

基于国产平台的可视化分析诊断系统

李志刚,刘自强,张 辉

(中国电子科技集团公司第五十二研究所,浙江 杭州 311100)

摘 要:随着国产平台在各行业信息系统中的推广使用,其系统规模及复杂度日益提高,可靠运行面临较大挑战。针对面临的问题及挑战,从故障快速定位排查入手,对国产平台在运行维护和故障诊断排查中存在的问题进行分析,设计一种集日志分析、智能诊断和可视化监测等技术相融合的可视化分析诊断系统。基于日志分析可从大量日志噪声数据中自动识别关键信息并进行异常检测;通过智能推理诊断,可实现在错综复杂环境中故障的快速诊断及排查;通过可视化监测,以用户易懂的方式可视化展现众多监测数据,可提高用户对系统运行状态的理解和把控。该系统在传统监控的基础上,通过融入日志聚类异常检测技术、专家推理诊断技术和数据可视化技术,可有效提高国产平台的故障排查速度和可靠运行水平。

关键词:日志解析;异常检测;知识管理;推理诊断;可视化监测;分层架构

中图分类号:TP302

文献标识码:A

文章编号:1673-629X(2022)03-0096-06

doi:10.3969/j.issn.1673-629X.2022.03.016

Visual Analysis and Diagnosis System Based on Domestic Platform

LI Zhi-gang, LIU Zi-qiang, ZHANG Hui

(52nd Research Institute of China Electronics Technology Group Corporation, Hangzhou 311100, China)

Abstract: With the popularization and application of domestic platform in various industry information systems, the scale and complexity of the system are increasing, and the reliable operation is facing great challenges. Aiming at the problems and challenges, we analyze the problems existing in the operation and maintenance and fault diagnosis of domestic platforms from the perspective of rapid fault location and troubleshooting, and design a visual analysis and diagnosis system integrating log analysis, intelligent diagnosis and visual monitoring. Based on log analysis, key information can be automatically identified from a large number of log data and abnormal detection can be carried out. Through intelligent reasoning diagnosis, fault diagnosis and troubleshooting in complex environment can be realized quickly. Through visual monitoring, a large number of monitoring data can be visualized in a way that is easy for users to understand, which can improve the overall control of system operation state by users. On the basis of traditional monitoring, the system can effectively improve the troubleshooting speed and reliable operation level of domestic platform by integrating log clustering anomaly detection technology, expert reasoning diagnosis technology and data visualization technology.

Key words: log parsing; exception detection; knowledge management; reasoning diagnosis; visual monitoring; hierarchical architecture

0 引言

随着国内信息化领域自主化和国产化战略的稳步推进,在各行业信息系统中已大力推动国产平台部署使用。在此情况下,国产平台直接关系到国内信息系统自主化进展,其可靠稳定运行至关重要。目前国产平台系统规模及复杂度越来越高,国产平台的可靠运行面临着越来越大的挑战。在国产平台使用过程中,故障快速定位排查是保障平台可靠运行的有效手段。

该文设计了一种集日志分析、智能诊断和可视化监测等多种技术的可视化分析诊断系统,可有效提高

国产平台的故障排查速度和可靠运行水平。

1 概述

在国产平台的运行维护和故障诊断排查中,存在以下挑战和问题^[1]:

(1)系统日志和应用日志等记录着系统和业务应用运行期间的详细运行时信息,可被用作系统异常检测的主要数据源。对日志进行分析,不仅可以了解到国产平台中软硬件的运行状况,还可了解报错日志的源头,判断错误是由应用引起的还是系统引起的,从而

及时进行故障恢复,减少停机时间。

但系统中的日志存放分散、数据量巨大,且日志的格式和含义往往不明,管理人员往往难以快速从大量日志噪声数据中手动识别关键信息以进行异常检测。

(2)目前国产平台日趋复杂,多个应用软件间及数据间的关系更加紧密,影响其稳定可靠运行的因素众多。硬件因素上涉及到计算、存储、交换、电源以及其他专用硬件等;软件因素上涉及到操作系统、驱动、系统软件、中间件、数据库、应用软件等;同时由于硬件对环境依赖、软硬件间依赖、应用系统间依赖以及数据间依赖等关联依赖,使问题更加错综复杂。

