AI驱动的AFC系统异常行为检测与安全防护机制

李亚昆　田中林
郑州交通发展投资集团有限公司　河南　郑州　450000

摘　要：本文聚焦AI驱动的AFC系统异常行为检测与安全防护机制。先阐述研究背景与意义，指出AFC系统安全威胁及AI应用的重要性。接着介绍相关技术，包括AI技术在异常检测中的应用及AFC系统架构与安全需求。深入探讨AI驱动的异常行为检测模型，涵盖模型架构、关键技术及优化策略。详细说明安全防护机制设计，涉及防护体系架构、技术措施和管理策略。

关键词：AI驱动；AFC系统；异常行为检测；安全防护机制

1 引言

城市轨道交通发展迅猛，自动售检票系统（AFC）作为核心子系统，其安全稳定至关重要。该系统基于多种技术实现运营全流程自动化，但如今面临的安全威胁愈发复杂多样。工业互联网下，勒索病毒等肆虐，工作站等成重灾区，且先进技术引入使威胁多元化。城轨云建设完善，可安全一体化问题未解。AI技术融入为解决AFC系统安全问题提供新思路，其数据处理、自我学习及自动化能力强，能实时分析数据、发现威胁，通过AI驱动的机制可保障轨道交通安全稳定运行，意义重大。

2 相关技术与理论基础

2.1 AI技术在异常检测中的应用

2.1.1 机器学习算法

在异常检测中作用关键。监督学习如支持向量机（SVM）、决策树，利用已标记的正常和异常数据训练分类模型，像用SVM训练AFC系统交易数据模型可识别欺诈交易。无监督学习如聚类、孤立森林算法，无需标记数据，聚类算法将数据分簇，异常数据远离正常簇；孤立森林构建随机森林隔离异常点，能有效检测异常值。

2.1.2 深度学习模型

有独特优势。卷积神经网络（CNN）可自动提取数据特征，适用于图像、时序数据处理，能分析AFC系统乘客行为图像检测异常。循环神经网络（RNN）及其变体可处理时序数据，捕捉长期依赖关系，通过分析交易数据时序预测正常模式，不符则为异常。生成对抗网络（GAN）生成正常数据分布，与生成分布差异大的数据判定为异常。

2.1.3 自然语言处理技术

对处理AFC系统文本数据作用大。文本分类可对系统日志、用户反馈分类，识别安全相关信息；情感分析能分析用户反馈情感倾向，发现安全隐患；命名实体识别可从文本中识别关键实体，为异常检测提供准确信息。

2.2 AFC系统架构与安全需求

2.2.1 AFC系统架构概述

AFC系统一般具有四层架构，包括车票层、车站终端设备层、车站计算机系统层、线网管理中心系统（ANCC）。车票层是乘客所持的车费支付媒介，规定了储值卡和单程票的技术要求；车站终端设备层安装在各车站站厅，直接为乘客提供售检票服务；车站计算机系统层对车站终端设备进行状态监控和数据收集；ANCC系统基于云平台架构，采用资源池化和动态扩展，支持数据汇聚共享和业务合理分配。结合智能乘车综合业务平台（ITP），实现了刷码、刷脸过闸等互联网乘车业务，支持信用支付和离线过闸功能，提升乘客体验。

2.2.2 AFC系统安全需求分析

AFC系统面临着多种安全威胁，需要满足多方面的安全需求。在数据安全方面，要确保乘客信息、交易数据等在采集、传输、存储和使用过程中的机密性、完整性和可用性，防止数据泄露、篡改和丢失[1]。在系统安全方面，要保护AFC系统的各个组件免受恶意攻击，如防止黑客入侵、病毒感染等，确保系统的稳定运行。在网络通信安全方面，要保障AFC系统内部网络以及与外部系统网络通信的安全性，防止网络窃听、篡改和拒绝服务攻击等。此外，还需要满足合规性要求，遵守相关的法律法规和行业标准，如网络安全法、等保2.0等。

3 AI 驱动的 AFC 系统异常行为检测模型

3.1 检测模型架构设计

3.1.1 整体架构

AI驱动的AFC系统异常行为检测模型采用分层架构，包括数据采集层、数据预处理层、特征提取层、异常检测层和结果反馈层。数据采集层负责收集AFC系统中的各种数据，如交易数据、设备状态数据、用户行为

