文章编号:1671-4598(2021)05-0059-05 DOI:10.16526/j.cnki.11—4762/tp.2021.05.012 中图分类号:TP393 文献标识码:A

基于区块链技术的网络安全漏洞检测系统设计

熊 璟
(上海市网络技术综合应用研究所,上海 200335)

摘要:为解决传统网络安全漏洞扫描受限,导致网络应用环境的安全性承载能力较差的问题,设计基于区块链技术的网络安全漏洞检测系统;利用网络爬虫模块抓取任务管理模块所需的待检测信息参量,按照漏洞数据所属的具体类别,将其分别反馈至XSS检测模块、SQL检测模块与CSRF检测模块之中;在此基础上,定义区块信息的实际交易格式,联合各项智能化合约,实现对系统功能需求的定向化分析,并完成相关用例图的构建;通过上述软、硬件设备基础,完成基于区块链技术的网络安全漏洞检测系统设计;对比实验结果显示,与C/S型网络漏洞检测系统相比,基于区块链技术检测系统的安全性等级划分条件更加细致,扫描web漏洞覆盖范围也更为广泛,有助于网络应用环境安全性承载能力的稳定提升。

关键词:区块链技术;网络安全;漏洞检测;网络爬虫;注入漏洞;交易格式;智能合约;功能需求

Design of Network Security Vulnerability Detection System Based on Block Chain Technology

Xiong Lu
(Shanghai Institute for Integrated Application of Network Technology, ShangHai 200335, China)

Abstract: In order to solve the problem that traditional network security vulnerability scanning is limited, resulting in poor security carrying capacity of network application environment, a network security vulnerability detection system based on blockchain technology is designed. The crawler module is used to capture the information parameters needed by the task management module, and the vulnerability data are fed back to XSS detection module, SQL detection module and CSRF detection module according to the specific categories of vulnerability data. On this basis, it defines the actual transaction format of block information, combines various intelligent contracts, realizes the directional analysis of system functional requirements, and completes the construction of relevant use case diagrams. Through the above-mentioned software and hardware equipment foundation, the design of network security vulnerability detection system based on blockchain technology is completed. The experimental results show that compared with C/S network vulnerability detection system, the security classification conditions of the detection system based on blockchain technology are more detailed, and the coverage of scanning web vulnerabilities is more extensive, which is conducive to the stable improvement of network application environment security carrying capacity.

Keywords: block chain technology; network security; vulnerability detection; web crawler; injection vulnerability; transaction format; smart contracts; functional requirements

0 引言

区块链技术是加密算法、分布式数据存储、共识机制、点对点传输等计算机处理手段的新型应用模式。区块链的实用本质相当于一个完整的去中心化型数据库,作为最底层的比特流处理技术,每一个数据块组织都可与一串独立的编译密码保持定向化关联关系,且所有网络交易信息都必须记录于数据块存储结构之中,当核心处理主机确定验证信息的有效性后,相关下级设备元件中才会生成全新的区块应用组织[1-2]。所谓公有区块链是指任何团体或个人都能进行连接的交易组织,与私有区块链相比,该项结构组织能获得区块主机的直接认证,且所有客户端元件都能参与到链条结构体的共识建交过程中。

在计算机网络执行环境中,随着已插入web漏洞数量的增加,外界环境的安全性承载能力会出现明显的下降。为避免上述情况的发生,传统C/S型网络漏洞检测系统针对拓扑遍历网页进行专项编码,再根据缓冲区数据库中已存储信息的实际溢出条件,确定与网络应用环境所匹配的安全性承载范围极值。但此系统在安全性等级划分方面所设定的判别条件过于宽泛,很难实现对web漏洞节点的细致化扫描。为解决此问题,设计基于区块链技术的网络安全漏洞检测系统,在网络爬虫模块、任务管理模块等硬件执行设备的支持下,按需定义区块链组织的实际交易格式,

收稿日期:2020-10-19; **修回日期**:2020-11-12。
作者简介:熊 璟(1986-),男,湖北孝感人,硕士,工程师,主要从事网络安全、网络安全等级保护方向的研究。
引用格式:熊 璟.基于区块链技术的网络安全漏洞检测系统设计[J].计算机测量与控制,2021,29(5):59-63.