在此情况下,当国产平台系统出现故障时,故障从何查起、需要查看哪些因素,以及如何快速诊断及排查故障变得愈加困难。

(3)国产平台中可监测数据众多,包括传感数据(电压/电流/温度等)、系统静态信息(CPU/内存/存储/网络配置信息等)、系统动态信息(CPU占用率/内存占用率/网络流量等)、告警信息、故障信息、日志信息和应用信息等,并且所有监测的各种类型的数据都有其相应的意义和作用,不可或缺。

在此情况下,如何一目了然地以用户易理解的方式可视化展现众多监测数据,如何提高用户对数据理解和处理效率变得非常重要^[2]。

针对以上所述问题,该文设计构建可视化分析诊断系统,通过日志分析、智能诊断和可视化监测技术来解决上述3个问题及挑战。以下将从系统架构、日志分析、智能诊断和可视化监测等方面对该系统进行论述。

2 系统架构

基于国产平台的可视化分析诊断系统以监测数据为中心,对监测数据进行全生命周期管理分析,包括数据监控采集、数据存储管理及数据分析和可视化应用等,结合国产平台硬件及分层设计思想,可视化分析诊断系统架构设计^[3]如图1所示。

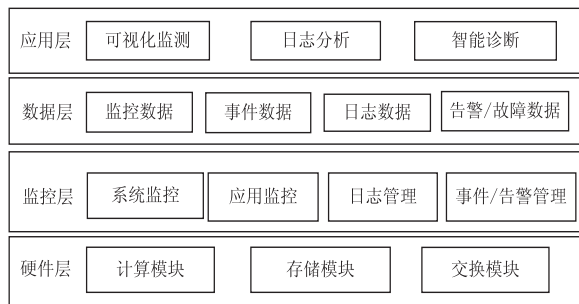


图1 可视化分析诊断系统架构示意图

由图1可知,可视化分析诊断系统采用分层架构设计,其中监控层实现监测数据的监控采集;数据层实

现监测数据的存储管理;应用层实现对监测数据的分析及可视化,各层间分工明确,相互独立。

(1)硬件层基于国产基础软硬件构建,主要包括计算模块、交换模块和存储模块等。其中计算模块采用国产飞腾 FT1500A/16 处理器和银河麒麟操作系统,为系统业务应用提供软硬件运行环境;交换模块采用国产盛科交换芯片,实现以太网数据的交换转发;存储模块采用国产 M.2 电子盘组合提供 TB 级大容量存储。

(2)监控层主要实现对平台系统、应用、日志、事件/告警等进行监控。包括对各模块资源使用率、系统负载、进程运行情况等进行监控以及对应用进程的资源占用情况进行跟踪监控;日志管理实现系统日志、服务日志、应用日志等内容的搜集。事件/告警管理则是在以上监控行为发生时按规则触发事件/告警等事项。

(3)数据层主要是存储并管理通过监控层采集汇总的状态数据、事件数据、日志数据、告警/故障数据等。

(4)应用层实现对数据的分析利用及可视化应用,主要实现日志分析、智能诊断和可视化监测功能。

3 日志分析

3.1 概述

近年来,随着大数据、机器学习、深度学习等技术的兴起,科研技术人员逐步将此类技术应用于日志分析中,如李飞飞等人^[4]的系统事件日志解析,Wang Mengying^[5]、Amey Agrawal^[6]、Liu Xiaojian^[7]、Rakesh Bahadur Yadav^[8]等基于日志进行的分析及异常检测研究等,基于日志进行系统问题分析的工作取得了较大进展。

日志分析主要包括日志解析、特征提取和异常检测三个主要步骤。

(1)日志解析:日志是非结构化的自由形式的文本,通过日志解析,每个日志消息都可以被解析成带有一些特定参数(可变部分)的事件模板(恒定部分)。

(2)特征提取:在日志解析成单独的事件后,进一步将其编码为数字特征向量,以便应用机器学习模型。首先使用窗口技术将原始日志分割成一组日志序列,然后,对于每个日志序列,生成一个事件计数向量,表示每个事件的发生次数。