数据等。数据预处理层对采集到的数据进行清洗、转换和归一化等处理，提高数据质量。特征提取层从预处理后的数据中提取有价值的特征，为异常检测提供依据。异常检测层利用AI算法对提取的特征进行分析，判断是否存在异常行为。结果反馈层将检测结果反馈给相关人员或系统，以便采取相应的措施。

3.1.2 各层功能详细说明

数据采集层通过多种方式收集数据，如在AFC系统的各个组件中部署数据采集代理，实时获取交易记录、设备日志等信息；利用网络监听技术捕获系统网络通信数据。数据预处理层对采集到的数据进行去重、缺失值处理、异常值处理等操作，将数据转换为适合后续处理的格式。特征提取层根据不同的数据类型和异常检测需求，提取相应的特征。例如，对于交易数据，可以提取交易金额、交易时间、交易地点等特征；对于用户行为数据，可以提取用户的操作频率、操作顺序等特征[2]。异常检测层采用多种AI算法进行异常检测，如基于机器学习的分类算法、基于深度学习的神经网络算法等。通过对比正常行为模式和实际行为模式，判断是否存在异常。结果反馈层将检测结果以可视化的方式展示给管理人员，同时可以通过短信、邮件等方式通知相关人员，并及时将异常信息记录到日志中，以便后续分析和追溯。

3.2 关键技术实现

3.2.1 数据采集与预处理技术

数据采集技术需要确保数据的完整性和准确性。可以采用分布式数据采集框架，提高数据采集的效率和可靠性。在数据预处理方面，针对AFC系统数据的特点，采用合适的方法进行处理。例如，对于时序数据，可以使用滑动窗口法进行分段处理；对于文本数据，可以使用分词、词干提取等技术进行预处理。同时，为了提高数据的质量，还可以采用数据增强技术，如生成合成数据来扩充训练集。

3.2.2 特征工程方法

特征工程是异常检测的关键环节。可以采用多种方法进行特征提取和选择。对于数值型数据，可以使用统计方法提取均值、方差、最大值、最小值等特征；对于类别型数据，可以使用独热编码等方法进行转换。此外，还可以利用领域知识提取更有意义的特征。例如，在AFC系统中，根据交易的业务规则提取特征，如同一用户短时间内多次进行大额交易等。特征选择方面，可以使用过滤法、包装法、嵌入法等方法，选择对异常检测最有价值的特征，减少特征维度，提高检测效率。

3.2.3 异常检测算法选择与优化

根据AFC系统的特点和异常检测的需求，选择合适的异常检测算法。对于数据量较小、特征维度较低的情况，可以选择机器学习算法，如SVM、决策树等；对于数据量较大、特征复杂的情况，深度学习算法具有更好的性能，如CNN、LSTM等。为了提高算法的准确性和实时性，需要对算法进行优化。例如，调整算法的参数、采用集成学习方法、对模型进行剪枝等。同时，还可以结合多种算法进行异常检测，提高检测的鲁棒性。

3.3 检测模型优化策略

3.3.1 模型训练与调优

模型训练是提高检测模型性能的关键步骤。在训练过程中，需要选择合适的训练数据集和验证数据集，确保数据的质量和代表性。采用交叉验证等方法评估模型的性能，避免过拟合和欠拟合。同时，对模型的参数进行调整和优化，如学习率、迭代次数等，以提高模型的准确性和泛化能力[3]。此外，还可以采用迁移学习的方法，利用预训练的模型进行微调，加快模型的训练速度和提高性能。

3.3.2 实时检测与动态更新机制

为了实现实时异常检测，需要优化模型的推理速度。可以采用模型压缩技术，如量化、剪枝等，减少模型的计算量和存储空间。同时，建立动态更新机制，根据AFC系统的实时数据和新的安全威胁，及时更新检测模型。例如，定期收集新的正常和异常数据，对模型进行增量训练，使模型能够适应不断变化的安全环境。此外，还可以采用在线学习的方法，让模型在运行过程中不断学习和调整，提高检测的实时性和准确性。

4 安全防护机制设计

4.1 安全防护体系架构

4.1.1 总体架构设计思路

基于AI的AFC系统安全防护体系采用分层防护和纵深防御的设计思路。从物理层、网络层、主机层、应用层和数据层等多个层面进行防护，形成综合性的安全保障体系。同时，结合AI技术的特点，将异常行为检测融入到各个防护层面，实现对安全威胁的实时感知和快速响应。