从而实现对系统功能需求的精确化分析。

1 网络安全漏洞检测系统模块设计

网络安全漏洞检测系统的硬件执行环境由网络爬虫模块、任务管理模块、相关检测模块 3 类应用元件共同组成，具体搭建方法如下。

1.1 网络爬虫模块

网络爬虫模块是网络安全漏洞检测模块的搭建基础，其执行精度及实施效率直接影响系统最终的漏洞扫描结果精度值。在进行区块链网页抓取时，网络爬虫模块的应用主要遵循最佳优先、广度优先、深度优先三项处置策略。所谓最佳优先是指所有已访问 URL 权限都必须存储于检测信息提取模块之中，在执行网页信息检测时，已爬行 URL 种子库可直接调取这些数据参量，从而避免非相关信息对网络安全漏洞排列顺序的影响[3]。广度优先是指网络安全漏洞检测系统必须按照既定搜索策略，实施对数据参量的扫描与处理，从而使得未爬行 URL 种子库可借助检测页面直接与系统提取模块相连，实现 对系统广度检测条件的无限扩张。深度优先是指网络爬虫模块必须在 URL 权限的作用下，直接与 Internet 区块链相连，当所有信息参量完全转存至漏洞数据存储信息库后，检测信息提取模块才会停止对数据信息的转存与录入，从而实现对待扫描 web 漏洞覆盖范围的无限扩张[4]。

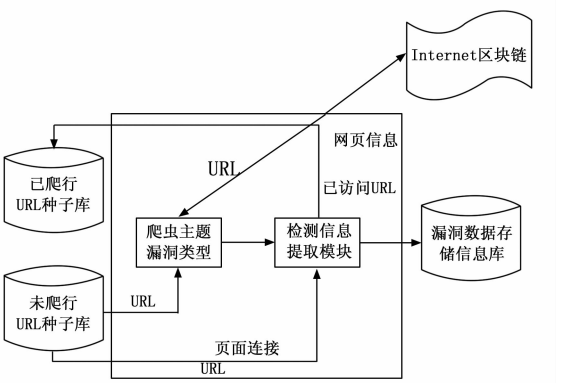

图 1 网络爬虫模块结构图

1.2 任务管理模块

任务管理模块的执行功能包括对网络安全漏洞检测任务的开始、排序、添加、编辑、删除、停止等多个处理部分。当区块链用户点击任务管理模块后，系统检测界面会自动跳转至任务管理器显示列表，其中包含 CPU、内存、硬盘、WLAN、蓝牙、以太网等多个任务操作选项。其中，CPU 任务可显示安全漏洞检测系统的当前网络布施形式，通常情况下，该元件结构体的平均占用率越低，系统所表现出的检测运行速率也就越快，反之则会造成严重的系统卡顿现象[5]。内存任务表现了检测系统的现有运行状态，若待扫描的网络安全漏洞总数值水平过高，则会造成内存占用数值的持续上涨，最终使区块链网络陷入相对复杂的执行应用状态。硬盘状态能够描述系统所承载的网络安全漏洞检测任务的具体数值情况，若该项数值指标的表现数值过大，则会导致系统检测精准性的持续下降[6]。WLAN、蓝牙、以太网 3 类任务指令并不能独立存在，一般情况下，三者总是处于相同的应用连接状态，能够反映系统检测指令的实际执行强度。

1.3 XSS 漏洞检测模块

XSS 漏洞检测模块可直接从数据库 t－urls 表中读取与网络爬虫相关的安全漏洞检测字符串参数，并利用这些数据信息，构造全新的待检测 URL 队列形式，从而读取 XSS 漏洞载荷中可被替换的查询字符串定义值，也就是 XSS 漏洞检测代码，但这些信息参量却只能保存在 xsspayload.txt 区块链文件之中。在利用爬虫模块的提取目标保持不变时，XSS 漏洞检测模块中的区块链网址与数据存储表单也始终保持不变。根据所获取网络完全漏洞数据形式的不同，XSS 漏洞检测模块的源码编译行为可在 GET 或与 POST 型之间来回变换，直至系统应用主机中生成唯一的漏洞数据检测结果[7-8]。在区块链主机的支持下，若安全漏洞数据的响应状态码保持为 2XX 形式，则表示目标网络中不存在明显的 XSS 型漏洞；若安全漏洞数据的响应状态码为 2XX 形式，且网络服务器中会随之生成一系列的 HTML 文档，则表示目标网络中存在明显的 XSS 型漏洞。根据上述信息检测结果，与区块链漏洞表进行对比，如果不存在数据冲突行为，则可将判别结果直接反馈至系统检测主机之中。

