doi: 10.3969/j.issn.1672-6073.2025.05.002

智能轨道交通数据安全防护体系：挑战、技术与未来演进

陈 磊[1,2]，杨玉欣[3]，公 备[3]
（1. 国防科技大学计算机学院，长沙 410073；2. 中国工程院战略研究中心，北京 100088；
3. 北京工业大学计算机学院，北京 100124）

摘 要：为解决轨道交通数据规模急剧膨胀、数据价值不断提升导致的安全问题，对智能轨道交通数据的安全防护体系进行研究。首先梳理轨道交通数据具有的多源异构、高实时性及强敏感性的特征，并分析在数据传输、存储和处理过程中的主要安全风险点；然后探讨针对网络攻击、数据泄露等威胁的联邦学习、轻量级加密、动态访问控制等前沿防护技术在资源受限环境下的应用现状、适用条件与性能表现；最后提出人工智能赋能的主动防御、跨系统协同治理等智能轨道交通数据安全未来的重点研究方向。研究结果表明：联邦学习可有效解决数据孤岛问题，在保证隐私前提下提升模型训练效率；轻量级加密算法在轨旁设备中展现出毫秒级响应优势，具有显著的应用潜力，是未来的发展趋势。研究成果可以为构建高效、可靠的智能轨道交通数据安全防护体系提供理论支撑和实践指导。

关键词：轨道交通；数据安全；网络安全；隐私保护；加密技术
中图分类号：U231 **文献标志码：**A **文章编号：**1672-6073(2025)05-0008-07

Security Protection System for Intelligent Rail Transit Data: Challenges, Technologies, and Future Evolution

CHEN Lei[1,2], YANG Yuxin[3], GONG Bei[3]
(1. Computer College, National University of Defense Technology, Changsha 410073; 2. Center for Strategic Studies, Chinese Academy of Engineering, Beijing 100088; 3. Computer College, Beijing University of Technology, Beijing 100124)

Abstract: Addressing the critical challenges in constructing a data security protection system for intelligent rail transit, this paper systematically reviews recent research advances in this field. First, it examines the characteristics of rail transit data, including its multi-source heterogeneity, high real-time demands, and strong sensitivity, along with the primary security risks during data transmission, storage, and processing. Second, it explores the current application status, suitability conditions, and performance metrics of cutting-edge protection technologies—such as federated learning, lightweight encryption, and dynamic access control—against threats like cyberattacks and data breaches in resource-constrained rail transit environments. Finally, it identifies key future research directions, including AI-empowered active defense and cross-system collaborative governance. The findings demonstrate that federated learning effectively resolves data silo issues while enhancing model training efficiency under privacy guarantees. Lightweight encryption algorithms demonstrate millisecond-level response advantages in wayside equipment, exhibiting significant application potential and representing a major future development trend. The research outcomes

收稿日期：2025-03-29 修回日期：2025-06-13
第一作者：陈磊，男，博士研究生，从事网络空间安全、数据安全的理论研究，cl@cae.cn
基金项目：科技部(2019YFB2102303)
引用格式：陈磊，杨玉欣，公备. 智能轨道交通数据安全防护体系：挑战、技术与未来演进[J]. 都市快轨交通，2025，38(5)：8-14.
CHEN Lei, YANG Yuxin, GONG Bei. Security protection system for intelligent rail transit data: challenges, technologies, and future evolution[J]. Urban rapid rail transit, 2025, 38(5): 8-14.

provide both theoretical underpinnings and practical guidance for building an efficient and reliable intelligent rail transit data security protection system.

Keywords: rail transit; data security; network security; privacy protection; encryption technology

轨道交通系统作为现代城市基础设施的重要组成部分，其重要性不仅体现在日常交通运输功能的实现上，更在于它对城市经济、社会发展和居民生活质量的深远影响[1]。从轨道线路的规划建设到列车的调度运行，从车站的日常管理到乘客服务的优化提升，轨道交通系统构成了一个庞大而复杂的运行体系。随着城市化进程的加速推进和轨道交通网络的持续扩张，这一系统所承载的运输压力和管理挑战也日益凸显。

