doi: 10.3969/j.issn.1672-6073.2022.06.011

智慧城轨云平台和数据平台及网络安全融合协同技术研究

王 皓
（中铁第四勘察设计院集团有限公司，武汉 430063）

摘 要： 通过调研国内外城轨领域云平台、数据平台、网络安全的现状，针对目前国外无参考案例以及国内云平台、数据平台、网络安全建设融合协同性不足的问题，分析云架构下数据平台的实施需求，重点研究云数据库、数据平台的技术栈比选、云平台与数据平台纳管等，分析城轨云平台网络安全的总体需求，深入研究云内统保和系统自保、云平台和数据平台与网络安全资源池的协同，提出融合云平台、数据平台、网络安全、数据资源和系统运维统一协同化的管理中心。研究表明，做好数据平台总体规划和选型，利用软件定义安全技术，可实现云平台、数据平台、网络安全的融合协同，为城市轨道交通数字化转型及智慧化升级提供参考和借鉴。

关键词： 城市轨道交通；云平台；大数据；网络安全；融合；协同
中图分类号： U231 **文献标志码：** A **文章编号：** 1672-6073(2022)06-0064-05

Cloud Number Fusion and Security Coordination System of Smart Urban Rail

WANG Hao
(China Railway Siyuan Survey and Design Group Co., Ltd., Wuhan 430063)

Abstract: This study investigates the research status of cloud platforms, data platforms, and network security in the field of urban rail at home and abroad. Currently, no reference case is available from abroad, and the integration and cooperation of domestic cloud platform, data platform, and network security construction is insufficient. This study analyzes the implementation of the requirements for data platforms under a cloud architecture; the study primarily focuses on the cloud technologies of databases, data platforms, cloud platforms, and data platform convergence, etc., to analyze the overall cloud city rail network security requirements. The deepening of the cloud was studied in the same system with self-preservation, with cloud platform, data platform, and network security resources pooled together. A unified and collaborative management center that integrates a cloud platform, a data platform, network security, data resources, and system operation and maintenance is proposed. The study shows that the overall planning and selection of a data platform and use of software-defined security technology can achieve the integration and collaboration of a cloud platform, data platform, and network security, which can provide reference and guidance for the digital transformation and intelligent upgrading of urban rail transit.

Keywords: urban rail transit; cloud platform; big data; network security; convergence; collaboration

目前国外城轨领域在云平台和数据平台尚未得到大范围使用，仅有个别项目进行了云平台单一业务的试点。在城轨行业内，基于云原生的网络安全协同体系基本无相关工程案例。

收稿日期：2022-07-25 修回日期：2022-09-05
作者简介：王皓，男，硕士，高级工程师，主要从事轨道交通弱电系统设计科研工作，49739020@qq.com
基金项目：中国城市轨道交通协会研究项目(0904)；铁四院重点科研项目(2020K170)
引用格式：王皓. 智慧城轨云平台和数据平台及网络安全融合协同技术研究[J]. 都市快轨交通，2022，35(6)：64-68.
WANG Hao. Cloud number fusion and security coordination system of smart urban rail[J]. Urban rapid rail transit, 2022, 35(6): 64-68.

部分城市由于建设主体、建设时机等问题，存在多个品牌的云平台，甚至部分项目建设网域的范围和时序有所不同[1]。但总体上遵循中国城市轨道交通协会标准城轨云[2]，用统一的基础架构进行服务[3]，实现了建设和运维成本的降低[4]。

对北京、广州、武汉、南京、苏州数据平台方案的研究发现，目前大部分城市已不采用传统数据仓库来构建数据平台的技术路线，而采用 MPP+Hadoop 混合的方式进行数据平台的建设[5]，个别城市甚至采用了数据湖技术，但轨道交通领域基于云原生架构的数据平台，以及其与云平台的融合尚处于起步阶段。

1 城轨云平台与数据平台融合体系研究

1.1 云数据库应用概况

城轨云平台可为云上部署的业务系统统一提供数据库服务，并且在投资、可靠性、可用性方面具有一定的优势，但同时也影响了业务系统的数据库选型。目前，云数据库主要以国内信创厂家为主，轨道交通内得到应用的云数据库主要有华为的 Gauss DB 数据库、南大通用云数据库、武汉达梦云数据库。