(3)异常检测:可将特征提取阶段生成的一个个事件计数向量馈送给机器学习模型进行训练,从而生成异常检测模型,所构建的模型可用于识别新进入日志序列是否异常。

3.2 日志解析

日志是由固定部分和可变部分组成的纯文本,开

发人员在源代码中预先定义了常量部分,变量部分通常是动态生成的。日志解析的目的是将常量部分与变量部分分开,并形成日志事件,如下示例的“StopRecordProc ullChannel is <*>, ulChannelNum is <*>”。

如图 2 所示,日志分析的第一步就是将无结构的日志文本转化成有结构的数据。每个日志信息通过时间戳、日志级别和日志内容等记录一个具体的系统行为。日志内容是由不变的字符串和可变的值构成的。不变的部分是需提取的日志模板,可变的值代表着动态的运行信息。通过日志数据结构化可把每一个日志信息转化成具体的模板和参数,<*>就代表着每一个参数的位置,如图 2 中 EVENT TEMPLATE 所示。

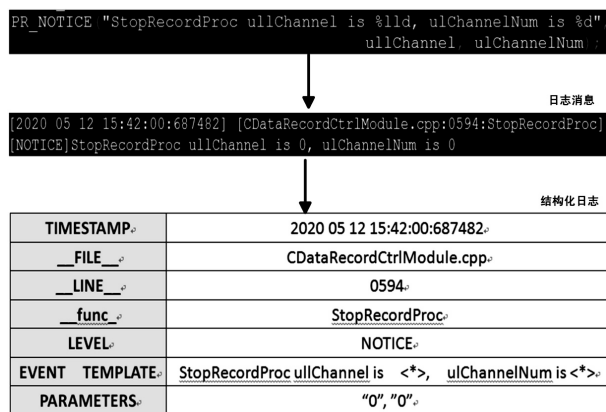


图 2 日志数据结构化示意图

3.3 特征提取

该步骤的主要目的是从日志事件中提取有价值的特征,这些特征可以被输入异常检测模型。特征提取的输入是日志数据以及日志解析中生成的日志事件,输出是事件计数向量。

为了提取特征,首先将日志数据分成不同的组,其中每个组代表一个日志序列。可采用窗口技术将日志数据集划分成有限块,同一窗口中发生的日志被视为日志序列^[8]。

目前常用的窗口技术有固定窗口、滑动窗口和会话窗口,考虑到通用性及异常检测的准确性,选择基于滑动窗口的方式对日志数据集进行划分,生成多组日志序列。

在利用窗口技术构建日志序列之后,对每个日志序列,可计算每个日志事件发生次数,形成事件计数向量。例如事件计数向量[0,1,3,0,0,1,0],这意味着在这个日志序列中,事件 2 发生了 1 次,事件 3 发生了 3 次,事件 6 发生了 1 次。

3.4 基于聚类的异常检测

由上可知,日志序列通过特征提取生成事件计数向量,其可作为聚类模型的输入。聚类模型选择 K-

Means 算法来设计实现,其基本思想是先从样本集中随机选取 K 个样本作为簇中心,并计算所有样本与这 K 个簇中心的距离,对于每一个样本,将其划分到与其距离最近的簇中心所在的类别中,对于新的簇计算各个簇的新的簇中心。

在系统运行期间,日志数据不断产生,通过日志解析和特征提取生成的事件计数向量被一个接一个地添加到异常检测聚类模型中。对于新日志序列的状态,可根据其所生成的事件计数向量,计算它和现有代表向量之间的距离。如果最小距离大于阈值,则日志序列被报告为异常。