近年来，以大数据、物联网、人工智能为代表的新一代信息技术在轨道交通领域得到了广泛应用，为行业带来了前所未有的发展机遇[2]。这些技术的深度融合正在深刻改变着传统轨道交通的运营模式和管理方式。通过部署各类智能感知设备和数据采集系统，轨道交通运营方能够实时获取海量的运行数据，包括列车运行状态、轨道设备健康状况、车站客流分布、乘客出行特征等多维度信息。这些数据不仅为日常运营决策提供了重要依据，更为系统优化和服务升级奠定了坚实基础。

为解决轨道交通数据规模急剧膨胀、数据价值不断提升导致的安全问题[3]，构建适应轨道交通数据特点、具备前瞻性和扩展性的科学防护体系，本文对智能轨道交通数据安全的挑战、技术和未来演进进行了深入分析，提出了融合联邦学习、轻量级加密与动态访问控制等前沿技术的智能轨道交通数据安全防护体系，实现了在保障数据机密性、完整性和可用性以及处理过程合规可控的同时，有效平衡安全防护强度与系统运营效率[4]，确保不影响正常运行和服务质量的目标，为构建未来适应性强的安全体系提供了创新路径。

1　轨道交通数据的安全需求

轨道交通系统作为城市交通的核心组成部分，承载着海量的运营数据、乘客信息以及设备监控数据。这些数据的安全不仅关系到系统的正常运行，更直接影响公共安全和社会稳定。轨道交通数据包含列车定位指令、乘客支付信息、设备运行日志等高敏感性内容。如图 1 所示，行业实践中存在 3 个主要矛盾：①信号系统及外部网络的安全隔离需求与智能调度数据共享需求的冲突；②设备监测数据的实时分析需求与边缘计算资源受限的困境；③乘客轨迹数据的匿名化处理与出行服务精准化要求的矛盾。

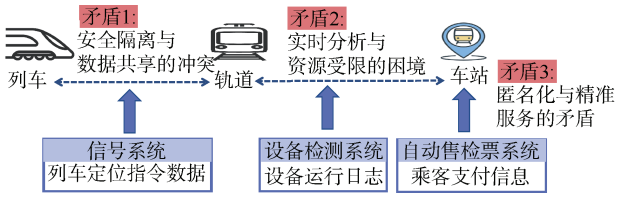


图 1　轨道交通数据安全中的主要矛盾

Figure 1　Key contradictions in rail transit data security

随着数字化转型的加速，轨道交通数据的安全需求变得更加复杂和迫切。这些需求可以从数据保密性、数据完整性、数据可用性和数据追溯性 4 个核心维度进行深入分析。

1.1　数据保密性

数据保密性是指确保敏感信息不被未经授权的个人或系统访问。在轨道交通领域，需要保护的数据主要包括乘客个人信息(如身份信息、支付记录、出行轨迹)、运营核心数据(如列车调度指令、信号系统参数)以及设备运行状态(如供电系统、轨道监测数据)。这些数据一旦泄露，可能造成严重后果：乘客隐私被滥用，会导致诈骗等犯罪行为；泄露的运营数据被恶意利用，可能干扰列车运行或实施网络攻击；设备数据的暴露则可能使系统漏洞被利用，威胁基础设施安全[5]。

为了保障数据保密性，轨道交通系统需要采取多层次的安全措施。例如，对乘客个人信息进行脱敏处理，确保在数据共享和分析过程中不暴露原始数据；对乘客个人信息实施 k-匿名化处理($k \geqslant 50$)，使得至少 k 个主体无法区分，确保在数据共享过程中单条记录不可识别；对核心控制系统实施严格的 4 级访问权限管理，权限粒度达字段级；在数据传输过程中采用强加密技术，防止数据在通信过程中被截获，密钥更新频率不低于 1 次/h。此外，随着人工智能和大数据的应用，如何在数据挖掘和智能分析的同时保护隐私，也是保密性需求的重要挑战。

1.2　数据完整性

数据完整性是指确保数据在生成、传输、存储和处理过程中不被篡改或损坏。轨道交通系统的运行高度依赖数据的准确性，任何数据篡改都可能导致严重

后果[6]。列车控制系统的指令若被恶意修改，可能引发列车相撞或脱轨等重大事故；自动售检票系统的交易数据若被篡改，可能造成财务损失或客流统计错误；设备监测数据的不准确可能导致故障未能及时发现，进而影响运营安全。

