地铁AFC系统中生物特征支付的安全风险与防护策略

高丽丽　李亚昆
郑州交通发展投资集团有限公司　河南　郑州　450000

摘　要：本文聚焦于地铁自动售检票（AFC）系统中生物特征支付的安全问题。首先介绍了生物特征支付在地铁AFC系统中的应用现状与优势，接着深入分析了该支付方式面临的多种安全风险，包括生物特征数据泄露、伪造与欺诈、系统漏洞被利用等。随后着重从技术层面详细阐述了丰富且有效的防护策略，同时也从管理和法律层面提出相应措施，旨在全方位保障地铁AFC系统中生物特征支付的安全稳定运行，促进地铁交通的智能化发展。

关键词：地铁AFC系统；生物特征支付；安全风险；防护策略

1 引言

随着城市轨道交通的快速发展，地铁自动售检票（AFC）系统作为地铁运营的重要组成部分，其支付方式的便捷性和安全性越来越受到关注。生物特征支付作为一种新兴的支付方式，凭借其唯一性、便捷性和难以伪造等特点，逐渐在地铁AFC系统中得到应用。生物特征支付通过识别用户的生物特征信息，如指纹、面部、虹膜等，来完成支付过程，无需携带实体卡片或现金，大大提高了乘客的出行效率。然而，生物特征支付在带来便利的同时，也面临着诸多安全风险。一旦生物特征数据泄露或被恶意利用，将给用户带来严重的损失。因此，深入研究地铁AFC系统中生物特征支付的安全风险与防护策略具有重要的现实意义。

2 生物特征支付在地铁 AFC 系统中的应用现状与优势

目前，国内外部分城市地铁AFC系统已引入生物特征支付方式，如支持指纹或面部识别进站、出站和支付车费，乘客首次注册绑定生物特征信息后，后续乘车可快速完成支付，提高通行效率且降低运营方票卡成本。其优势显著：一是便捷性，无需携带额外支付工具，双手忙碌或忘带时优势更突出；二是唯一性，生物特征独一无二，难被伪造冒用，提升支付安全性；三是高效性，生物特征识别技术能快速识别验证，加快乘客通行，提高地铁运营效率。

3 地铁 AFC 系统中生物特征支付面临的安全风险

3.1 生物特征数据泄露风险

3.1.1 数据存储环节

地铁AFC系统需要存储大量乘客的生物特征数据，这些数据通常存储在系统的数据库中。如果数据库的安全防护措施不到位，如存在弱密码、未及时更新安全补丁等问题，就容易受到黑客的攻击，导致生物特征数据泄露。一旦黑客获取了乘客的生物特征数据，就可以利用这些数据进行非法活动，如伪造生物特征进行支付、冒用乘客身份等。

3.1.2 数据传输环节

在生物特征支付过程中，生物特征数据需要在不同的设备和系统之间进行传输，如从识别设备传输到后台服务器。如果数据传输过程中没有采用加密技术进行保护，就容易被中间人截取和窃取。例如，黑客可以通过搭建虚假网络环境，拦截乘客与地铁AFC系统之间的通信数据，从而获取乘客的生物特征信息。

3.1.3 数据共享环节

为了提高地铁运营的效率和便利性，地铁AFC系统可能会与其他相关系统进行数据共享，如与城市公共交通一卡通系统、银行支付系统等进行数据交互。在数据共享过程中，如果缺乏严格的安全管理和控制机制，就可能导致生物特征数据在共享过程中泄露[1]。例如，数据共享方的系统存在安全漏洞，或者数据共享协议不完善，都可能导致乘客的生物特征数据被非法获取。

3.2 生物特征伪造与欺诈风险

3.2.1 指纹伪造

指纹是生物特征支付中常用的一种生物特征。然而，指纹可以通过多种方式进行伪造，如使用硅胶、凝胶等材料制作指纹模具，然后利用模具进行指纹识别。一些高级的指纹伪造技术甚至可以复制出与真实指纹几乎一模一样的假指纹，从而绕过指纹识别系统的验证。

3.2.2 面部伪造

面部识别技术也是生物特征支付中广泛应用的技术之一。随着人工智能技术的发展，面部伪造技术也越来越成熟。黑客可以利用深度学习算法生成逼真的虚假面部图像或视频，然后通过这些虚假信息进行面部识别，从而实施欺诈行为。例如，黑客可以使用换脸技术将他人的面部图像替换到自己的视频中，然后通过面部识别