4 智能诊断

4.1 概述

近年来随着信息系统的日益复杂,故障定位及诊断难度进一步加大。在此情况下,国内外技术人员在故障快速定位和有效诊断方面投入了较多的研究。如 PHM 技术研究^[9-10]、时序诊断技术研究^[11]、故障预测技术研究^[12]、贝叶斯网络系统^[13]和专家系统研究^[14-15]等。

文中智能诊断采用基于规则的故障诊断专家系统模式,主要由知识库管理模块、推理诊断模块、数据库和人机交互模块等组成,如图 3 所示。

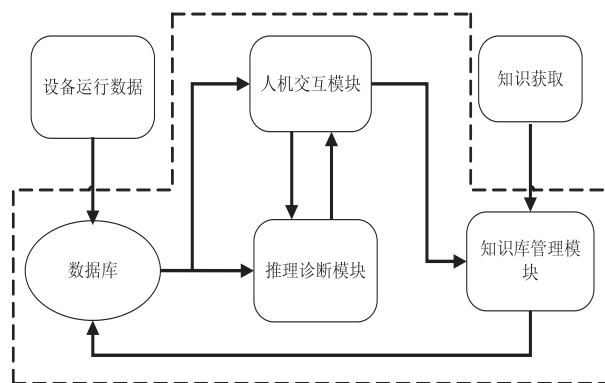


图 3 智能诊断系统各模块交互图

其中:

(1) 数据库主要用于记录存储和管理系统实时监控数据、用户配置阈值信息、系统告警/故障信息、设备诊断专业知识信息以及推理过程中的中间信息与诊断结果等数据。

(2) 知识库管理模块主要用于通过外部获取设备诊断专业知识,处理后形成规则,根据不同设备类型、不同知识类型存入数据库表中,同时具备知识检索、修改、增加、删除等管理功能。

(3) 推理诊断模块作为诊断过程中的核心部分,根据设备触发各告警/故障信息,通过关键词表提取后,选择相关联的数据库表提取规则进行匹配推理,并

得出诊断结果。

(4) 人机交互模块主要用于执行用户下发的诊断指令、返回诊断结果并进行可视化展示,还可通过人机交互模块进行知识录入、修改、删除、查询等。

4.2 诊断流程

系统首先通过可视化的人机交互模块展示出各模块当前运行状态趋势,并实时获取告警系统触发的告警/故障信息列表。用户选择指定告警/故障信息进行诊断分析时,人机交互模块将告警/故障事件发送给推理诊断模块进行推理诊断。

推理诊断模块接收到诊断请求后,根据关键词表对告警/故障信息进行关键词提取,然后采用树状结构将知识库中的规则构建规则集,并与告警/故障信息

关键词进行匹配,得出初步诊断结论,再将得出的结论缓存到内存中,再次进行规则的搜索与匹配,直到缓存的数据不再发生变化为止,得到最终的推理结论,并进行验证,得出诊断结果。

最后推理诊断模块将推理诊断结果推送给人机交互模块进行展示,以便用户或系统管理人员进行维护处理。

4.3 数据库

系统中存储的数据类型分为综合数据库和知识库两类。其中综合数据库主要存储用于监控数据、阈值信息、告警/故障信息等,数据按照不同类型进行分表,主要存储信息如表1所示。

表1 综合数据库信息列表

信息	内容
系统信息	CPU/内存/磁盘使用率、网络信息、进程信息等
传感信息	温度、电压、电流等
阈值信息	CPU使用率阈值、内存使用率阈值、磁盘使用率阈值、温度阈值、电压阈值、电流阈值等
告警/故障信息	CPU异常、内存异常、磁盘异常、网口异常、温度异常、电压异常、电流异常、应用异常、数据异常等

知识库主要存储用于推理诊断的规则信息,其组织结构对推理效率有很大的影响,该系统采用高效分层模式对知识库进行管理分类。根据设备类型分为通用服务器知识库、通信设备知识库、专用设备知识库等若干个子库,再根据监控属性对子知识库进行分表,从而形成具有树状层次结构的知识库。

4.4 知识库管理模块

知识作为故障诊断的理论依据,是智能诊断系统的核心要素之一。知识库中的规则集决定了诊断系统推理的正确性与全面性。知识库的管理主要包括知识获取、知识表达与规则管理三个方面。