保障数据完整性需要从技术和管理两个层面入手。在技术层面，可采用数字签名、哈希校验等技术手段，确保数据在传输和存储过程中未被篡改[7]。同时，可以利用区块链等分布式账本技术，增强数据的不可篡改性，使任何数据修改行为都能被追溯和验证，基于区块链的分布式存证系统需实现 1000 笔/s 以上的交易处理能力。在管理层面，需要建立严格的数据审计机制，定期检查关键数据的完整性，并对异常操作进行实时监测和告警。

1.3 数据可用性

数据可用性是指确保数据在需要时能够被正常访问和使用，避免因系统故障、网络攻击或人为错误导致数据不可用。轨道交通是一个实时性要求极高的系统，任何数据访问延迟或服务中断都可能影响运营效率，甚至威胁运营安全[8]。列车调度系统若因数据访问受阻而无法获取实时位置信息，可能导致列车运行混乱；车站监控系统若因数据丢失无法调取视频记录，将影响突发事件的处理；乘客信息服务系统若因数据不可用而无法提供实时到站信息，将会降低出行体验。

提升数据可用性需要构建高可靠的存储和计算架构，如采用分布式数据库和容灾备份机制，确保即使部分节点故障，数据仍可正常访问。同时，需防范分布式拒绝服务(distributed denial-of-service，DDoS)攻击等恶意行为，通过流量清洗、访问控制等手段保障系统的稳定运行，DDoS 防护系统需具备 100Gbit/s 的攻击流量清洗能力，每月进行 2 次数据恢复演练，成功率需达 100%。此外，建立应急预案，定期进行数据恢复演练，也是确保数据可用性的重要措施。

1.4 数据追溯性

数据追溯性是指对数据的访问、修改、删除等操作进行完整记录，以便在发生安全事件时能够快速定位问题源头。轨道交通系统涉及多部门协作，数据流动复杂，如果没有完善的日志记录和审计机制，一旦发生数据泄露或篡改事件，将难以追责和修复。具体来说，若某次列车控制指令异常，需能快速查明是人为操作失误、系统漏洞还是恶意攻击；若乘客数据被非法访问，需能追踪到具体的访问者和操作时间[9]。

数据追溯示意如图 2 所示，实现数据追溯性需要建立全面的日志管理系统，记录所有关键数据的操作行为，并确保日志本身的安全性和不可篡改性。同时，结合人工智能技术，可对日志数据进行智能分析，自动识别异常行为并发出预警。日志管理系统需支持 10 000 条/s 记录的写入能力，操作记录保存期限≥180 天，异常行为识别准确率≥90%。此外，在数据共享和跨境流动场景下，需明确数据主权和合规要求，确保所有操作符合法律法规。

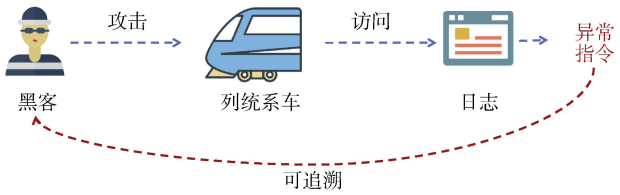


图 2 数据追溯示意

Figure 2 Data traceability diagram

轨道交通数据的安全需求是一个系统性工程，涉及保密性、完整性、可用性和追溯性等多个方面。随着技术的进步和威胁的演变，这些需求也在不断深化。未来，轨道交通系统需结合新兴技术构建更加智能、动态的安全防护体系，以应对日益复杂的网络安全环境，确保轨道交通的稳定运行和乘客的安全出行。

2 轨道交通数据安全体系的关键技术

随着城市轨道交通系统智能化程度的不断提升，数据安全防护面临着前所未有的挑战。为应对这些挑战，行业内已形成了一套较为完善的数据安全技术体系，具体包括联邦学习技术、数据加密技术、访问控制技术、数据备份与容灾技术和实时监控与报警技术。