从数据模型的角度看，云数据库并非是一种全新的数据库技术，而只是以服务的方式提供数据库功能。云数据库没有专属于自己的数据模型，所采用的数据模型可以是关系数据库所使用的关系模型，也可以是 NoSQL 数据库所使用的非关系模型。同一个轨道公司针对不同业务，也可能采用不同数据模型的多种云数据库服务。

目前轨道交通业务采用的云数据库主要存在以下问题：安全生产业务网域的部分业务系统依然采用国外的传统数据库(如 Oracle、DB2 等)，AFC 的清分中心对此有较为严重的思维惯性，近期有所改变，如武汉地铁 ACC 三期、武汉光谷空轨 ACC 都采用了上云的达梦数据库；此外，信号 ATS 由于涉及行车安全和 SIL-2 级认证，大部分信号系统集成商也不愿意改变自身 ATS 产品的数据库选型，这是下阶段工作的难点。

1.2 数据平台技术栈比选

数据仓库与数据平台的架构以数据为驱动，自下而上进行设计，提供数据集或分析报表，用于支持管理决策分析等分析型场景，在大数据基础上融合结构化和非结构化数据。在处理数据量 100 TB 以下、以结构化数据为主的场景下，数据仓库具有较好的优势，因此用在线网数量较少或中低运量轨道交通企业、二次开发能力较弱的轨道交通企业，以及部分线路级传统生产的智能运维系统和企业管理的数据分析系统中。这种方案投资较小，交付较为便捷。

数据直接加载到数据湖中，然后根据分析的需要再转换数据。数据湖产品是一套产品组合的解决方案，因此在建设初期投资较大，解决方案较为厚重，有明确的分析场景需求才可实现数据分析。而且，数据湖的使用对象更适合数据科学家、数据开发人员和业务分析师，与目前大多数轨道交通业主单位在数据平台初期建设的定位及现阶段业务需求的契合度不高。此外，数据湖技术的软件和服务的起步价较高，约为 7000 万～8000 万元。以上分析表明，数据湖技术较为适合超大线网规模，且轨道集团内部业态丰富，数字化信息化的规划全面到位，具有强大的二次开发能力的场景条件。

数据中台不是一个产品，而是与业务强相关。绝大部分轨道交通业务的访问量通常情况近似稳态，业务的访问量和数据处理量在短时间内不会骤增或骤减。若要发挥数据中台的相关效应和优势，其建设必然伴随着技术中台、业务中台甚至 AI 中台的建设。这种数据平台建设的模式较为厚重，初期起步的投资预计将达到 6000 万～7000 万元。以上分析表明，数据中台适用于轨道交通线路较多、数字化及信息化规划有一定的不确定性、业务系统有快速敏捷上线开发的需求、二次开发能力较强的轨道交通企业使用。

在目前阶段，轨道交通的大部分数据是结构化且有具体专业含义的，大部分的业务并不是需求突变、要求快速部署上线的。由于轨道交通数据的积累是从无到有的过程，所以需要实现结构化数据的联机分析处理(OLAP)。基于以上分析，现阶段推荐采用数据仓库与数据平台的架构。数据平台推荐选择基于 Apache Hadoop 开源社区组件的方案，基于 MPP+Hadoop 建设企业级的大数据处理环境，提供海量数据的存储、分析查询、全文搜索和实时流式数据处理分析等功能[6]。这种方案主要针对以下轨道交通公司：线网规模较大，未来具备一定的二次开发能力，以处理结构化数据为主，同时处理一定量的非结构化数据，且信息化规划的大体板块较为明晰。

1.3 云平台与数据平台融合纳管

在云数据库与云平台的融合纳管方面，云平台可以采用数据库日志、数据资源、数据库配置、Console 控制台等服务列表，呈现出租户数据库的服务管理。

数据平台、数据仓库与云平台进行融合，可以共用云资源池和管理节点，通过一套云管平台，实现统一的运营维护管理。数据平台和数据仓库可灵活选择，部署在物理机、裸金属(云化物理机)和虚拟机上。轨道交通运维单位后续可以灵活选择多种大数据集群部署方式，根据业务场景以及规模情况进行扩展混合部署；同时，可以依托云管平台，对混合部署的多集群实现统一运营维护，提高运营维护效率。

依托云平台的运维中心，可以实现对多站点的大数据和数据仓库的统一集中运维，提升运维效率。多站点的大数据平台可以通过云管平台，实现统一运营维护，从而实现对全部局点原厂监控、远程升级。通过中心侧专家资源，快速解决各站点的集群问题和运维问题，大大提高问题处理效率，从软件管理运维走向软硬件统一运维，包括服务器、网络、存储等。

