大部分玩家（节点）对于变形词汇都能够理解其表达的意思，在区块链模式下，只有 2 个以上节点认证某位玩家发表的是政治言论，才可以达到节点间的共识，进而上传到区块链的模块，使其第一时间发现敏感信息。敏感信息在网络中被挖掘的整体效率取决于网络中所有具有挖掘（举报）能力的节点。每个节点都对所检测出的敏感信息进行记录，当节点间交换数据时，节点间会进行真实性验证。如果验证成功，确定属于网络敏感信息，则将它接收到的信息提交给网络安全部门进行认定和屏蔽处理，这也极大地提高了信息挖掘效率。

2.2.2 敏感信息的可溯性

区块链的时间戳技术可被用来确认每笔数据的发生，在数据中加入时间维度，通过时间维度记录敏感信息转化的顺序，使得数据挖掘过程具有可追溯性。在交易进程中，区块链技术的时间戳机制能够为每笔信息的发布（交易）生成一个 ID，这为信息来源的追查提供了极大的帮助。区块链将持续生成的信息加入到现有全部区块中，一旦新区块的生成条件被所有用户认证，则当前区块就会被加入到主区块链中，每个区块通过特定算法生成的哈希值来标记自身的唯一性，且此过程不可逆。由此可以判断网络敏感信息的演进发酵过程以及未来走向。时间戳技术在保证数据原始性的同时降低了挖掘（交易）追溯的成本，其时序性强化了信息的不可篡改性。针对敏感信息的长期发布来源，游戏公司网络安全部门应引起足够重视，并提交给国家安全部门进行侦查处理，以避免国外恶意势力针对国内青少年的长期舆论导向作用。

2.2.3 敏感信息发布者身份数据加密及信息链式合约

区块链技术应用非对称密码学的原理进行数据

加密。该技术能够妥善保障网络中挖掘(交易)数据的安全,降低由交易数据丢失而引起的风险。倘若外部入侵者意图篡改部分数据,则需要对所有区块的数据进行修改,因此这种改动无法在完善的区块链中产生保障。另外,区块链架构下的敏感数据挖掘模型中,数据在网络中传播需要具有数字签名,用以作为签名人的身份标识及签名人对交易数据内容的认可。大型社交类网游往往在最初要求实名制注册和手机注册相结合,以便通过注册信息核对来确保实名认证,从而保证游戏发言玩家身份(交易者)的安全性。而区块链的特色就是其自动担保程序的智能合约是架设在区块链上而非服务器上,这极大地提高了较大数据量下的分布处理效率[16]。这样,对个人身份的认证则由上传到整个区服的认证,转化为在区块链上(某个具体区的服务器)的认证,极大地提高了认证效率。有研究认为,通过可编程的智能合约能够预测每一个合约的结果,一旦触发合约成立的条件,则代码合约立即执行。也就是通过最初的简短信息的发布,以及该节点一直以来发信息的文字规律,预测该节点即将发布信息的内容,在敏感舆情信息发布之前进行预警处理,提前屏蔽,在舆情爆发之前遏制源头信息。

本文构建的系统保持现有系统的模块化结构。不同的结构或者应用能保证自身模块的独立性和完整性;在保护数据隐私的前提下,允许数据的互操作。每个机构可以定义自己的对外访问接口和形式,实现不同层级的灵活性。

3 改进深度学习算法在区块链数据模型层中的应用

本文尝试将深度学习方法应用到区块链模式下敏感信息挖掘过程的数据模型层当中。主要有三个层次,即文本预处理、词向量表示和深度学习模型。深度学习通过其多层结构来提升训练过程中对数据集特征的学习能力,以实现复杂函数的逼近,解决了传统文本分类中对复杂问题泛化受限从而导致的准确率低的问题。

