

doi: 10.3969/j.issn.1672-6073.2022.06.012

超大线网标准城轨云及 共享数据平台研究

吴昊¹, 梁樑², 张月坤³, 田可心⁴, 李申⁵, 熊辉⁶

(1. 北京协同创新轨道交通研究院有限公司, 北京 100101; 2. 北京轨道交通路网管理有限公司, 北京 100101;
3. 京投轨道交通科技控股有限公司, 北京 100029; 4. 北京京投亿雅捷交通科技有限公司, 北京 100012;
5. 交控科技股份有限公司, 北京 100070; 6. 北京京投信安科技发展有限公司, 北京 100029)

摘要: 基于《中国城市轨道交通智慧城轨发展纲要》的“1811”布局以及《北京智慧轨道交通发展行动策划方案》, 研究城轨云与大数据的标准化、自主化、多云异构的安全可信云计算平台; 构建城轨业务数据的综合承载、共享、挖掘、治理、质量评估大数据平台体系, 发挥城轨大数据要素的流转、互联、互通效能, 推进城轨业务对大数据要素的深化应用与数据价值提升; 推动智慧城轨发展, 建设“三张网”的标准化、协同化网络纵深防御技术体系, 采用其关键对称与非对称的密码应用技术, 最大化地提升城轨云的安全能力; 研究可复制的、高度可用的云平台运维常态与应急管理体系与机制, 保障城轨云的业务持续性、数据安全性, 以及云平台基础设施运维的集约化。

关键词: 轨道云; 云异构; 大数据采集; 网络安全; 运营与运维

中图分类号: U231

文献标志码: A

文章编号: 1672-6073(2022)06-0069-06

Standard Urban Rail Cloud and Shared Data Platform of a Super-Large Line Network

WU Hao¹, LIANG Liang², ZHANG Yuekun³, TIAN Kexin⁴, LI Shen⁵, XIONG Hui⁶

(1. Beijing Collaborative Innovation Institute of Rail Transit Co., Ltd., Beijing 100101; 2. Beijing Metro Network Administration Co., Ltd., Beijing 100101; 3. BII Railway Transportation Technology Holdings Co., Ltd., Beijing 100029; 4. Beijing BII-ERG Transportation Technology Co., Ltd., Beijing 100112; 5. Traffic Control Technology Co., Ltd., Beijing 100070; 6. BII Information Security Technology Development Co., Ltd., Beijing 100029)

Abstract: Based on the “1811” outline layout for the development of smart urban rail transit in China issued by the China Urban Rail Transit Association and action plan for the development of smart rail transit in Beijing led by Beijing Infrastructure Investment Co., Ltd., and relying on the advantageous resources of “government, industry, university and research” of the Beijing Collaborative Innovation Rail Transit Research Institute Co., Ltd., the standardization, automation, and multi-cloud heterogeneous securement of a trusted cloud computing platform and big data of urban rail is studied. A big data platform system was built to comprehensively carry, share, mine urban rail business data, conduct governance and quality evaluations, provide full play to the circulation, interconnection, and interoperability efficiency of the urban rail big data elements, and promote and improve the further applications of urban rail business to big data elements. Based on this, the development of a smart city rail is promoted, the standardized “three networks” and collaborative network defense in a depth technology system and its key symmetric and asymmetric password application technology is built, and the cloud security capability of urban rail

收稿日期: 2022-07-25 修回日期: 2022-09-07

第一作者: 吴昊, 女, 本科, 教授级高级工程师, 从事轨道交通核心技术及重大装备自主创新及应用研究, wuhao1@bii.com.cn

引用格式: 吴昊, 梁樑, 张月坤, 等. 超大线网标准城轨云及共享数据平台研究[J]. 都市快轨交通, 2022, 35(6): 69–74.

Wu Hao, Liang Liang, Zhang Yuekun, et al. Standard urban rail cloud and shared data platform of a super-large line network[J]. Urban rapid rail transit, 2022, 35(6): 69–74.

is maximized. Finally, replicable and highly available cloud platform operations, normal maintenance, and emergency management system and mechanisms are studied to ensure the business continuity of the urban rail cloud, data security, and the intensive operation and management of the cloud platform infrastructure.