表 1 XSS 型漏洞数据检测原理

表单类型	数据库 t－urls 表	源码编译行为	POST 型、GET 型
信息参量	与安全漏洞相关的字符串参数	状态码	2XX 形式——不存在明显的 XSS 型漏洞
检测队列形式	URL 队列		
区块链文件名称	xsspayload.txt		2XX 形式(HTML 文档)——存在明显的 XSS 型漏洞
存储目标	区块链网址、数据表单		

1.4 SQL 注入漏洞检测模块

SQL 注入漏洞检测模块采用经典的 and 搭建方法，即“and 1 命名代表网络安全漏洞数据的输入节点”、“and 2 命名代表区块链组织的射入节点”。出于服务连续性考虑，and 1 命名只能定义特殊的字符连接形式，且在网络爬虫模块的调度下，若 CPU 任务指令的承载水平不断提升，则该类节点的最终表现形式也会逐渐发生改变，直至其中通过的网络安全漏洞信息总量能够完全满足系统主机的核心检测需求[9]。and 2 命名可定义与网络安全漏洞数据相关的特征码参量，随着任务管理模块内已运行信息指令总量的提升，内存系数指标开始不断变化，当该数值参量的表现形式逐渐趋于稳定时，系统检测主机即可判定 SQL 型信息漏洞已注入区块链应用环境中[10]。与 XSS 漏洞检测模块不同的是，SQL 注入漏洞检测模块可同时面对多个网络安全漏

洞数据的攻击行为，且能够跟随网络爬虫模块的执行变化行为，更改与区块链组织相关的信息输入控制指令。

表 2　SQL 型注入漏洞数据检测原理

分类依据	and 1 命名	and 2 命名
字符形式	特殊的字符连接形式	与网络安全漏洞数据相关的特征码参量
参与调度模块类型	网络爬虫模块	网络爬虫模块、任务管理模块
节点连接状态	由稳定连接转变为输入性应用连，GDEMBGWGWLLW-LAWRRGL,,LLLRM,R,N 接	更改已运行信息检测指令的执行状态
执行结果	满足系统主 V 机”}va 对于网络安全漏洞数据的实际检测需求	判定 SQL 型信息漏洞是否注入区块链应用环境中

1.5　CSRF 漏洞检测模块

CSRF 型网络安全漏洞的物理攻击能力相对较强，可直接作用于系统网络爬虫模块与任务管理模块，在 Csrftester 应用软件的作用下，该模块可屏蔽掉一切不必要的区块链连接行为，从而使核心控制主机的检测实施能力得到有效促进。Csrftester 软件可面对单项网络安全漏洞数据进行信息抓取，再按照误报率由高至低的排列形式，剔除其中的不必要信息连接参量，降低漏洞数据对于系统检测主机的核心攻击强度[11]。由于 CSRF 型漏洞检测技术的应用行为相对较为完善，该模块可直接爬取区块链组织内的网络安全信息条例，再通过分级定义 form1、form2 的方式，按需满足检测主机的实际处置权限，当数据库中暂存的网络安全漏洞数据总量不再发生改变时，模块可直接认定 CSRF 型漏洞已完成对区块链网络的入侵性攻击。

表 3　CSRF 型漏洞数据检测原理

分类依据	form1	form2
应用软件名称	Csrftester 应用软件	
网络安全漏洞数据应用类型	单项漏洞数据	单项或多项漏洞数据
已抓取漏洞数据的排列形式	由高误报率排列至低误报率	
联合模块名称	网络爬虫模块	网络爬虫模块、任务管理模块
检测执行结果	数据库中暂存的网络安全漏洞数据趋于稳定后，核心主机判定 CSRF 型漏洞已完成对区块链网络的入侵	

2　基于区块链技术的漏洞检测系统需求分析

在网络安全漏洞检测系统应用模块的支持下，按照区块交易格式定义、区块链智能合约连接、系统功能需求分析、用例图构建的处理流程，实现基于区块链技术网络安全漏洞检测系统的顺利应用。

2.1　区块交易格式

系统核心检测主机需要将任务管理模块的连接请求封装成区块交易的形式，再借助各级输出信道，将这些数据包信息发送给网络客户端节点，具体交易字段的设计格式如下：

1）from：区块链 from 交易是一个长度为 20 字节的目标检测地址，能够标识交易请求初始发起点的地址信息。

2）to：区块链 to 交易也是一个长度为 20 字节的目标检测地址，能够标识交易接收节点所处的地址信息，但若系统内网络安全漏洞数据的检测指令需要智能合约的配合，则此地址可以非填写状态存在[12]。