云管平台在管理界面上统一了云服务入口，数据平台和数据仓库以云服务方式在云管平台界面上体现。用户可以通过云管平台页面访问所有云服务，云服务访问入口统一；像其他云服务一样，用户可以自主申请大数据集群资源，自助式管理集群，查看集群监控信息，实现高效运维；所有云服务统一，方便协调使用，提高其使用效率。

2 城轨云平台与网络安全协同体系研究

2.1 城轨云平台网络安全总体需求

城市轨道交通业务上云部署后，城轨云平台迫切需要解决安全问题。

1) 安全域机制被打破。在云计算环境中，计算和存储资源高度整合，基础网络架构统一化，传统的控制部署边界消失，安全域的机制被打破。

2) 东西向安全防护缺失。在同一宿主机中，不同业务系统间的通信(东西流向)用传统(南北流向)的物理安全设备无法检测，存在业务间的数据泄漏风险。

3) 满足云租户合规及安全需求。平台需要统筹考虑自身的网络安全建设，以及承载其上的应用系统安全防护工作，满足自身和租户的等保合规及安全需求。

2.2 软件定义网络安全资源池研究

对于软件定义网络安全资源池，业界的实现方式有 3 种：硬件一虚多方式、网络虚拟化(NFV)方式和独立安全资源池方式。

硬件一虚多方式主要指高性能防火墙、高性能入侵检测系统等设备通过虚拟化技术，将一台物理设备划分为多个逻辑设备，每一个逻辑安全设备独享硬件资源，独立运行，独立转发。同时，可以联动硬件 SDN 控制器，对流量进行编排、调度。将防火墙病毒库、特征库内置于硬件设备中，应用层过滤时仍然需要回流至特征库，数据清洗完成才可将流量放通。此种方案需要配置性能高的硬件设备，交付起来较为简单，但二次开发性差，运维设备工作量较大，所以不作为重点分析。

以下重点对安全资源池方案进行论述，主要有两种实现方式：一种是 NFV(云平台内 VPC 云原生安全服务链)的方案，另一种是在云平台的业务核心交换机旁挂安全资源池的方案[7]。

从技术层面来看，两种技术方案均可实现，优缺点也很明显。从有利于业主招标的竞争性和业务生产厂商支持的角度看，推荐采用旁挂安全资源池方案。从运营维护便利性上看，推荐采用 VPC 云原生安全服务链方案。在实际项目中，可采用两者方案异构的结合方式，但对旁挂安全资源池的厂商数量应当做出控制，一般在 2～3 家为宜。

如果线路数目有限，业主单位二次开发能力不强，建设管理及运维管理投入人力及能力一般，建议采用 NFV(VPC 云安全服务链)的模式。这样做对于整体合同管理较好，并且方便整体交付。

对于线网规模较大，业主单位二次开发能力较强，数据量多，建议平台采用旁路部署的方式。通过在通用 x86 服务器上安装相关软件的方式，将云安全资源池部署到云平台机房，旁挂在云平台核心交换机上；再通过网络引流技术，将云平台南北向的业务系统流量牵引至云安全资源池内进行清洗，如云防火墙、云 WAF、云 DDoS 等安全服务；流量清洗完成后，再将正常流量原路回注过去，最终到达云平台内的业务云主机上，从而实现云上业务安全防护的目的。还有部分安全产品不需要网络引流来实现，只需把安全资源池与云内业务虚拟机之间的网络打通即可，如云堡垒机、云日志审计、综合扫描等安全服务，从而达到在子云平台上进行云业务安全监测和审计的目的。

软件定义安全资源池架构基于软件定义安全技术，通过使用 Overlay、服务链以及信息安全等相关技术，实现能够根据系统需求进行预定义和自由组合，选择一种自适应安全技术架构。在此架构上，建立能够为最终用户提供方便快捷的网络安全自动编排服务的云安全服务平台。

云安全架构从下往上分为 3 层，其组成和功能如下：

1) 基础硬件架构层：该架构层由标准的 x86 服务器、通用交换机和 SSD/磁盘构成。

2) 虚拟化架构层：该架构层基于底层基础硬件架构，将计算、网络和存储进行软件虚拟化，为上层安全资源池架构提供所需的资源单元。

3) 安全资源池架构层：该架构层利用虚拟化架构层提供的资源单元，将各类安全组件进行统一部署和管理，对内利用安全服务链将任意安全组件进行自由组合，对外提供自由的安全编排服务。