Keywords: orbital cloud; cloud heterogeneity; big data collection; network security; operation and maintenance

1 研究背景

随着我国城市轨道交通从自动化、信息化向智能化、智慧化迈进,以及中国城市轨道交通协会《中国城市轨道交通智慧城轨发展纲要》的颁布,城轨云和大数据已在我国城市轨道交通行业进入大规模建设和应用阶段^[1],建设和运营单位面临诸多核心问题,包括:城轨云方面,存在技术异构、厂商壁垒和价格难以降低的问题;数据交换共享方面,存在标准不一、数据拉通困难、缺失全局视角等问题^[2];安全方面,有待进一步深化落实城轨网络安全技术规范,强化安全保障能力;运维方面,有待摸索建立适用于城轨云和大数据等新技术驱动下的新型管理模式和管理机制。

北京作为超大城市,城市轨道交通线网规模大、

复杂程度高,城轨各专业系统众多,配合和协调组织工作繁琐,上述问题尤为突出。本研究结合北京等超大线网城市现状和需求,以解决当前行业痛点和难题为目标,提出构建城轨云和大数据平台,设计立体全方位的网络安全体系,打造全生命周期的降本增效运维体系,提供可复制、可推广、可迭代的解决方案,在行业内树立标杆,并提供有益的借鉴。

基于《中国城市轨道交通智慧城轨发展纲要》和《北京智慧轨道交通发展行动策划方案》,依托北京协同创新轨道交通研究院有限公司“政产学研用”的优势资源,重点进行城轨云多云管理及异构研究、城轨云大数据共享交换平台技术研究、城轨云网络安全纵深防御体系研究和城轨云运维维护体系与运行管理机制研究,具体架构如图1所示。

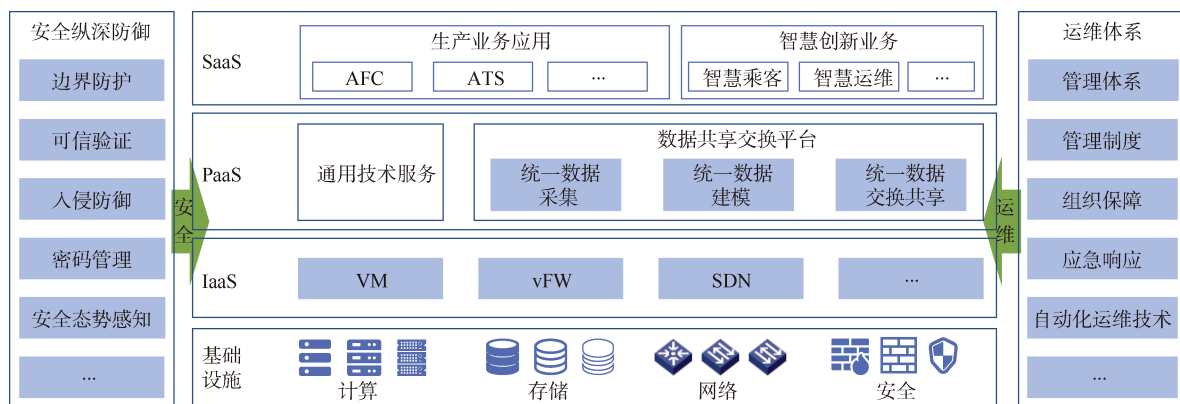


图1 总体架构

Figure 1 Overall research architecture

2 多云管理及异构研究

笔者调研了北京、深圳、广州、武汉等地的城市轨道交通建设情况,提出适用于不同规模城市 and 不同建设方式的云基本架构建议:一是超大线网以及管理集中的城市,适合“一云承载”方案,构建统一的资源池,集中承载线网、线路、车站业务,最大化地实现资源共享,打破管理壁垒^[3];二是多个管理主体或PPP项目的城市,适合线网与线路异构或中心云与边缘云异构方式,不同管理主体根据各自管理范畴内业务上的云诉求独立建设,在多云管理平台实现不同云平台的统一资源监控。