(1) 知识获取:操作人员采用与领域技术专家沟通交流或从文献资料中提取的方式获取相关知识,形成规则后编入知识库,并根据系统实际部署和运行状况进行扩充或修正;同时,还可以根据历史诊断结论的验证结果对知识库进行修正。

(2) 知识表达:采用基于确定性规则知识的产生式表示法将知识形成规则,即当某一条规则的条件被满足时,触发规则,然后执行下一步的推理直到给出最终结论^[15]。例如,系统负载过高会导致板卡温度异常升高的知识,通过规则表达如下:

IF 板卡温度过高;
AND 风扇转速正常;
AND 板卡散热正常;

AND 系统CPU占用;

THEN 触发板卡温度异常的原因为系统负载过高。

通过上述规则得出导致板卡温度异常的原因为系统负载过高后,再根据由系统负载相关知识形成的规则进一步推理,最终得出导致板卡温度异常的原因。

(3) 规则管理:采用基于故障树的结构对规则进行组织管理^[15],如图4所示。

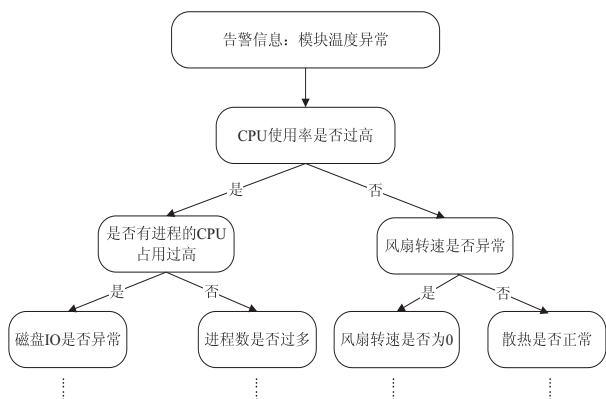


图4 规则推理树结构示例图

当推理诊断模块进行故障诊断时,首先从知识库中查找匹配故障现象的数据库表,然后将表中的规则集加载到内存中,组织形成故障树,并以根节点为故障树的当前节点,根据故障现象逐步判断故障是否满足各子节点规则,并根据各规则的关联关系,逐层递进,

最终得出诊断结论。

4.5 推理诊断模块

推理诊断模块是智能诊断系统中实施问题求解的核心执行模块。其主要任务是通过输入流从人机交互模块中获取告警信息,根据预先保存在配置文件中的关键词表提取关键字后,选择相关联的知识库,并将规则加载到内存,按照程序既定的步骤进行推理诊断,步骤如图 5 所示。

