 DOI: https://doi.org/10.12349/iser.v7i6.10789

# Reflections on Security Risk Control Measures for Biometric Payment in Urban Rail Transit AFC Systems

**Huayu Xu**

CHONGQING TRANSPORTATION CONSTRUCTION MANAGEMENT CO.,LTD., Chongqing, 400042, China

**Abstract**

With the ongoing urbanization, the AFC system has become increasingly vital in subway operations, meeting the demand for convenient and secure payment solutions in rail transit. Biometric payment methods such as facial recognition, fingerprint authentication, and iris scanning—thanks to their uniqueness, convenience, and anti-counterfeiting capabilities—simplify fare payment processes and enhance passenger experience. However, these methods pose security risks including biometric data breaches and identity fraud, potentially infringing on users' rights. This paper analyzes the security risks associated with biometric payments in urban rail transit AFC systems and proposes targeted mitigation measures to improve payment security and reliability, thereby advancing urban rail transit toward digitalization and intelligent operations.

**Keywords**

urban rail transit; AFC system; biometric payment; security risks; control measures

# 城市轨道交通 AFC 系统中生物特征支付的安全风险控制措施思考

徐话雨

重庆交通建设管理有限公司，中国 · 重庆 400042

**摘　要**

随着城镇化不断推进，AFC系统在地铁运营中作用愈发重要，可满足轨道交通便捷、安全的支付需求。人脸、指纹、虹膜等生物特征支付，凭借唯一性、便捷性、难伪造的优势，简化乘车支付流程，优化乘客出行体验。但该支付方式存在生物数据泄露、特征信息伪造等安全隐患，损害用户合法权益。本文结合实际，分析城市轨道交通AFC系统内生物特征支付的安全风险，探究针对性防控措施，以此提升轨道交通支付的安全性与可靠性，助力城市轨道交通向数字化、智能化方向发展。

**关键词**

城市轨道交通；AFC系统；生物特征支付；安全风险；控制措施

## 1 引言

随着城市人口数量的增加，城市轨道交通客流承载力急剧增长，传统的支付方式已经不能满足现代化地铁交通发展需求。AFC 系统，即自动售检票系统是一种新兴的支付方式，该系统与生物特征支付相结合，能够通过自动识别人脸、指纹、虹膜等生物特征进行身份核验与费用结算，不需要乘客携带卡、票等，实现乘客便捷化交通，缩短检票时间，强化城市轨道交通的服务水平。但是这种支付方式应用过程中也存在一定的安全风险问题，如生物特征数据泄露、篡改、滥用，或者出现系统漏洞等问题，都会引起支付系统的潜在风险。因此需要采取科学合理的风险防控措施，充分发挥生物特征支付的价值作用，推动公共出行安全。

【作者简介】徐话雨（1991–），男，中国四川成都人，本科，工程师，从事自动售检票系统研究。

## 2 城市轨道交通 AFC 系统中生物特征支付的安全风险

城市轨道交通 AFC 系统中生物特征支付安全风险类型如表 1 所示。

### 2.1 生物特征数据泄露风险

（1）数据存储风险。AFC 系统需要把乘客的生物特征数据存储到数据库中，一旦数据库安全防护不当，会引起黑客攻击，引起生物特征数据泄露问题，甚至利用乘客数据信息进行非法活动，严重危害乘客的合法权益。其中，该环节的安全风险体现为弱密码、未及时更新安全补丁，同时没有对乘客原始生物特征数据进行去标识化、分片加密存储等处理，加大数据安全风险 [1]。（2）数据传输风险，在支付过程中，生物特征数据需要从采集终端传输到云端进行存储，

一旦在此过程中没有采取加密技术进行保护，会加大非法分子窃取、截取生物特征数据的风险几率；没有及时更新老旧 AFC 系统的加密协议，出现明文传输漏洞，引发数据泄露问题。（3）数据滥用风险。部分运营企业在支付范围外收集乘客数据信息，甚至将其共享给第三方机构用于商业营销、人像监控等用途，侵害乘客的信息自主权。部分内部人员违规下载、拷贝乘客数据信息，非法售卖获利，引发数据泄露风险。