在确定超大线网城市城轨云建设采用“一云承载”

方案的基础上,进一步研究超大线网的云基本架构设计要点,进行“一云承载”的线路接入研究以及“一云承载”的异构研究。

2.1 超大线网云基本架构设计

“一云承载”的关键设计要点包括计算资源池、存储资源池、网络以及容灾设计。

1) 计算资源池设计原则:为实现资源共享,建议优先使用虚拟机、容器资源池,大型商用数据库或业务功能受限时使用裸金属资源;为提升计算资源利用率,虚拟机资源池配置1~2倍CPU超分比,云桌面建议配置2~3倍超分比。

2) 存储资源池: 中心云建议对重要的裸金属承载的核心数据库业务, 使用 FC SAN 集中存储; 对于影响行车的 ATS、ISCS 关键业务虚拟机, 采用 IP SAN 集中存储; 对于其他通用的云化服务, 存在横向扩展需求以及大容量存储的场景, 使用分布式存储。车站云采用超融合架构, 不使用外置共享存储。

3) 网络设计: 在城轨云平台各网域内, 根据承载流量属性又可细分为不同的功能区, 相比传统网络架构更为复杂, 所以建议采用 SDN 方案来满足业务快速

部署、简化配置维护的需求。

4) 容灾设计: 建议对核心业务进行容灾, 非核心业务采用基于远程存储复制实现的数据级容灾和备份软件实现的本地数据备份方式。

2.2 “一云承载”的线路接入

建议采用搭积木方式, 分步建设、按需扩展, 既能发挥类似异构云的成本分期投资优势, 又能避免多云异构带来的高昂定制成本及运维难度, 业务上云原则如表 1 所示。

表 1 业务上云原则

Table 1 Principles of deploying the business app to cloud platforms

序号	项目	原则
1	涉及安全	云化应考虑应用软件是否涉及线路运营安全, 若应用软件的运行环境产生故障、将对线路运营安全产生极大影响时, 需慎重考虑和平衡系统云化的必要性和风险性。影响安全功能认证测试的, 可暂不考虑入云
2	业务复杂度	云化应考虑应用软件采用云化虚拟机的必要性: 根据业务请求的会话量和处理的复杂度选择, 会话量小、复杂度低的业务适合采用虚拟机部署; 根据业务系统运行时的资源占用情况, 资源占用低的业务适合采用虚拟机部署
3	运算性能	云化应考虑应用软件对服务器运算性能的要求, 若应用软件对服务器运算性能的要求特别高, 且在单个服务器上配置最大计算能力的虚拟机依然不能满足业务应用的计算能力, 则不能云化
4	硬件限制	云化应考虑应用软件对服务器芯片的要求, 若业务应用对服务器的芯片有特殊要求, 且芯片不支持在虚拟化环境中运行, 则不能云化; 云化应考虑应用软件对软件许可加密方式的要求, 若应用软件的许可加密方式不支持虚拟化的场景, 则不能云化; 云化应考虑应用软件对服务器板卡、外设的要求, 若业务应用对服务器的板卡有特殊要求, 且板卡不支持在虚拟化环境中运行, 则不能云化
5	工程表现	云化应考虑系统云化在实际应用案例中的使用情况和成熟度, 若系统云化反馈情况不理想或成熟度不足, 则应慎重考虑系统云化的必要性

2.3 “一云承载”的异构研究

城轨云计算、安全异构, 能有效打破单一品牌锁定, 解决线路分期建设、分步投资的问题^[4]。

1) 计算异构: 可按照不同资源池的配置方式形成标准化配置原则, 并开展适当的兼容性验证测试; 后续资源池扩容时, 在兼容性允许的前提下, 可任意采购符合配置要求的服务器设备来扩容不同的资源池。主要硬件配置基线包括: 云管理、云主机、裸金属服务器。