3.1 文本预处理

无论训练深度学习模型的文本是否已标记,都需要对文本数据进行预处理,包括过滤非中文信息(数字、英文字母、标点、特殊符号、全角字符等)、模板提取(根据具体分类需求,通过模板提取文本样本中的关键信息,剔除其他信息)、文本分词(分词算法根据预设的词典对样本进行匹配识别或标注训练)和去停用词(过滤某些对分类无作用的字或词)等操作。

例如,在一条信息中,网友举报有人借助游戏平台发布色情信息广告,过滤非中文后,归纳提取的模板为“内容+费用+联系方式”。分词分类词典一般采用国家语委语料库、搜狗语料库等。用户定义词典则是由通用词典未包括的、专业的单词组成。网游信息当中的词典,就需要根据实际应用场景,建立用户定义词典,并适时定时进行更新。例如,在聊天网络敏感信息中“操”被列入暴力侮辱性词汇,但是在网游中,“曹操”这个词汇出现几率非常高,因此要建立两个专业单词的区分度。深度学习分词的实现思路为:通过对大量汉字和单词进行标注训练,利用机器学习工具,识别文本中的词语。

3.2 词向量表示

文本预处理后,为了更好地被深度学习模型识别,需要对高维度、高稀疏的样本文本进行词向量表示,以达到较高质量的特征提取以及格式转换。词向量输出包含了每个词向量的向量矩阵,即将高维度、高稀疏编码方式的文本数据转换为连续稠密数据。在基于深度学习的文本分类系统中,将一条网友针对游戏充值未到账表达极度不满的文字信息设为50维向量,样本预处理后,进行Word2Vec计算,输出结果如图2所示。

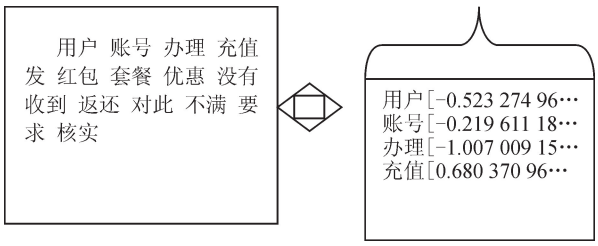

图2 谣言信息转码示例

Fig. 2 Example of rumor information transcoding

3.3 TextCNN模型

建立深度学习分类模型的过程:①训练过程,即用足够量的已标记类别的文本样本集来训练分类;②验证过程,用去除标记的文本样本来测试模型的分类准确性。再通过多轮训练并优化模型,达到分类模型的稳定。本文将深度学习改进模型的几种文本测试结果,与常见的朴素贝叶斯文本分类结果进行对比,测试结果如图3所示。

由于网游对话的特性及对话框字数的限制,网游对话大部分以短文本为主。在深度学习理论中,TextCNN对文本浅层特征的抽取能力很强,在短文本领域(如搜索、对话领域)专注于意图分类时效果很好、应用广泛且速度快,具有明显优势[17]。

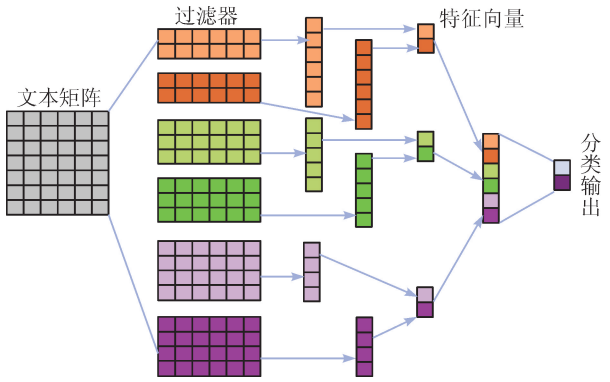

图 3　TextCNN 模型架构图

Fig. 3　Architecture diagram of TextCNN model

图 3 中，词向量构成文本矩阵，过滤器的卷核大小分别为 2、3、4，经过卷积池化得到特征向量，其维数等于卷积核尺寸的个数乘以每种尺寸卷积核的个数，TextCNN 分为 4 层。