**表 1 城市轨道交通 AFC 系统中生物特征支付安全风险类型**

| 风险类型 | 核心管控措施 | 技术 / 管理手段 |
|---|---|---|
| 活体欺骗攻击 | 多模态活体校验 | 3D 结构光、红外检测、动态动作校验 |
| 传输数据泄露 | 全程加密传输 | 国密算法、隧道专线、数据分片 |
| 生物信息泄露 | 杜绝原始数据存储 | 特征提取 + 模板加密、不可逆运算 |
| 系统漏洞入侵 | AFC 系统安全加固 | 漏洞扫描、防火墙、接口白名单 |
| 内部人为风险 | 权限隔离与审计 | 最小权限原则、操作日志、定期轮岗 |

### 2.2 技术攻击风险

（1）生物特征伪造攻击。非法分子伪造乘客的生物特征，骗取 AFC 系统的核验通过，冒用他人身份乘车，甚至存在盗刷风险。生物特征伪造类型包含：指纹伪造，即利用硅胶、凝胶等材料制作指纹模具，利用模具进行指纹识别，进而通过指纹识别系统验证；面部伪造，黑客通过深度学习算法生成逼真的虚假面具图像、视频，利用虚假信息进行面部识别，进行欺诈行为；虹膜伪造，利用高分辨率相机拍摄乘客虹膜图像，然后利用 3D 打印技术制作虹膜模型，进而绕过虹膜识别系统进行验证。（2）系统网络攻击风险，系统边缘节点和云端服务器存在安全漏洞，容易受到黑客网络攻击，如利用 DDoS 攻击瘫痪生物特征核验系统，导致车站闸机无法正常运行。同时，部分黑客攻击第三方服务商的信息系统，窃取用户的生物特征数据，引发批量盗刷攻击风险[2]。（3）深度伪造攻击风险。非法分子利用人工智能技术把泄露的生物特征数据生成高度仿真的动态生物特征，绕过当前大多数活体检测算法，对生物特征支付造成新型安全威胁。（4）系统漏洞攻击风险。软件漏洞，AFC 系统应用的软件程序存在很多漏洞，如缓冲区溢出漏洞、SQL 注入漏洞等，黑客利用这些漏洞攻击系统，篡改生物特征数据、窃取支付信息；硬件漏洞，如指纹识别设备传感器缺陷，黑客利用特殊方法干扰、欺骗，引发识别错误问题，硬件设备故障缺陷，引发黑客对设备的恶意攻击；网络漏洞，网络系统中没有设置防火墙、入侵检测系统等，黑客利用分布式拒绝服务供给、网络钓鱼等手段干扰地铁支付系统的正常运行。

### 2.3 运营管理风险

（1）用户注册过程中没有核验生物特征本人与账户所有人的一致性，容易发生冒用他人身份证注册生物支付的现象；（2）权限管理漏洞，AFC 系统访问权限没有设置分级管控，引发数据泄露风险。第三方运维服务商权限管控不到位，普通员工可以直接接触敏感数据，引发泄露风险。（3）缺乏应急预案，不能快速响应处置突发数据泄露、系统被攻击事件，加大风险扩散几率。

## 3 城市轨道交通 AFC 系统中生物特征支付安全风险防控措施

### 3.1 创新安全防护技术

（1）创新数据加密技术。常用的加密技术有：对称加密算法，如 AES 算法，该技术能够对数据快速加密处理，将加密数据存储出数据库并传输发送，接收方使用相同密钥解密，保证数据保密性；非对称加密算法，即利用公钥和秘钥，发送方利用秘钥签名，接收方利用公钥验证，保障数据传输完整性和安全性；混合加密方式，利用非对称加密算法交换对称加密算法秘钥，然后利用对称加密算法加密传输数据，保障数据安全性[3]。（2）生物特征活体检测技术，利用红外成像、3D 结构光、动态行为检测等新型技术手段，精准识别各类伪造攻击。针对指纹活体检测，对电容式与压力传感器相结合的方式，分别检测指纹纹路特征和按压压力变化，判断是否为活体；针对面部活体检测，需要通过红外活体检测技术识别面部皮肤温度、血液流动特点，然后利用动态交互检测技术要求用户做特定动作，分析动作流畅性，判断是否为活体；虹膜活体检测技术，即利用多光谱成像技术采集虹膜不同光谱图像信息，眼球运动检测技术检测眼球微小运动。针对深度伪造攻击，需要利用生成式人工智能对抗检测技术，强化对深度伪造生物特征的识别能力。（3）多因素认证技术，生物特征与动态令牌结合技术，即用户支付时输入动态密码，密码自动更新，确保两者一致才能完成支付；生物特征与短信验证码结合，系统向用户绑定手机发送短信验证码，在规定时间内输入正确验证码才能完成支付；生物特征与密码结合，用户输入支付密码，如面部识别通过后输入密码才能完成支付。（4）强化系统安全加固技术，开展等级保护测评，落实三级等级保护，定期进行漏洞扫描和渗透测试，及时修复安全漏洞并安装安全补丁，利用代码审计和漏洞扫描工具检测代码，修复潜在漏洞。安装防火墙和入侵检测系统，阻断非法网络访问，实时告警异常访问行为。强化对硬件设施的安全加固力度，利用硬件加密模块对数据进行加密；安全加固操作系统，设置强密码策略，限制