2) 安全异构: 网络信息安全作为独立领域, 可为各专业系统实现更全面的安全防护, 对安全管理型设备可优先采用异构方案。基于以上研究, 目前已形成了一项多云与异构平台的研究成果, 并通过北京城轨云证明其合理性, 具备指导后续项目建设的作用。

3 大数据共享交换平台

笔者以基于数据驱动导向的统一数据平台建设模式作为核心目标, 相关研究的内容包括 9 个方面。

3.1 建设模式分析

通过对比应用驱动导向的分散建设模式和数据驱

动导向的统一建设模式, 建议如下: 超大线网城市采用数据驱动统一建设模式, 逐步取代分散建设模式; 新建地铁城市直接采用数据驱动导向的统一建设模式, 在建设初期形成数字化驱动底座。

3.2 数据平台整体架构

构建统一数据集成、统一数据服务、统一数据共享的思路(见图 2)。

3.3 数据采集标准研究

依托并借鉴《城市轨道交通运营指标体系》的相关内容^[5]。

3.4 统一数据接入平台

依托并借鉴《城市轨道交通大数据平台技术规范》的相关内容^[6]。

3.5 统一数据存储技术

结合线网数据内容、特点及来源, 提出混合存储技术方案, 满足结构化、半结构化、非结构化数据的存储要求。

1) 结构化数据存储支持: 各业务主题的离线 OLAP 分析数据使用 Hive 数据仓库进行存储, 数据集市层宜

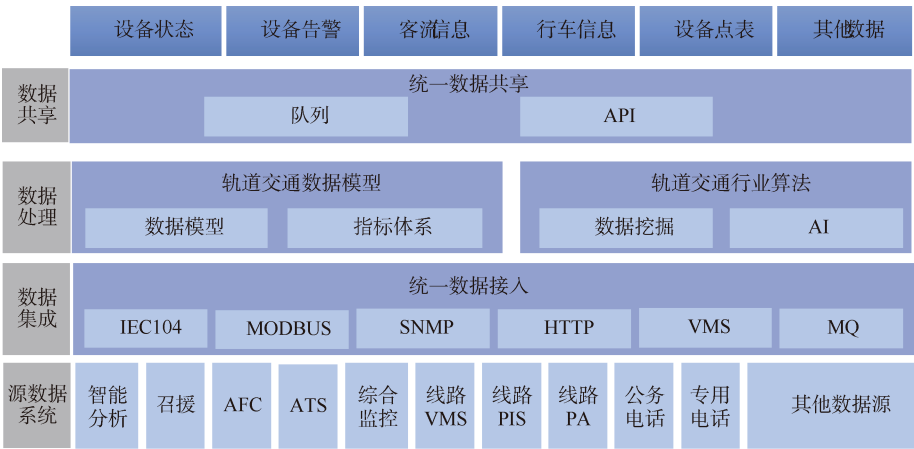


图 2 数据共享交换平台整体架构
Figure 2 Overall architecture of the data sharing and exchange platform

采用 Kylin、ClickHouse、GreenPlum 等技术手段进行优化，主数据管理或其他业务系统的独立数据使用关系型数据库进行存储，相关查询结果可采用 NoSQL 进行缓存优化。

2) 半结构化数据支持：文本、日志类数据若业务有实时分析需求，则需解析为结构化数据，并采用 NoSQL 进行存储，如 Elasticsearch 等；文本、日志类数据若无直接业务分析需求，则直接使用文件系统存储，存储过程中可结合数据湖技术(如 Hudi、Iceberg)进行管理，为后期数据取用提供可能性。

3) 非结构化数据：设施设备运行状态数据，可考虑采用实时数据库进行存储，如 Influxdb、Opentsdb 等；多媒体数据可采用支持分布式的对象文件系统进行存储，如 MinIO 等，相关存储能力由云平台统一提供。