2.3 云平台与网络安全协同融合研究

2.3.1 接口对接设计要点

网络安全平台与云管平台对接的主要难度是北向接口，北向接口可采用 Restful/Webservice/Syslog 等方式。这其中的关键设计点是：

1) 网络安全厂商多层次的性能优化：基于 SR-IOV 技术的虚拟网卡优化，基于 PCI passthrough 技术的虚拟网络性能优化，基于 DPDK 优化虚拟化平台性能，单组件 7 层性能可以与云平台网络设备匹配。

2) 弹性高可用性设计：基于云原生技术的安全资源弹性扩展，持续监测虚拟安全组件运行状态，实现故障组件自动切换/自动迁移。

2.3.2 云管平台对接流程

主要分为以下 4 个步骤：

1) 安全资源池的网络接入到云平台的 SDN 网络中；

2) 在大多数情况下，云平台通过 CSSP Plugin，与安全资源池上的 CSSP Agent 进行对接，实现对 CSSP 上的 API 接口的调用；

3) 在云平台管理界面中，增加安全资源池策略配置相关的栏目；

4) 当租户通过云平台管理界面配置了安全资源池的策略路由后，云平台先基于 CSSP Plugin 通知 CSSP 生成对应的租户网络，创建对应的安全组件，然后基于 SDN Plugin 生成的租户网络，将引流的服务链规则下发到 SDN 交换机，从而完成对接。

云平台和 SDN 交换机管理界面通过对安全资源池的标准 RESTFUL 接口的调用，实现了基于 SDN 的服务链对租户流量的自动化引流，无需手动配置策略路由。租户流量到达引流交换机后，能够自动生成策略路由信息，把已经开通安全服务的租户流量转发到安全资源池。安全资源池自动完成内部的流量编排，从而完成对全部租户流量的自动化引流。

2.3.3 与网络安全池对接

在城轨云平台业务侧，安全资源池与数据平台的对接主要是实现数据共享，数据平台与网络安全资源池对接的主要场景如下：

1) 网络安全资源池开放 resuful API，支持第三方数据平台的数据读取；网络安全资源池开放 https restfuAPI，提供 GET 方法进行数据的读取。第三方系统平台需要从安全管理平台获取安全事件、资产信息、脆弱性数据等结果性数据的场景。

2) 网络安全资源池通过 syslog，主动上报安全事件和安全告警数据至数据平台系统；网络安全资源池通过 syslog 标准日志数据传输协议，发送安全事件数据。数据平台需要安全管理平台通过 syslog 上报安全事件数据的场景。

3) 数据平台支持第三方日志接入，接入方式包含 syslog、agent 等。第三方安全设备、平台、网络设备、中间件、数据库等日志接入到网络安全管理平台，在其统一解析、分析、展示后，将相关数据上传至数据平台。

4) 探针作为 kafka 客户端，将流量日志数据上报到第三方数据平台的 kafka 服务端。

5) 探针支持同时上报数据至 2 个平台，在与网络安全管理平台对接的同时，通过 kafka 对接方式与第三方数据平台对接。

云平台全域态势感知系统通过接入第三方安全设备(如防火墙、IPS、IDS、WAF、终端安全等)、网络设备(如路由器、交换机等)、操作系统(如 Windows、Linux 各系列)、中间件(Web 中间件如 Apache 等，数据库中间件如 Mysql、Sql server 等中间件)等日志数据进行关联分析，结合 AI 机器学习和数据挖掘技术，发现安全威胁和安全风险，结合可视化呈现，构造多源化监视和分析的安全系统，旨在帮助用户通过多源数据分析检测威胁和溯源。

通过安全信息和事件管理分析系统，将网络环境中各种 Event 原始数据(包括主流厂商的设备日志，Windows、Linux 操作系统日志，Apache、Nginx、SSH、MySQL、Oracle 等常用组件日志)进行采集、清洗、范式化、存储、分析和展示，帮助安全分析人员早期识别和阻止攻击。

3 结语

本研究提出了一套具有国内自主知识产权云数融

合的数据平台。构建基于安全资源池架构的城轨云安全体系创新，基于软件定义、态势感知、云-网-安全联动技术，实现基于云原生的云内安全设备的软件定义化及服务链化，支持网络安全策略的云上自动化部署，主动感知防护进化，可实现第三方安全能力的无缝接入。通过本研究成果的推广，能够在城轨云的云数融合和云安协同等方面得到进一步的落地应用，主要包括：