用户权限，设置复杂 root 密码。注重安装入侵检测技术和防御技术，其中包含 NIDA、HIDS、IPS，具体如表 2 所示。

**表 2 入侵检测技术和防御技术**

| 系统类型 | 全称 | 部署位置 | 核心功能 | 典型防护场景 | 响应方式 |
|---|---|---|---|---|---|
| NIDS | 基于网络的入侵检测系统 | 地铁 AFC 系统网络中 | 实时监测网络流量，分析数据包异常行为，通过规则库识别攻击 | 端口扫描、IP 欺骗、DDoS 攻击等网络层攻击 | 检测到异常后发出警报并启动防御 |
| HIDS | 基于主机的入侵检测系统 | 服务器、终端设备上 | 监测主机运行状态、文件完整性，检测异常进程与文件篡改 | 生物特征数据文件被恶意修改、主机异常进程 | 检测到异常后及时发出警报 |
| IPS | 入侵防御系统 | 网络链路中 | 实时监测流量，集成多维度检测与防御策略 | 各类可被识别的实时网络攻击 | 检测到攻击后立即阻断攻击流量 |

### 3.2 优化运营管理

为了保障支付系统安全，需要制定完善的安全管理制度，对不同部门、岗位的数据管理、支付安全职责和权限进行明确划分、具体落实，对生物特征数据的操作流程进行细化，如数据收集需要获得授权、数据存储需要利用加密技术、数据共享需要签订相关协议。此外要严格执行身份核验机制，尤其在乘客注册环节采用多种方式验证身份，如身份证核验、人脸活体验证、支付账户实名验证等，保障注册人就是生物特征本人。同时要完善权限分级管控机制，对内部人员的数据访问权限进行合理划分，落实最小权限、分级授权制度，工作人员只享有本职工作所需的最小数据访问权限。实施严格的操作日志审计制度，对访问操作留下可追溯的日志记录，定期审计日志内容，一旦发现异常行为需要及时处理。提高第三方机构的安全准入标准，明确第三方机构的数据安全责任，要求严格执行安全防护措施。要制定严格的应急响应处置机制，针对突发安全风险事件制定专项应急预报，明确应急处置流程与分工，定期开展应急演练，强化处置能力。

### 3.3 完善合规管理体系

建立完善的法律法规，明确生物特征数据的操作规则和标准，加大对违法行为的处罚力度，切实保障用户的合法权益。只有获得乘客同意后才能收集生物特征数据，保障乘客的知情权和选择权。强化监管与合作力度，对不同监管部门的职责和分工进行明确，强化支付全过程的监管力度，保障生物特征支付的合法、合规性。要定期展开安全合规评估工作，及时发现合规风险并及时整改，同时构建完善的个人信息保护影响评估制度，及时上报评估报告。完善行业标准和规范，统一生物特征数据的格式、加密方式等，强化支付系统的兼容性和互操作性。

## 4 结论

综上所述，为了提升城市轨道交通的支付安全，需要对 AFC 系统中的生物特征支付进行优化应用，并详细分析该系统运营过程中的风险类型，制定可行性的应对措施，优化法律规范建设，强化运营管理，保障城市轨道交通支付可靠性。

## 参考文献

[1] 邓冉然,程明硕,盛昊宇,等. 面向智慧运维的轨道交通AFC设备状态智能评估系统 [J]. 交通科技与管理, 2026, 7 (03): 10-12.

[2] 周驰华. 探究地铁自动售检票（AFC）系统的设计与实现 [J]. 中国科技论文在线精品论文, 2025, 18 (04): 165-167.

[3] 夏骏. 地铁AFC系统中的人脸识别检测技术应用 [J]. 集成电路应用, 2025, 42 (11): 118-120.