3.6 统一数据服务技术

对数据 API 服务低代码创建、统一管理、全生命周期管理进行研究。

3.7 轨道交通数据模型

该模型面向轨道交通业务主题的、集成的、随时间变化的、信息本身相对稳定的数据集合，服务于决策过程管理。根据相关标准及历史积累，提出当事人、线网、设备、行车、票务、渠道、OD、客流、清算、事件、能耗等 11 大数据主题模型。

3.8 数据应用与展示

以建立轻便易用的自助式分析及可视化平台为研究目的，提出自助式分析、贴近业务场景、敏捷大数据三大核心功能需求，并在北京地铁 11 号线乘客服务数据分析中进行功能验证。

3.9 数据质量评估系统

针对轨道交通实际场景对维度进行说明细化，并提出数据质量管理框架。

基于以上研究，大数据共享交换平台方面目前已实现了统一数据交换及共享平台架构设计，相关组件技术及平台在 11 号线的数据分析平台及路网大数据中心数据治理项目中进行了试点落地验证。

4 城轨云安全

通过分析北京、呼和浩特、武汉、西安等城市的建设情况，针对当前存在的核心痛点问题进行研究。

4.1 全生命周期安全防护需求

从防护对象、安全角色、安全威胁、安全措施、生命周期 5 个视角，分析标准城轨云及数据的安全威胁及安全能力^[7]，明确将云边缘节点、中心云平台、平台数据作为标准城轨云的安全范畴防护对象。

4.2 数据安全标记强访技术

超大线网城轨云边界模糊化，采用安全标记强访设计，能实现安全生产网、内部管理网、外部服务网及运维管理网的各类业务访问控制，加强域间跨网数据交换的安全性，阻断非正常应用传播。但是，安全标记强访技术基于支持安全标记的安全级操作系统^[8]，其推广应用需各方共同推进，并需进一步研究验证其性价比。

4.3 东西向建模与精细化隔离管控技术

对于超大线网城轨云，建议采用微隔离技术模式构建业务系统流量模型，完成自适应安全策略配置管理；提供进程级细粒度安全管控、威胁溯源的功能，解决虚拟网络内部攻击面过大的问题^[9]。

4.4 统一云密码服务技术

对于超大线网城轨云应用的商用密码服务，建议采用密钥和密码运算解耦、先聚合再分片的设计架构，按照混合部署、代理调用方式，构建数据于产生、采集、存储、传输、分析、应用、安全交换共享、数据隐私保护^[10]等安全为一体的云密码资源池。

对于实施密码技术，建议采用具有国家密码管理部门颁发的密码产品型号证书的密码产品或密码模块，并在投入运行前，经商用密码应用安全性测评机构进行安全性评估。

4.5 统一安全管理平台技术

对于超大线网城轨云安全管理,建议基于异构安全理念的松耦合资源池建设,融合密码机资源,以策略路由引流和安全资源自动化编排方式,实现安全过程自动化,降低安全运维压力;统一安全管理服务平台,对所有安全资源、安全服务、安全策略实现统一管理和运维,安全态势分析明晰可见^[11]。对于规模不大、业务应用简单的场景,则可以考虑采取安全资源紧耦合或虚拟化方式,实现平台的安全防护。基于以上对国内主要城轨云安全的调研,结合北京超大线网云需求架构设计,目前已取得了一批城轨云安全的研究成果。

5 城轨云运维

国内城轨云大多近两年建设完成,城轨云的运维仍处于摸索阶段,根据北京城轨云的情况进行相关研究。

5.1 云平台运维方案

根据北京轨道云平台的运维情况,建议中心云平台 IaaS、硬件基础设施、机房基础环境由云平台运维单位负责,业务系统运维由线路运营单位负责。针对站段级云节点,主要对以下 3 种方案进行研究(见表 2)。结合北京超大线网城市的情况,推荐采用方案 3。

表 2 城轨云运维方案对比

Table 2 Application of unified data storage technology

运维内容	方案 1	方案 2	方案 3
业务系统运维	线路运营单位	线路运营单位	线路运营单位
IaaS 运维	线路运营单位	云平台运维单位	云平台运维单位
硬件基础设施运维	线路运营单位	线路运营单位	云平台运维单位
机房基础环境运维	线路运营单位	线路运营单位	线路运营单位