2.1 联邦学习技术

联邦学习技术在轨道交通数据安全中的应用具有显著优势。该技术通过分布式机器学习框架，使得各参与方可以在不共享原始数据的情况下进行联合建模，有效解决了数据孤岛问题[10]。在轨道交通场景中，不同线路、车站和业务系统产生的数据往往分散存储且涉及多方主体，联邦学习技术能够在不直接交换敏感数据的前提下，实现跨部门、跨系统的协同分析。在客流预测模型中，各车站可以通过联邦学习共享模型参数而非共享原始乘客数据，既保护了用户隐私，又提升了预测准确性。轨道交通中联邦学习架构的设计逻辑如图 3 所示，其中，车站级节点负责边缘设备数据采集与轻量化特征提取，线路级聚合器接收车站

级节点的特征参数，输出线路级模型参数，线网级管理中心接收线路级聚合器的加密参数，输出全局优化模型，整个流程体现了从数据采集到全局模型优化的全流程治理机制。在典型的轨道交通场景中，联邦学习系统需满足车站级节点与线路级聚合器之间的参数传输延迟控制在 50 ms 内，以适应列车实时调度的需求。采用梯度压缩技术可将通信量减少 60%，同时保障模型准确率损失不超过 2%。

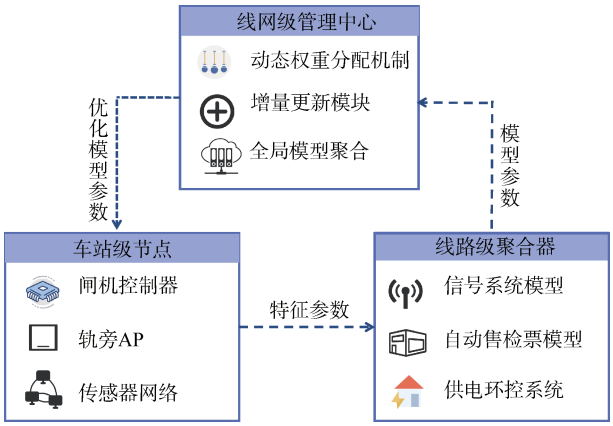


图 3　轨道交通中的联邦学习架构

Figure 3　Federated learning architecture in rail transit

2.2　数据加密技术

数据加密技术构成了轨道交通数据安全的基础防线。现代加密体系包含传输加密和存储加密两个关键环节[11]。在传输过程中，数据加密技术采用传输层安全协议(transport layer security，TLS)和安全套接层协议(secure sockets layer，SSL)等对车地通信、系统间交互等数据流进行端到端保护，防止中间人攻击。对于存储环节，则运用高级加密标准(advanced encryption standard，AES)等强加密算法对数据库中的敏感信息进行加密处理，即使发生数据泄露，攻击者也无法直接获取有效信息。针对轨道交通系统的实时性要求，业界正在研发低延迟的轻量级加密算法，在确保安全性的同时不影响系统响应速度。轨道交通环境对加密技术提出了特殊要求，具体性能指标需满足：①数据包加密延迟需控制在 5 ms 以内；②数据库加密的读写性能衰减不大于 15%；③密钥轮换周期严格遵循：列车控制数据 1 次/h，乘客信息 1 次/d，设备日志 1 次/周。

2.3　访问控制技术

访问控制机制是防止未授权访问的核心保障。轨道交通系统采用基于角色的访问控制与属性基加密相结合的混合模式[12]。基于角色的访问控制机制根据用户的职责分配权限，如调度员只能访问运行数据，维修人员仅能查看设备状态；而属性基加密技术则实现了更细粒度的数据访问控制，可以依据数据敏感程度动态调整访问策略[13]。此外，多因素认证技术的引入进一步强化了身份验证环节，将生物特征、硬件令牌与传统密码相结合，此方式认证完成时间小于 3 s，大幅提高了系统入口的安全性。

2.4　数据备份与容灾技术

数据备份与容灾体系为业务连续性提供最后保障。轨道交通系统采用“两地三中心”的灾备架构，通过实时数据同步确保关键信息的冗余存储[14]。在备份策略上，灾备架构采用全量备份与增量备份相结合的方式，满足全量备份速率≥1 TB/h，增量备份延迟≤15 min，既保证恢复效率又节省存储空间。容灾演练被纳入常规运维流程，通过定期模拟各类故障场景，验证恢复预案的有效性。目前，新型的云原生灾备方案正在被引入，它可以利用容器化和微服务架构实现更灵活的故障切换能力。