4.1.2 各层级安全防护重点

物理层安全防护主要关注AFC系统设备的物理安全，如防止设备被盗、被破坏等。采用门禁系统、监控摄像头等措施，确保设备所在环境的安全。网络层安全防护重点在于防止网络攻击，如DDoS攻击、网络窃听等。采用防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等技术，对网络流量进行监控和过滤。主机层安

全防护主要保护AFC系统的服务器和工作站，防止恶意软件感染、系统漏洞利用等。通过安装杀毒软件、定期更新系统补丁等方式，提高主机的安全性[4]。应用层安全防护关注AFC系统应用程序的安全，防止应用程序被篡改、注入攻击等。采用代码审计、安全编码规范等措施，确保应用程序的安全性。数据层安全防护重点在于保护乘客信息、交易数据等敏感数据的安全，采用数据加密、访问控制等技术，防止数据泄露和篡改。

4.2 安全防护技术措施

4.2.1 访问控制技术

基于AI的智能访问控制通过分析用户的行为模式、设备信息和网络环境，动态调整访问权限。例如，根据用户的操作习惯和历史访问记录，判断用户的访问请求是否合法。当用户的行为模式与正常模式不符时，限制其访问权限或要求进行二次认证。同时，结合多因素认证技术，如密码、指纹、人脸识别等，提高访问控制的安全性。

4.2.2 数据加密技术

采用先进的加密算法对AFC系统中的敏感数据进行加密处理。在数据传输过程中，使用SSL/TLS等加密协议，确保数据在传输过程中的安全性。在数据存储方面，对乘客信息、交易数据等进行加密存储，防止数据在存储过程中被窃取。同时，采用密钥管理技术，对加密密钥进行安全存储和定期更换，提高数据加密的安全性。

4.2.3 入侵检测与防御技术

基于AI的入侵检测系统能够实时分析网络流量和系统日志，识别出潜在的入侵行为。通过机器学习算法建立正常行为模型，当检测到与正常模型不符的网络流量或系统操作时，判定为入侵行为。入侵防御系统则能够自动阻止入侵行为的进一步发展，如阻断恶意网络连接、隔离受感染的设备等。同时，结合威胁情报技术，及时获取最新的安全威胁信息，提高入侵检测和防御的准确性。

4.3 安全防护管理策略

4.3.1 安全管理制度建设

制定完善的AFC系统安全管理制度，明确安全管理的职责和流程。包括人员管理、设备管理、数据管理等方面的制度。例如，制定人员准入制度，对进入AFC系统工作的人员进行背景调查和安全培训；建立设备采购、使用和维护的管理制度，确保设备的安全性；制定数据分类分级管理制度，对不同级别的数据采取不同的安全防护措施。

4.3.2 安全培训与意识提升

加强对AFC系统相关人员的安全培训，提高其安全意识和操作技能。培训内容包括安全政策法规、安全技术知识、安全操作流程等方面。定期组织安全演练，让人员在实际操作中熟悉安全应急处理流程。同时，通过宣传教育等方式，提高全体员工对AFC系统安全的重视程度，形成良好的安全文化氛围。

4.3.3 应急响应与处置机制

建立完善的应急响应与处置机制，确保在发生安全事件时能够快速、有效地进行应对。制定应急预案，明确应急响应的流程和责任分工。当发生安全事件时，立即启动应急预案，组织相关人员进行应急处置。同时，对应急事件进行及时的分析和总结，不断完善应急预案，提高应对安全事件的能力。

结语

本文围绕AI驱动的AFC系统异常行为检测与安全防护机制深入探究，分析了系统安全需求与威胁，设计了基于AI的异常行为检测模型和安全防护体系架构，在异常行为检测上采用多种AI算法实现实时准确识别，安全防护则从技术与管理两方面构建综合性机制。尽管取得一定成果，但仍有不足。未来将进一步优化检测模型，降低误报和漏报率；加强AI与其他安全技术融合；研究不同场景下的防护策略；开展跨区域安全防护研究，建立统一标准，推动城市轨道交通安全发展。

参考文献

[1]韩鹰.智慧化城市轨道交通AFC系统的应用研究[J].机械工程与自动化,2024,(02):155-156+159.

[2]卢肖静.“互联网+”新形态下AFC系统的创新应用[J].现代信息科技,2022,6(24):114-116.

[3]吕欢,吴松,郭戈,等.基于云平台的新一代智慧型AFC系统方案应用研究[J].现代城市轨道交通,2022,(04):72-77.

[4]黄俪,甘超莹.基于人工智能的图像识别技术在城市轨道交通AFC系统的应用[J].交通世界,2020,(22):23-24.