5.2 质量量化评估体系

主要对量化评估目标进行了研究,包括运行成效评价、业务系统效率评价、系统可用性评价和运维服务状态评估。

5.3 运行维护

分别从云平台运营和运维管理流程体系两个方面进行运行维护研究。

5.4 自动化工具和自动感知方向

主要是故障处理技术路线研究,制定目标和技术举措,包括模块设计和实现功能,规划设计如下功能:个人中心、权限管理、监控管理、配置管理、流程管理。

5.5 云平台使用和管理效果评估

以管理体系完善、落实、改进的评估为主,主要

通过现场检查等手段,对云平台管理成效进行总体评价,包括工作合规性管理和运营团队服务质量。

5.6 联合保障

基本任务以实现“地铁平安运营”为目标,坚持“安全第一,预防为主”的方针和“防、保、救”相结合的原则,在云平台或设备系统发生故障、险情和意外事故时,各单位联合行动,共同实施抢险救援,共同进行故障处理,做到及时抢修,缩短故障时间,减少损失,尽快恢复运营。

基于以上研究,目前已完成云平台运维方案和质量量化评估体系框架的搭建,并在北京轨道交通生产业务云平台进行了初步尝试,后续将推动体系落地的全面实施,促进云运维工作的良性循环发展。

6 研究成果

6.1 关键技术创新

1) 创新性提出了基于超大轨道交通路网运行条件下,适配异构技术框架的标准化、自主化,城轨云平台的总体架构、技术路线,以及面向全生命周期的建设与运营场景方案。对超大线网云基本架构异构、“一云承载”的线路接入和“一云承载”的异构等内容进行了深入研究,并提出了超大线网环境下的推荐方案。

2) 首次提出以轨道交通数据资产为核心的数据共享平台的技术实践方法,打破了传统的“烟囱式”数据管理思路,并探索建立基于行业特性的 11 大主题数据模型及数据治理方案。

3) 从防护对象、安全角色、安全威胁、安全措施、生命周期 5 个视角,深化全生命周期的安全防护需求,并全面分析了基于安全标记的数据强访体系架构和组成特点。同时,对东西向建模与精细化隔离管控技术进行了探讨展示,并深入研究面向云端业务的云密码服务,提出了统一安全管理平台技术。

4) 探索并构建了适用于超大线网云的运维质量评估体系,并在北京地铁 11 号线进行了联合保障研究的试运行,相关研究成果表明,可显著提升行业云平台的运维效能。

6.2 社会效益

本研究的成果逐步在北京试点、落地,为行业提供了借鉴,也为世界范围内的轨道交通行业提供了中国的解决方案,解决了超大城市城轨云/大数据平台的建设及运维难题,成果逐步推广至全国,助力交通强国的建设。

多云及异构方面的研究,能有效地打破云厂商的锁定,实现城轨云建设的分批次、分阶段投入,避免前期一次性大额投资;数据共享交换平台方面的研究,可有效地改善现有的数据接入难、数据管理难、数据服务难等问题,通过数据驱动改善现有的业务体系,提升业务价值,为轨道交通数字化驱动转型提供参考;云安全方面的研究,能够有效提高城轨云平台的网络安全保障能力,保护数据资源,保障正常的运维工作,网络安全与云平台的异构能吸引大量网络安全厂商参与,可进一步降低建设成本;云运维方面的研究,有助于实现城轨云运维分工的精细化和专业化,提升运维质量和运维效率,在原有体系的基础上能够进一步实现降本增效。

综上所述,超大线网云具有广阔发展前景,研究成果有助于适配线路建设周期,可更好地服务于地铁建设,服务于大众,提高社会效益;同时也有助于促进轨道交通产业升级,助推产业发展,有助于城轨云全生命周期的降本增效,提升经济效益。