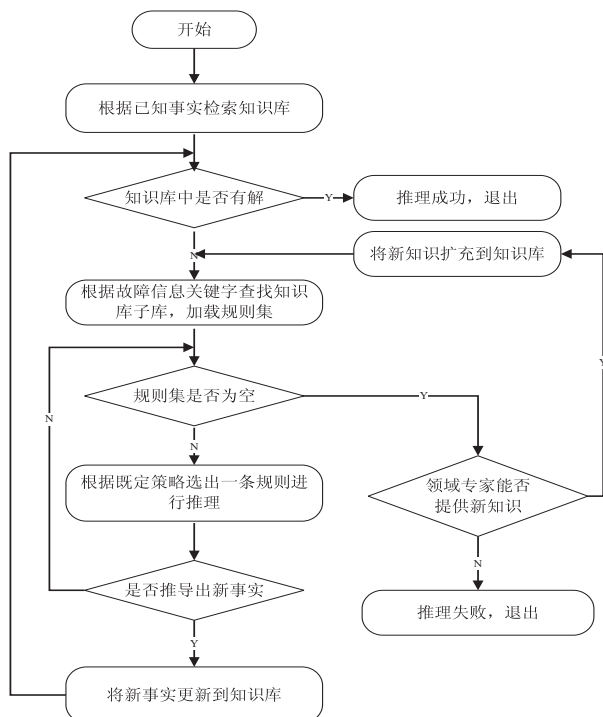


图 5 推理诊断模块诊断流程

5 可视化监测

可视化监测基于数据可视化技术,借助图形化的手段,可以将各种监控数据清晰高效地传达给用户或系统管理人员,以便于用户对设备状态进行管理维护。

数据可视化技术采用图元对数据集中的数据进行表示,数据项中的每个属性以多维数据的形式存储在图元中,然后整合成图像,如柱形图、条形图、饼图、环形图、线图、散点图、面积图、雷达图、K 线图、地图等图表^[16],通过可视化界面进行展示,可实现监测数据多维度分析,提高数据分析效率及直观性。

在可视化监测界面设计时主要遵循以下设计原则^[17]:

(1) 注重用户体验。

无论是风格、元素、配色、文字、交互上还是细节上,可视化界面在设计时需注重用户的视觉体验,让用户一目了然。

(2) 亲密性分组。

在可视化设计时,要表达的内容不能是无序呈现,

这样会给用户造成理解上的混乱。

可视化界面应遵循多数用户所能理解的思维逻辑,将内容分成几部分按顺序一步一步地表达出来。相同部分的内容,彼此相关,应当靠近,放在一起。不同部分的内容,应当明显地隔开。

(3) 对齐。

在版式布局上,任何元素的摆放都可能会影响甚至主导用户的视觉流程。因此,任何元素都不能随意摆放,否则会造成混乱,而混乱会令人不适。

对齐使每个元素都与其他元素建立起某种视觉联系,也可使可视化界面更加清晰、精巧、清爽。

(4) 重复/统一。

在可视化界面中反复使用一些视觉要素,建立上下文之间的联系,增加条理性,保持视觉上的统一。任何视觉元素都可以在同一系统中重复使用,例如颜色、形状、材质、空间关系、线宽、字体、大小和图片等等。

(5) 对比/强调。

在做可视化设计时,初衷是以图文的形式把所要表达的信息清晰地传递给用户,让用户一目了然,尽量不需要太多思考和理解。为了达到这个目的,需强调重点,弱化次要,避免系统中所有的元素看起来重要程度都一样。

(6) 表达力求准确且简洁易懂。

当用户看到可视化界面时,需保证所表达的信息能被用户正确理解。除使用上面几个原则外,还要附加一些辅助信息,例如文字、箭头等。文字的表达,要准确、到位、简洁、易懂,要能引导用户正确地理解图表的意思,不引起任何歧义。

基于以上设计原则,在整个可视化分析诊断系统设计时,可视化监测界面采用扁平化设计风格,界面背景选用深色调,数据部分则采用亮色系,使内容与背景有足够的对比,从而起到弱化背景,聚焦内容的作用。整个界面以极简的线面为主,大量使用色彩饱和度较高的可视化数据图表,实现系统拓扑展示、系统状态及告警展示和日志分析可视化展示等功能。

其中系统拓扑展示界面以实际的硬件架构为原型,结合对应的 CAD 图纸,通过三维立体模型展示各模块位置及拓扑连接关系,场景真实直观,便于用户对整个系统进行监控和管理。同时实现对各个模块的基本信息分别展示。当用户关注点聚焦于单个模块时,界面会将整个系统进行重构,将其他模块虚化展示,突显当前模块的状态结构,实现可视化动态展示该模块负载、网络流量及环境传感等信息。

系统状态及告警展示采用可视化数据大屏形式,通过不同的图元模型对系统监管要素进行多维实时展示,先进行核心数据(如系统负载、故障、告警、统计等

信息)展示,再逐级浏览二三级内容,并隐藏部分细节数据,确保用户聚焦关键数据。当系统监测到设备发生告警或模块的某一指标偏离正常值时,系统会自动将展示界面切换到该模块的最佳查看视角,并自动弹出该模块当前运行参数的概要信息,以便于用户或管理人员进行故障排查。