卷积层：在本文的 TextCNN 模型中，有 3 个过滤器（卷积核大小分别为 2、3、4）可以分别提取不同的文本特征。过滤器将大小为 3×3×1 的节点矩阵转化为单位节点矩阵，而对于单位节点矩阵中的第 i 个节点，假设 $wi_{x,y}$ 表示过滤器输入节点 (x,y) 的权重，b_i 表示第 i 个输出节点对应的偏置项参数，那么单位矩阵中的第 i 个节点的取值 $a(i)$ 为：

$$a(i) = f\left(\sum_{x=1}^{3}\sum_{y=1}^{3} c_{x,y} \times wi_{x,y} + b_i\right) \qquad (1)$$

式中：$c_{x,y}$ 为过滤器中节点 (x,y) 的取值；f 为激活函数。所有 $a(i)$ 组成的单位向量就是卷积层所得出的特征图，将其作为池化层的输入。

池化层：池化层的汇合操作能够产生降维的效果，减小计算量和参数的个数，同时防止过拟合的发生。

融合层：将 3 个池化层所得的特征进行拼接，融合成一个对文本向量来说更具有代表性的向量。

全链接层：通过在融合层之后加入隐含层和最后的 softmax 层，来充当一个分类器，对文本进行最终的分类。

为了测试 TextCNN 模型在数据集上的表现，实验数据集选取《乱世王者》2019 年 5 月聊天文本信息，分别采用朴素贝叶斯、CNN、TextCNN 三种模型对数据集进行分类，实验步骤为：

1）先对短文本语料进行标注，并进行预处理，执行数据清洗、分词、去停用词等操作；

2）用已训练好的（中文）Word2Vec 模型对分词结果进行向量化；

3）利用朴素贝叶斯、CNN、TextCNN 三种不同模型对数据集进行分类，并计算其准确率。

表 1 为《乱世王者》2019 年 5 月聊天文本信息的分类模型对比结果，其中数据集 1 包含训练样本 14 792 条、测试样本 2 324 条，类别数设为 15；数据集 2 包含训练样本 11 487 条、测试样本 1 794 条，类别数设为 5。数据预处理基于 Python 的 SKLearn 库实现，模型训练和验证基于 TensorFlow 实现。

表 1　文本分类模型对比结果

Tab. 1　Comparison results of text classification models

数据来源	分类模型	训练集样本数/条	测试集样本数/条	类别数	准确率/%
数据集 1	朴素贝叶斯	14 792	2 324	15	65.92
	CNN	14 792	2 324	15	66.17
	TextCNN	14 792	2 324	15	69.89
数据集 2	朴素贝叶斯	11 487	1 794	5	70.56
	CNN	11 487	1 794	5	72.34
	TextCNN	11 487	1 794	5	75.76

由表 1 可知，TextCNN 文本分类系统的测试准确率明显高于朴素贝叶斯和 CNN 文本分类系统。该结果表明，在社交类网游的短文本语境中，TextCNN文本分类系统具有显著优势。

4　结　语

本文结合业务实际，分析了大型社交类网游中网络敏感信息挖掘的常见问题。结合区块链技术的分布式记账方法、去中心化特性，改进了深度学习算法，提出了区块链模式下的网络敏感信息挖掘模型，并将数据层面和控制层面解耦，其中数据层面分类采用卷积神经网络进行特征提取及文本分类。实验结果表明，区块链机制下的网络敏感信息挖掘模型具有较强的安全防误判能力、快速高效的点对点识别机制，能够有效发掘并建立网游中敏感信息的词典，同时保持高效精准的特性。在区块链技术架构下研发精准、高效的网游舆情防控体系，可为网络安全提供事前、事中、事后全过程的舆情数据辨识、处理、溯源，具有广泛的社会需求、较高的技术可行性和良好的应用前景；同时，也为后续公安大数据网络敏感信息的挖掘提供了借鉴。

参考文献：

[1] 中国互联网络信息中心. 中国互联网络发展状况统计报告[R]. 北京：互联网络信息中心，2020.