7 结语

综上所述,基于多云及异构、大数据共享交换平台、城轨云安全和城轨云运维4个方向的研究,可有效解决行业在城轨云异构、大数据共享、云安全和云运维等方面的问题,实现“一片云”下分步建设与技术迭代相互融合的科学路径,构建海量数据优质资产,打造城轨云平台的安全防护技术,形成高效可复用的运维保障与应急联动机制。通过提升云业务连续性、数据安全性,以及云平台基础设施运管的集约化,持续保证城轨云与大数据核心技术处于国际领先水平。本研究成果将加快城轨云关键技术的持续攻关,推动自主可控和创新驱动不断进步,为实现“交通强国,城轨担当”贡献力量。

参考文献

- [1] 仲建华. 智慧城轨建设重点体系深化研究任重道远[J]. 城市轨道交通, 2022(5): 1.
ZHONG Jianhua. A long way to go in deepening research on key system of smart city rail construction[J]. China metros, 2022(5): 1.
- [2] 李得伟, 张天宇, 周玮腾, 等. 轨道交通大数据运用现状及发展趋势研究[J]. 都市轨道交通, 2016, 29(6): 1-7.
LI Dewei, ZHANG Tianyu, ZHOU Weiteng, et al. Research on application status and development trend of big data in rail transit[J]. Urban rapid rail transit, 2016, 29(6): 1-7.
- [3] 张晶鑫. 智慧城市轨道交通云平台建设构想及其架构与应用探讨[J]. 智慧中国, 2021(10): 70-72.
ZHANG Jingxin. Construction concept, architecture and application of smart city rail transit cloud platform[J]. Wisdom China, 2021(10): 70-72.
- [4] 王晓倩, 付立仕, 李岩, 等. 多级异构云数据中心体系平台研究[C]//第八届中国指挥控制大会论文集. 北京, 2020: 38-43.
WANG Xiaoqian, FU Lishi, LI Yan, et al. Research on multi-level heterogeneous cloud data center system platform[C]//Proceedings of the 8th China Command and Control Conference, Beijing, 2020: 38-43.
- [5] 城市轨道交通运营指标体系: GB/T 38374—2019[S]. 北京: 中国标准出版社, 2019.
Operational index system of urban rail transit: GB/T 38374—2019[S]. Beijing: Standards Press of China, 2019.
- [6] 城市轨道交通大数据平台技术规范: T/CAMET 11003—2020[S]. 北京: 中国铁道出版社有限公司, 2020.
Technical specification for big data platform of urban rail transit: T/camel 11003—2020[S]. Beijing: China Railway Publishing House Co., LTD. 2020.
- [7] 中国信通院及工业互联网产业联盟. 工业互联网平台安全白皮书(2020)[R]. 北京, 2020.
Alliance of Industrial Internet. National industrial security industry alliance (2020)[R]. Beijing, 2020.
- [8] 朱涛, 董鹏, 朱贺, 等. 基于标记技术的强制访问控制模型设计与应用[J]. 铁路计算机应用, 2022(1): 55-60.
ZHU Tao, DONG Peng, ZHU He, et al. Design and application of mandatory access control model based on tag technology[J]. Railway computer application, 2022(1): 55-60.
- [9] 游益峰. 面向虚拟化环境的微隔离技术研究[D]. 成都: 电子科技大学, 2019.
YOU Yifeng. Research on micro isolation technology for virtual environment[D]. Chengdu: University of Electronic Science and Technology of China, 2019.
- [10] 魏晓燕, 纪方. 商用密码在铁路的应用. 铁路计算机应用[J]. 2013, 22(8): 43-45.
WEI Xiaoyan, JI Fang. Application of commercial password in railway[J]. Railway computer application, 2013, 22(8): 43-45.
- [11] 吴雨农. 基于云计算技术的云安全管理平台设计[J]. 信息安全与通信保密, 2020(S1): 93-97.
WU Yunong. Design of cloud security management platform based on cloud computing technology[J]. Information security and communications privacy, 2020(S1): 93-97.

(编辑: 王艳菊)