3）gas：区块链 gas 交易是隶属于 bigInteger 数据范畴的信息检测行为，其标识处理过程能够为系统检测指令提供可直接消耗的网络安全漏洞数据，并通过币值兑换的方式，得到准确的数据检测结果，当交易结束时，未被消耗的 gas 会直接退回原始发起节点，从而弥补区块链网络中或缺的物理信息参量。

4）gasPrice：区块链 gasPrice 交易也是隶属于 bigInteger 数据范畴的信息检测行为，其标识处理过程能够记录区块链网络中的 gas 消耗实值，通常情况下，可用字节兑换率来表示，在网络安全漏洞数据检测实值不超过理想限度条件时，gas 交易的设置量也始终保持为网络默认值。

5）value：区块链 value 交易虽具备 bigInteger 数据的连接能力，但很难直接面对系统数据库中暂存的网络安全漏洞信息，因此只能标识交易过程中发起节点向接收节点传输的信息参量实值。

6）data：区块链 data 交易是满足十六进制编码需求的信息字符串，能够标识该次检测指令中附带网络安全漏洞信息的具体数值量条件，当编译好的智能合约进入区块链网络后，所有满足系统处理需求的安全漏洞数据都可被记录在该次信息交易之中[13]。

7）nonce：区块链 nonce 交易可在暂存的网络安全漏洞数据中做出明确记录标注，当系统检测指令使用相同的交易请求时，最近一次的物理操作便可覆盖前一次的操作记录，从而实现对系统检测结果的实时更新。

2.2　区块链智能合约

智能合约是区块链代码与区块链数据的集合表现形式，可直接部署在网络应用环境中。在漏洞数据制裁者节点与中间方节点的作用下，该合约协议可将区块链事件与区块链通知同时反馈至执行器结构体之中，从而使系统协商者与验证者之间的发送关系得到满足[14-15]。在区块链网络中，系统检测节点始终保持并列分布状态（如图 3 中的 1～5 号节点），而随着事件信息总量的增加，执行器中的强制者与观察者会快速占据系统存储仓库中的智能合约文件，当验证者与协商者之间的数据发送关系不再发生改变时，合约

协议的执行效率也会随之达到最大输出数值。

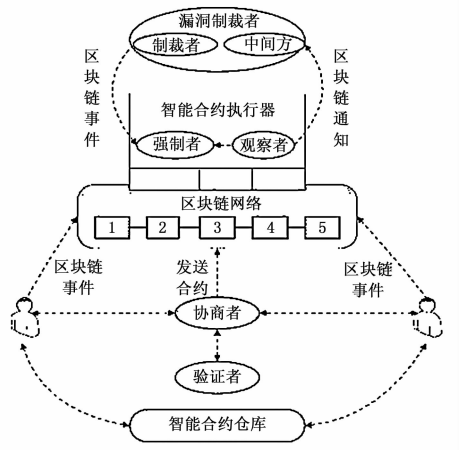

图 2 区块链智能合约生成示意图

2.3 系统功能需求

网络安全漏洞检测系统的功能需求分析包含如下几个执行环节。

1）设备注册功能：

为了实现区块链组织对网络安全漏洞数据的精确检测，各项硬件执行设备在使用之间需要在网络环境中进行注册，且注册后结构体必须保持初始的交互信息筛选能力[16]。

2）设备信息上传：

区块链网络需要频繁地对安全漏洞数据自身所运行的信息进行记录，在此情况下，已接入区块链网络的硬件设备结构体可将自身的定频检测数值直接上传至系统核心检测网络之中。

3）信息获取功能：

系统硬件设备元件想要获取网络安全漏洞信息首先需要对检测主机进行请求，经过既定权限验证处理后，若数据参量满足相应的权限检测条件，区块链智能合约才能捕获到想要获取的信息数据[17]。

2.4 系统用例图

用例分析是网络安全漏洞检测系统设计的末尾处理环节，在区块链技术的支持下，随接入主机数量的不断增加，执行客户端所负载的任务总量也会持续增长。当区块链主机接入检测网络应用环境后，各项信息文件可在检测客户端的作用下，更改已录入信息的存在形式，并可按照既定序列条件对其进行排列处理，待查询需求得到核心主机的应用批准后，实现对系统检测指令的删除与处置[18-19]。至此，完成各项软硬件执行条件的设置与搭建，在区块链技术的支持下，实现网络安全漏洞检测系统的顺利应用。