2.5　实时监控与报警技术

实时监控与预警系统构建了主动防御体系。通过部署网络流量分析、用户行为分析(user and entity behavior analytics，UEBA)等监测工具，对系统运行状态进行 7×24 h 监控[15]，保证威胁检测覆盖率≥98%，零日攻击识别平均时间≤30 min。基于机器学习的异常检测算法能够识别出偏离正常模式的操作行为，如异常登录、数据批量导出等可疑活动。预警机制采用分级响应策略，根据威胁级别自动触发相应的处置流程。为提高监测效率，部分系统已开始尝试将数字孪生技术应用于安全运维，通过构建虚拟映像实现攻击行为的可视化分析与预测。

上述这些关键技术并非孤立存在，而是通过系统集成形成协同防御体系。联邦学习为跨系统数据协作提供安全基础，加密技术保障数据传输存储安全，访问控制规范数据使用边界，备份容灾确保业务韧性，实时监控则实现威胁的及时发现与处置。

3　轨道交通数据安全面临的挑战

在数字化转型浪潮下，轨道交通系统正经历着前所未有的智能化变革，然而这一进程也带来了严峻的数据安全挑战。当前，虽然已经建立了较为完善的数据安全防护体系，但在实际运营中仍然面临着诸多亟

待解决的安全问题，这些问题不仅威胁着系统的稳定运行，更可能危及公共安全和社会秩序。

3.1 数据传输安全风险

数据传输安全风险是轨道交通面临的首要挑战。现代轨道交通系统高度依赖无线通信网络实现列车控制、调度指挥和乘客服务等功能。车地通信系统作为连接列车与地面控制中心的关键纽带，其安全性直接关系到整个系统的运行安全[16]。然而，无线通信的开放性特征使车地通信系统容易遭受中间人攻击、信号干扰等安全威胁。攻击者可能通过伪造基站、信号劫持等手段获取敏感数据，甚至篡改控制指令，造成严重后果。此外，随着 5G、WiFi 6 等新技术的应用，通信协议的复杂性增加，新的安全漏洞也随之产生。如何确保海量数据在复杂网络环境中的安全传输，成为轨道交通数据安全的重要课题。

3.2 系统复杂性

系统复杂性带来的安全隐患同样不容忽视。现代轨道交通系统是由多个子系统构成的庞大体系，包括信号、供电、自动售检票、乘客信息等子系统。这些子系统往往采用不同的技术架构和安全标准，系统间的接口和交互环节成为安全防护的薄弱点。更为复杂的是，许多轨道交通系统是在不同时期建设的，新旧系统并存导致安全防护水平参差不齐。攻击者可能利用系统间的兼容性问题或旧系统的安全漏洞实施渗透，一旦某个子系统被攻破，就可能引发连锁反应，威胁整个系统的安全运行[17]。此外，第三方供应商提供的设备和软件也可能引入潜在的安全风险，如何确保供应链安全成为系统建设中的重要考量。

3.3 物联网设备的安全问题

物联网设备的安全问题日益凸显。随着智能轨道交通的发展，各类物联网设备被广泛应用于车站管理、列车监控、环境监测等领域。这些设备数量庞大、分布广泛，且大多采用嵌入式系统，计算能力和安全防护能力有限。许多设备在设计时更注重功能实现而忽视了安全性，存在默认密码、固件漏洞等安全隐患[18]。更令人担忧的是，这些设备往往直接接入轨道交通核心网络，一旦被攻破就可能成为攻击者入侵系统的跳板。近年来，针对物联网设备的攻击事件频发，包括恶意软件感染、拒绝服务攻击等，严重威胁着轨道交通系统的安全稳定运行。

3.4 跨系统数据共享的隐私问题

跨系统数据共享带来的隐私保护挑战尤为突出。数字化城市轨道交通示意如图 4 所示，数字化城市建设背景下，轨道交通数据需要与多个平台进行共享和交换，以实现更高效的协同管理。