[2] 张庆庆. 基于机器学习的文本情感分类研究[D]. 西安：西北工业大学，2016.

ZHANG Qingqing. Research on text sentiment classifi-

cation based on machine learning [D]. Xi'an: Northwestern Polytechnical University, 2016.

[3] 闫琰. 基于深度学习的文本表示与分类方法研究[D]. 北京:北京科技大学,2016.
YAN Yan. Text representation and clssification with deep learning [D]. Beijing: University of Science and Technology Beijing, 2016.

[4] 刘婷婷,朱文东,刘广一. 基于深度学习的文本分类研究进展[J]. 电力信息与通信技术,2018,16(3):1-7.
LIU Tingting, ZHU Wendong, LIU Guangyi. Advances in deep learning based text classification[J]. Electric Power Information and Communication Technology, 2018, 16(3):1-7.

[5] ZHAO Weijie. Blockchain technology: development and prospects [J]. National Science Review, 2019, 6 (2): 193-197.

[6] ZHENG Zibin, XIE Shaoan, DAI Hongning, et al. Blockchain challenges and opportunities: a survey[J]. International Journal of Web and Grid Services, 2018, 14(4):352-375.

[7] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and smart contracts for the internet of things [J]. IEEE Access, 2016(4):2292-2303.

[8] 宾晟,孙更新,周双. 基于区块链技术的社交网络中舆情传播模型[J]. 应用科学学报,2019,37(2):191-202.
BIN Sheng, SUN Gengxin, ZHOU Shuang. Public opinion propagation model in social network based on blockchain [J] Journal of Applied Sciences, 2019, 37 (2):191-202.

[9] 贾盼斗,尹春华. 区块链社交网络信息传播特征及规律研究[J]. 情报科学,2021,39(1):35-40, 47.
JIA Pandou, YIN Chunhua. Research on characteristics and rules of information transmission in blockchain social network [J]. Information Science, 2021, 39(1):35-40, 47.

[10] 曾海泉,李荣陆,胡运发. 基于语义分析的倾向性文本过滤[J]. 通信学报,2004,25(7):78-85.
ZENG Haiquan, LI Ronglu, HU Yunfa. Polarity text filtering based on semantic analysis [J]. Journal on Communications, 2004, 25(7):78-85.

[11] SAMUEL J G, DAVID M B. A tutorial on Bayesian nonparametric models [J]. Journal of Mathematical Psychology, 2012, 56 (1):1-30.

[12] LI Zhiyu, ZHANG Junfeng, HU Shousong. Incremental support vector machine algorithm based on multi-kernel learning [J]. Journal of Systems Engineering and Electronics, 2011, 22(4):702-706.

[13] SHEN Furao, OUYANG Q B, KASAI W, et al. A general associative memory based on self-organizing incremental neural network [J]. Neurocomputing, 2013, 104:57-71

[14] LEE P Y, HUI S C, FONG A C M. Neural networks for web content filtering [J]. IEEE Intelligent Systems, 2002, 17(5):48-57.

[15] 李静元,范祥辉,王颖. 基于区块链的共享经济隐私保护机制的设计[J]. 计算机应用与软件,2019,36(1):296-301.
LI Jingyuan, FAN Xianghui, WANG Ying. Design of sharing economy privacy protection mechanism based on blockchain [J]. Computer Applications and Software, 2019, 36(1):296-301.

[16] 赵阔,邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. 信息网络安全,2017(5):1-6.
ZHAO Kuo, XING Yongheng. Security survey of internet of things driven by blockchain technology [J]. Netinfo Security, 2017(5):1-6.

[17] 李志杰,耿朝阳,宋鹏. LSTM-TextCNN联合模型的短文本分类研究[J]. 西安工业大学学报,2020,40(3):299-304.
LI Zhijie, GENG Chaoyang, SONG Peng. Research on short text classification based on joint LSTM-TextCNN model[J]. Journal of Xi'an Technological University, 2020, 40(3):299-304.

(责任编辑 周 蓓)