日志分析可视化则通过图表形式对日志查询及日志聚类分析的结果进行综合展现。针对海量的日志查询结果,界面通过高亮显示标记出关键词组,可以方便用户快速识别关键信息并定位分析。针对日志聚类分析结果,界面支持通过多种图表形式对分析结果进行不同维度的统计展示。

6 结束语

针对国产平台系统规模及复杂度高、故障排查诊断困难、系统可靠运行要求高的情况,提出一种集日志分析、智能诊断和可视化监测等多种技术相融合的可视化分析诊断系统。该系统基于日志分析可从大量零散、非结构化日志文本中自动识别关键信息并进行异常检测;通过知识管理、数据库构建以及推理诊断,可实现在错综复杂环境中故障的快速诊断及排查,通过基于数据可视化技术的多维度监测,以用户易懂的方式可视化展现众多监测数据,可提高用户对系统整体运行状态的理解和把控。

该系统在传统监控的基础上,融入日志聚类异常检测技术、专家推理诊断技术和数据可视化技术,可有效提高国产平台的故障排查速度和可靠运行水平。

参考文献:

- [1] 方 锐. 大数据平台下动车组运维数据可视化系统的设计与实现[D]. 北京:北京交通大学,2017.
- [2] 陈 为,沈则潜,陶煜波. 数据可视化[M]. 北京:电子工业出版社,2013:302-330.
- [3] 贾夫松. 基于 Zabbix 的服务器监控平台的研究[D]. 济南:山东师范大学,2018.
- [4] DU Min, LI Feifei. Spell: streaming parsing of system event logs[C]//IEEE international conference on data mining. Barcelona, Spain; IEEE, 2016: 859-864.
- [5] WANG Mengying, XU Lele, GUO Lili. Anomaly detection of system logs based on natural language processing and deep learning[C]//IEEE 4th international conference on frontiers of signal processing. Poitiers, France; IEEE, 2018: 140-144.
- [6] AGRAWAL A, KARLUPIA R, GUPTA R. Logan: a distributed online log parser[C]//IEEE 35th international conference on data engineering. Macao, China; IEEE, 2019: 1946-1951.
- [7] LIU Xiaojian, ZHU Yi, JI Shengwei. Web log analysis in genealogy system [C]//IEEE international conference on knowledge graph. Nanjing, China; IEEE, 2020: 536-543.
- [8] YADAV R B, KUMAR S P, DHAVALE S V. A survey on log anomaly detection using deep learning[C]//The 8th international conference on reliability, infocom technologies and optimization. Noida, India; IEEE, 2020: 1215-1220.
- [9] 张素明, 赵小卓, 张 翔, 等. 一种通用测试系统故障诊断功能设计[J]. 计算机测量与控制, 2016, 24(7): 10-13.
- [10] 吕 琛, 马 剑, 王自力. PHM 技术国内外发展情况综述[J]. 计算机测量与控制, 2016, 24(9): 1-4.
- [11] 姜 婕, 马 磊. 一种基于时序的状态监控及故障诊断系统[J]. 测控技术, 2020, 39(7): 1-7.
- [12] 李向前. 复杂装备故障预测与健康管理关键技术研究[D]. 北京:北京理工大学, 2014.
- [13] CAI B P, LIU H L, XIE M. A real-time fault diagnosis methodology of complex systems using object-oriented Bayesian networks[J]. Mechanical Systems and Signal Processing, 2016, 80(1): 31-44.
- [14] 张蒙蒙. 基于专家系统的船舶电气设备故障诊断研究[J]. 无线互联科技, 2019(10): 1-2.
- [15] WANG Wei, ZHANG Tao. Research and implementation of fault diagnosis of seed source assembly device based on expert system[C]//The 4th international conference on control science and systems engineering. Wuhan, China; IEEE, 2018: 375-379.
- [16] 宋美娜, 崔丹阳, 鄂海红, 等. 一种通用的数据可视化模型设计与实现[J]. 计算机应用与软件, 2017, 34(9): 38-42.
- [17] 邱南森. 数据之美: 一本书学会可视化设计[M]. 北京: 中国人民大学出版社, 2014: 192-223.