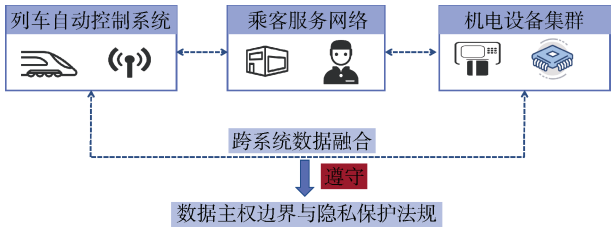


图 4 数字化城市轨道交通示意

Figure 4 Digitalized urban rail transit

然而，这种数据流动大大增加了隐私泄露的风险。一方面，数据在多个系统间流转时，访问权限管理变得异常复杂，难以确保每个环节都得到有效保护；另一方面，数据聚合分析可能导致隐私信息的间接泄露，即使单个系统采取了匿名化处理，通过多源数据的关联分析仍可能识别出特定个体。如何在保障数据价值挖掘的同时维护个人隐私权益，成为轨道交通数据治理中的关键难题[19]。

随着技术的不断发展和安全威胁的持续演变，轨道交通数据安全将是一个需要长期关注和投入的重要领域。只有通过技术创新、管理优化和多方协作，才能有效应对各种安全挑战，为智慧轨道交通的发展保驾护航。

4 轨道交通数据安全的未来发展趋势

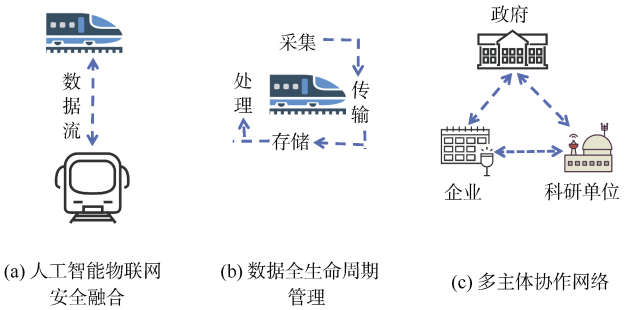
在数字化浪潮和智慧城市建设的双重推动下，轨道交通数据安全体系正迎来革命性的变革。未来几年，随着新兴技术的快速发展和安全理念的持续创新，轨道交通数据安全将呈现出多维度的演进趋势，这些变革将从根本上重塑行业的安全防护格局。

人工智能与大数据的深度融合将引领安全防护的智能化升级[20]。传统的安全防护手段主要依靠规则匹配和特征识别，难以应对日益复杂的网络攻击。而人工智能技术的引入，特别是深度学习算法的应用，使得安全系统具备了自我学习和进化能力。通过分析海量的安全日志和网络行为数据，AI 系统可以建立正常行为基线，实时检测异常活动。更为重要的是，基于机器学习的安全预测模型能够通过对历史攻击模式的分析，预测潜在的攻击路径和时间窗口，实现从被动防御到主动预防的转变。在轨道交通场景中，这种智能安全系统可以同时监控数以万计的物联网设备，识

别设备异常行为，预防大规模网络攻击的发生。以深圳地铁为例，其通过基于长短期记忆网络(long short-term memory，LSTM)神经网络分析历史攻击数据，构建攻击时间序列模型，预测高峰时段(如节假日前后)攻击概率提升 62%；通过数字孪生构建虚拟靶场，模拟北京大兴机场线遭受勒索软件攻击的场景，使应急响应时间缩短 40%。未来，随着边缘计算技术的发展，AI 安全分析能力将进一步下沉到车站、列车等边缘节点，形成分布式的智能安全防护网络。

全生命周期安全管理理念的深化将推动安全防护体系的系统化重构。未来的数据安全管理将突破传统边界防护的局限，将安全考量贯穿数据从产生到销毁的整个生命周期。在数据采集环节，通过可信执行环境(trusted execution environment，TEE)技术确保采集设备的可信度和数据的真实性；在数据传输环节，采用端到端加密和完整性校验机制；在数据存储环节，实施细粒度的访问控制和加密存储；在数据处理环节，运用隐私计算技术保护数据使用过程中的隐私安全；在数据销毁环节，建立完善的数据清理和审计机制。这种全生命周期的安全管理需要统一的安全策略框架和技术标准作为支撑，同时也依赖于自动化安全管控平台的建设和部署。对于轨道交通行业，实现全生命周期安全管理的一个关键挑战是如何平衡安全要求与运营效率，特别是在实时性要求极高的列车控制系统等关键场景中。