3 系统应用与检测分析

为验证区块链技术网络安全漏洞检测系统的实际应用价值，设计对比实验。在区块链网络环境中，统一所有 IP 网关参数，使其在既定执行时间内始终趋于稳定。分别连接多个 Alive 主机，使其与 Windows NT、Solaris、HT 等

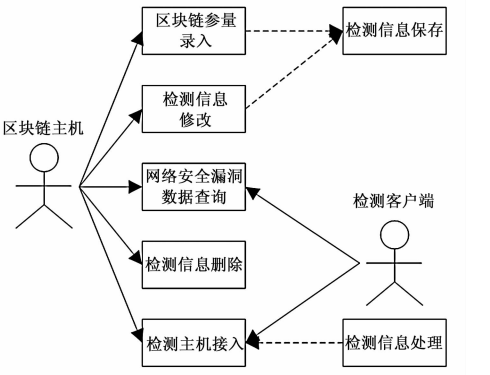

图 3 网络安全漏洞检测系统用例图

多个执行设备的调度行为保持一致，在既定检测模块的作用下，获取多个数据检测结果，以用于后续的实验指标分析与研究，其中实验组主机搭载基于区块链技术的网络安全漏洞检测系统，对照组主机搭载 C/S 型网络漏洞检测系统。

定义 opetare object 代表连贯的网络安全漏洞数据信息、data level 代表单向的网络安全漏洞数据信息、operate type 代表双向的网络安全漏洞数据信息、description 代表非连贯的网络安全漏洞数据信息，在既定实验环境中，分别统计各项指标参量的具体变化情况。

表 4 实验参数设置表

名称	类型	长度	特性
opetare object	连贯的网络安全漏洞数据信息	235	非空
data level	单向的网络安全漏洞数据信息	63	
operate type	双向的网络安全漏洞数据信息	默认	主键，非空，唯一
description	非连贯的网络安全漏洞数据信息	默认	

已知 GYT 指标能反映系统的安全性等级划分能力，通常情况下，前者的指标数值越大，后者的划分能力也就越强，反之则越弱。图 4 记录了实验组、对照组 GYT 指标的具体变化情况。

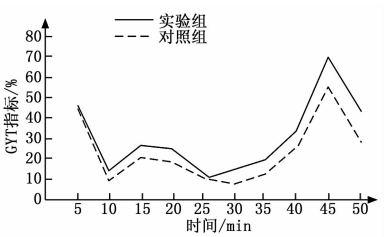

图 4 GYT 指标对比图

分析图 4 可知，在整个实验过程中，实验组、对照组 GYT 指标基本保持较为一致的变化趋势。第 30～45 min 的

实验时间内，实验组、对照组 GYT 指标均呈现不断上升的变化趋势，但前者的最大值达到 69.9%，后者却只能达到 55.6%，二者的极值差达到 14.3%。

KLD 指标可描述系统 web 漏洞的实际扫描覆盖范围，一般情况下，KLD 指标数值越大，系统扫描行为所覆盖的范围也就越宽泛，反之则越狭窄。表 5 记录了实验组、对照组 KLD 指标的具体变化情况。

表 5　KLD 指标对比表

实验时间/(min)	实验组 KLD 指标/(%)	
	1	2
5	63.1	63.5
10	63.3	63.5
15	63.2	63.4
20	63.1	63.4
25	63.0	63.3
30	63.1	63.4
35	63.1	63.4
40	63.1	63.5
实验时间/(min)	对照组 KLD 指标/(%)	
	1	2
5	60.5	60.7
10	60.3	60.4
15	60.0	59.8
20	59.7	59.2
25	59.4	58.9
30	59.2	58.5
35	58.7	58.1
40	58.5	57.6

分析表 5 可知，随着实验时间的增加，实验组 KLD 指标始终保持相对稳定的波动变化趋势，且第二组实验的记录均值结果明显高于第一组。对照组 KLD 指标则始终保持不断下降的变化趋势，且第一组实验的记录均值结果明显高于第二组。选取实验组、对照组的极大值进行对比，可知二者之间的最大差值为 2.8%，实验组均值水平远高于对照组。