1) 云数融合方面，首先通过共享数据平台在合肥、无锡等地落地，然后逐步向国内主流城市推广，并最终向国内其他城市和国际领域推广；将云平台与数据平台融合、云上数据库的建设模式和交付效果进行推广[8]，降低因云平台建设与数据平台建设脱节造成的额外成本支出，提升数据共享效果，为管理层快速、有效、正确的决策提供保障[9]。

2) 云安协同方面，推广软件定义的网络安全技术。集约硬件网络安全设备配置数量，降低设备维护及能耗成本。

此外，城轨云势必为智慧城轨信息化发展奠定坚实的基础[10]，可解决信息不对称的问题。通过数据共享和数据交换，可精准对接供需、高效配置资源，促进城市轨道交通领域的信息资源高度开放共享和综合开发利用，为民众多元化的信息需求提供跨越式发展的服务。

参考文献

[1] 智慧城市轨道交通信息技术架构和网络安全规范：第 1 部分：总体需求：T/CAMET 11001.1[S]. 北京：中国铁道出版社有限公司，2019.

[2] 智慧城市轨道交通信息技术架构和网络安全规范：第 2 部分：技术架构：T/CAMET 11001.2[S]. 北京：中国铁道出版社有限公司，2019.

[3] 智慧城市轨道交通信息技术架构和网络安全规范：第 3 部分：网络安全：T/CAMET 11001.3[S]. 北京：中国铁道出版社有限公司，2019.

[4] 城市轨道交通云平台构建技术规范：T/CAMET 11002[S]. 北京：中国铁道出版社有限公司，2021.

[5] 城市轨道交通大数据平台技术规范：T/CAMET 11003[S]. 北京：中国铁道出版社有限公司，2021.

[6] 城市轨道交通云平台网络架构技术规范：T/CAMET 11004[S]. 北京：中国铁道出版社有限公司，2021.

[7] 城市轨道交通云平台网络安全技术规范：T/CAMET 11005[S]. 北京：中国铁道出版社有限公司，2021.

[8] 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]. 都市快轨交通，2016，29(6)：1-7.
LI Dewei, ZHANG Tianyu, ZHOU Weiteng, et al. State-of-the-art and trend analysis of big data application in rail transit[J]. Urban rapid rail transit, 2016, 29(6): 1-7.

[9] 史歌，刘婷婷，高琳，等. 大数据平台下城市轨道交通信息系统建设[J]. 微型电脑应用，2020，36(2)：35-38.
SHI Ge, LIU Tingting, GAO Lin, et al. Construction of urban rail transit information system under big data platformt[J]. Microcomputer applications, 2020, 36(2): 35-38.

[10] 王皓，杨承东. 城市轨道交通融合云平台的探讨[J]. 都市快轨交通，2018，31(5)：50-53.
WANG Hao, YANG Chengdong. Research on fusion cloud platform of urban transit[J]. Urban rapid rail transit, 2018, 31(5): 50-53.

（编辑：王艳菊）

（上接第 18 页）

[4] 胡文艳. 钕铁硼永磁材料的性能及研究进展[J]. 现代电子技术，2012，35(2)：151-152.
HU Wenyang. Property and research progress of NbFeB permanent magnets[J]. Modern electronics technique, 2012, 35(2): 151-152.

[5] 王晓卫. 稀土永磁钕铁硼材料磁性能改进工艺[D]. 哈尔滨：哈尔滨工业大学，2008.
WANG Xiaowei. Process to improve the performance of rare-earth permanent magnet NdFeB[D]. Harbin: Harbin Institute of Technology, 2008.

[6] 陈致初，李益丰，符敏利. 永磁同步牵引电动机的特殊性[J]. 大功率变流技术，2012(3)：25-30.
CHEN Zhichu, LI Yifeng, FU Minli. Specificity of permanent magnet synchronous traction motor[J]. High power converter technology, 2012(3): 25-30.

[7] 中国工程建设标准化协会. 直流照明系统技术规程：T/CECS 705—2020[S]. 北京：中国建筑工业出版社，2020.

[8] 中国城市轨道交通协会. 城市轨道交通 2021 年度统计和分析报告[J]. 城市轨道交通，2022(7)：10-15.

（编辑：王艳菊）