轨道交通数据安全未来生态体系如图 5 所示，轨道交通数据安全的发展将呈现出技术融合、体系重构和生态协同 3 大特征。新技术的交叉融合将催生更强大的安全解决方案，安全理念的革新将推动防护体系的系统性升级，而多方参与的治理模式则将构建更富韧性的安全生态。在这个演进过程中，需要特别注意技术创新与标准制定的协同推进，确保新技术的安全



(a) 人工智能物联网安全融合　(b) 数据全生命周期管理　(c) 多主体协作网络

图 5　轨道交通数据安全未来生态体系

Figure 5　Future ecosystem of rail transit data security

可靠应用。同时，人才培养和队伍建设也是不可忽视的关键因素，只有建立专业化的安全团队，才能有效驾驭日新月异的安全技术。随着这些趋势的逐步实现，轨道交通数据安全水平将迈上新的台阶，为智慧轨道交通的发展奠定坚实的安全基础。

5　结论

轨道交通数据安全不仅关乎轨道交通系统的稳定运行，更与公众安全息息相关。随着数据量的不断增加，轨道交通数据安全体系的建设显得尤为重要。本文针对智能轨道交通数据安全防护体系的挑战，技术和未来趋势进行了深入分析，得出如下结论：

1) 智能交通数据安全需求包括保障数据保密性、完整性、可用性及追溯性 4 大核心维度，需满足毫秒级实时响应、大攻击流量清洗等严苛性能指标；

2) 轨道交通数据安全体系的关键技术包括通过联邦学习破解数据孤岛、轻量级加密实现轨旁设备毫秒级安全通信、动态访问控制达成字段级权限管理，结合区块链存证与 UEBA 异常监测形成纵深防御。

未来，智能交通数据安全防护将向 AI 赋能的主动防御、TEE 硬件级可信计算及跨系统协同治理演进，推动安全机制从边界防护向全生命周期管理跃升。研究成果为构建下一代轨道交通安全体系提供了可行的技术路径。

参考文献

[1] 陈光. 关于城市轨道交通系统协同及最小化的思考[J]. 城市轨道交通研究, 2025, 28(3): 170-174, 180.
CHEN Guang. Thoughts on coordination and minimization of urban rail transit systems[J]. Urban mass transit, 2025, 28(3): 170-174.

[2] 杨志远. 城市轨道交通数字化转型的关键问题与策略研究[J]. 中阿科技论坛(中英文), 2025(3): 39-43.
YANG Zhiyuan. Research on key issues and strategies of digital transformation of urban rail transit[J]. China-Arab states science and technology forum, 2025(3): 39-43.

[3] 张娴, 蒋建峰. 基于数据全生命周期的城市轨道交通云平台数据安全治理研究[J]. 城市轨道交通研究, 2023, 26(12): 288-291.

[4] 刘宇, 黎琳, 鲁放, 等. 轨道交通“四网融合”数据治理关键技术研究[J]. 铁路计算机应用, 2023, 32(6): 82-86.
LIU Yu, LI Lin, LU Fang, et al. Key technologies of data governance of “four-network integration” for rail transit[J]. Railway computer application, 2023, 32(6): 82-86.

[5] 赵伟慧, 孙同庆, 汪晓臣, 等. 城市轨道交通乘客服务信息发布安全保障方案研究[J]. 铁道运输与经济, 2022, 44(4): 106-111.
ZHAO Weihui, SUN Tongqing, WANG Xiaochen, et al. Security scheme for passenger service information release in urban rail transit[J]. Railway transport and economy, 2022, 44(4): 106-111.

[6] 井柯, 安尚平. 浅析城市轨道交通综合监控系统数据安全检测方法[J]. 新型工业化, 2021, 11(10): 175-178.

[7] 周云飞, 史明, 杨云霞. 基于区块链的云存储数据完整性和安全性方案[J]. 山西能源学院学报, 2024, 37(4): 92-94.
ZHOU Yunfei, SHI Ming, YANG Yunxia. Cloud storage data integrity and security scheme based on blockchain[J]. Journal of Shanxi Institute of Energy, 2024, 37(4): 92-94.