综上可知，在既定实验环境下，随着区块链技术网络安全漏洞检测系统的应用，系统所具备的安全性等级划分能力与 web 漏洞的实际扫描覆盖范围均得到不同程度的提升，不仅可解决由 C/S 结构引起的 web 漏洞扫描受限的问题，也能够大幅提升网络应用环境的安全性承载能力。

4　结束语

在网络爬虫模块、任务管理模块等多个硬件执行设备的作用下，基于区块链技术的网络安全漏洞检测系统可根据漏洞数据的具体所属类别对其进行分类处理，且随着区块交易格式的逐渐统一，系统的功能执行需求也得到充分满足。从实用性角度来看，GYT 指标、KLD 指标的快速提升，可在扩大 web 漏洞实际扫描覆盖范围的同时，实现对系统安全性等级划分能力的提升，具备较强的实际应用意义。

参考文献：

[1] 丁　伟，王国成，许爱东，等. 能源区块链的关键技术及信息安全问题研究 [J]. 中国电机工程学报，2018，38 (4)：1026 - 1034.

[2] 杨　敏，张仕斌，张　航，等. 异构联盟系统中基于二层区块链的用户信任协商模型 [J]. 应用科学学报，2019，37 (2)：98 - 106.

[3] 董禹龙，杨连贺，马　欣. 主动获取式的分布式网络爬虫集群方法研究 [J]. 计算机科学，2018，45 (z1)：428 - 432.

[4] 刘爱琴，王友林，尚　珊. 基于爬虫技术的关键词关联推荐算法优化与实现 [J]. 情报理论与实践，2018，41 (4)：134 - 138.

[5] 连云龙，张子轩，黎树明，等. 多机器人系统任务分配及编队控制研究 [J]. 电子设计工程，2019，27 (18)：20 - 23.

[6] 李海伟，潘江江，徐海运，等. 基于耗能最小算法的飞行器任务管理方法 [J]. 电源技术，2018，42 (9)：1372 - 1373.

[7] 夏志坚，彭国军，胡鸿富. 基于权限验证图的 Web 应用访问控制漏洞检测 [J]. 计算机工程与应用，2018，54 (12)：63 - 68.

[8] 靖二霞，应凌云，路晔绵，等. 基于 Dalvik 寄存器污点分析的 Android 漏洞检测方法 [J]. 计算机应用研究，2018，35 (3)：916 - 921.

[9] 潘秋红，崔展齐，王林章. Android 应用中 SQL 注入漏洞静态检测方法 [J]. 计算机科学与探索，2018，12 (8)：1225 - 1237.

[10] 尹中旭，张连成. 一种数据流相关过滤器自动插入的注入入侵避免方案 [J]. 计算机科学，2019，46 (1)：201 - 205.

[11] 孙骁永，王　伟，霍　玮，等. 动态事件序列制导的 Android 应用漏洞验证技术 [J]. 计算机工程与应用，2018，54 (6)：86 - 94.

[12] 龚钢军，王慧娟，张　桐，等. 基于区块链的电力现货交易市场研究 [J]. 中国电机工程学报，2018，38 (23)：6955 - 6966.

[13] 尤　瑶，孔兰菊，肖宗水，等. 一种支持区块链交易溯源的混合索引机制 [J]. 计算机集成制造系统，2019，25 (4)：192 - 198.

[14] 盛念祖，李　芳，李晓风，等. 基于区块链智能合约的物联网数据资产化方法 [J]. 浙江大学学报 (工学版)，2018，52 (11)：2150 - 2158.

[15] 徐美强，高志远，王　伟，等. 基于区块链技术的智能变电站配置版本管理 [J]. 电力系统保护与控制，2020，48 (2)：60 - 67.

[16] 施亚虎，石海龙，崔　莉. EasiDARM：基于分布式的物联网设备自适应注册方法 [J]. 计算机研究与发展，2019，56 (3)：453 - 466.

[17] 魏　晨，龚　龑，鲁　啸，等. 基于语义 Web 的多功能情报信息自适应检索技术 [J]. 科学技术与工程，2019，19 (5)：216 - 221.

[18] 章　骞，关于消防计算机网络信息安全管理的探讨 [J]. 养生保健指南，2018 (33)：194.

[19] 窦　磊，张亚东，李　耀，等. 基于场景法的列控系统等级转换功能测试用例设计 [J]. 铁道标准设计，2019，63 (7)：141 - 145.