[8] 管剑波, 毛照平, 徐振磊. 城市轨道交通网络安全供应链管理探索与实践[J]. 工业信息安全, 2024(5): 75-81.
GUAN Jianbo, MAO Zhaoping, XU Zhenlei. Exploration and practice in cyber supply chain management for urban rail transit security[J]. Industrial information security, 2024(5): 75-81.

[9] 顾嘉辉, 王潇骁, 姚归. 城市轨道交通数据汇聚共享系统的设计与研究[J]. 精密制造与自动化, 2024(2): 32-35.
GU Jiahui, WANG Xiaoxiao, YAO Gui. Design and research of data aggregation and sharing system for urban rail transit[J]. Precise manufacturing & automation, 2024(2): 32-35.

[10] 仇健, 马海英, 王占君, 等. 联邦学习中隐私保护聚合机制综述[J]. 计算机应用研究, 2025, 42(6): 1601-1610.
QIU Jian, MA Haiying, WANG Zhanjun, et al. Survey of privacy-preserving aggregation mechanisms in federated learning[J]. Application research of computers, 2025, 42(6): 1601-1610.

[11] 许玲, 汪可可, 管剑波. 云计算下的轨道交通信息系统数据安全[J]. 工业信息安全, 2022(11): 69-77.
XU Ling, WANG Keke, GUAN Jianbo. Data security of rail transit information system under cloud computing[J]. Industry information security, 2022(11): 69-77.

[12] 华高锋. 基于区块链的轨道交通数据共享计算研究[D]. 北京: 北京交通大学, 2022.
HUA Gaofeng. Research on blockchain-based data sharing and computing for rail transit systems[D]. Beijing: Beijing Jiaotong University, 2022.

[13] 刘为俊. 城市轨道交通云平台网络安全访问控制技术研究[J]. 铁道通信信号, 2024, 60(3): 69-74.
LIU Weijun. Research on network security access control technology for the cloud platform in urban rail transit[J]. Railway signalling & communication, 2024, 60(3): 69-74.

[14] 许子恒, 李王睿, 张立东, 等. 基于信息备份技术提升城市轨道交通数据单向传输可靠性的设计方法[J]. 城市轨道交通研究, 2024, 27(9): 227-230.
XU Ziheng, LI Wangrui, ZHANG Lidong, et al. A design method for improving the reliability of urban rail transit one-way data transmission based on information backup technology[J]. Urban mass transit, 2024, 27(9): 227-230.

[15] 刘珺晖. 基于物联网的轨道交通信号系统监控与故障预警研究[J]. 科技资讯, 2025, 23(3): 41-43.
LIU Junhui. Research on monitoring and fault warning of rail transit signal system based on Internet of Things[J]. Science & technology information, 2025, 23(3): 41-43.

[16] 吴国仁, 周光军, 邢军伟, 等. 城市轨道交通企业数据安全保障体系研究[J]. 城市轨道交通, 2023(7): 53-57.

[17] 李景虎, 杨骥, 刘悦. 上海轨道交通智慧消防物联网系统搭建[J]. 城市轨道交通研究, 2025, 28(5): 255-258.
LI Jinghu, YANG Ji, LIU Yue. Construction of smart fire protection IoT system for Shanghai rail transit[J]. Urban mass transit, 2025, 28(5): 255-258.

[18] 徐健钦. 基于窄带物联网的铁路通信网络安全加密控制系统设计[J]. 网络安全和信息化, 2024(6): 43-45.

[19] 段朝晖, 陈文宇, 魏镇安. 轨道交通网络安全防护的探究与实践[J]. 网络安全技术与应用, 2023(5): 126-128.

[20] 王磊, 贺俊, 位凯乐, 等. 大数据智能运维管理在轨道交通行业的应用[J]. 电视技术, 2023, 47(7): 221-228.
WANG Lei, HE Jun, WEI Kaile, et al. Application of big data intelligent operation and maintenance management in rail transit industry[J]. Video engineering, 2023, 47(7): 221-228.

（编辑：王艳菊）