系统进行支付。

3.2.3 虹膜伪造

虹膜识别是一种高精度的生物特征识别技术，但虹膜也可以通过一定的方式进行伪造。例如，黑客可以使用高分辨率的相机拍摄乘客的虹膜图像，然后利用3D打印技术制作出虹膜模型，从而绕过虹膜识别系统的验证。

3.3 系统漏洞被利用风险

3.3.1 软件漏洞

地铁AFC系统中的生物特征支付功能通常依赖于各种软件程序来实现。这些软件程序可能存在各种漏洞，如缓冲区溢出漏洞、SQL注入漏洞等。黑客可以利用这些漏洞对系统进行攻击，获取系统的控制权，从而篡改生物特征数据、窃取支付信息等。

3.3.2 硬件漏洞

生物特征识别设备作为地铁AFC系统中生物特征支付的关键硬件，也可能存在安全漏洞。例如，一些指纹识别设备的传感器可能存在缺陷，容易被黑客通过特殊手段干扰或欺骗，导致识别结果错误。此外，硬件设备的固件也可能存在漏洞，黑客可以利用这些漏洞对设备进行恶意攻击。

3.3.3 网络漏洞

地铁AFC系统通常是一个复杂的网络系统，涉及多个子系统和设备之间的通信。如果网络系统存在安全漏洞，如未设置防火墙、入侵检测系统不完善等，就容易受到网络攻击。黑客可以通过网络攻击手段，如分布式拒绝服务攻击（DDoS）、网络钓鱼等，干扰地铁AFC系统的正常运行，导致生物特征支付功能无法正常使用。

3.4 法律法规与监管风险

3.4.1 法律法规不完善

目前，我国关于生物特征数据保护和生物特征支付的法律法规还不够完善。虽然已经出台了一些相关的法律法规，如《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》等，但对于生物特征数据的收集、存储、使用和共享等方面的规定还不够具体和明确。这导致在生物特征支付过程中，一旦出现数据泄露或欺诈等问题，用户的权益难以得到有效的保障。

3.4.2 监管难度大

生物特征支付涉及多个领域和行业，如地铁运营、金融支付、信息技术等。不同领域和行业的监管标准和要求存在差异，这给生物特征支付的监管带来了很大的难度[2]。此外，生物特征支付技术的发展速度非常快，监管部门难以及时跟上技术的发展步伐，导致一些新兴的生物特征支付安全问题无法得到及时的监管和解决。

4 地铁 AFC 系统中生物特征支付的防护策略

4.1 数据加密技术

（1）对称加密算法：生物特征数据存储和传输时，可用对称加密算法加密，如AES算法，加密速度快、效率高。存储时将加密数据存入数据库，传输时加密后发送，接收方用相同密钥解密，保证数据保密性。（2）非对称加密算法：使用公钥和私钥，可用于数字签名和密钥交换。发送方用私钥签名，接收方用公钥验证，确保数据完整性和真实性，还能安全交换对称加密算法密钥，提高传输安全性。（3）混合加密方式：结合二者优点，传输开始时用非对称加密算法交换对称加密算法密钥，再用对称加密算法加密传输数据，兼顾安全性与效率。

4.2 生物特征活体检测技术

（1）指纹活体检测：电容式与压力传感器结合，电容式检测指纹纹路和特征，压力传感器检测按压压力变化，真手指压力分布均匀有弹性，假手指则相反，通过分析压力数据判断是否活体。（2）面部活体检测：利用红外活体检测技术检测面部皮肤温度和血液流动，动作交互检测技术要求用户做特定动作（如眨眼、转头），分析动作是否自然流畅，判断是否活体。（3）虹膜活体检测：多光谱成像技术获取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（如瞳孔收缩扩张、眼球转动），真实虹膜和眼球有相应特性，假虹膜则无，以此判断是否活体。

4.3 多因素认证技术

（1）生物特征与密码结合：生物特征支付时，除生物特征识别外，要求用户输入支付密码，如面部识别通过后输入密码才能完成支付，增加安全性。（2）生物特征与短信验证码结合：支付时向用户绑定手机发送短信验证码，用户在规定时间内输入正确验证码才能完成支付，验证码有时效性和唯一性，防止冒用。（3）生物特征与动态令牌结合：用户支付时需输入动态令牌显示的动态密码，密码自动更新，如指纹支付时输入6位动态密码，两者正确才能完成支付。

4.4 系统安全加固技术

（1）软件安全加固：对地铁AFC系统软件安全加固，及时修复漏洞，定期更新升级，安装安全补丁。用代码审计和漏洞扫描工具检测代码，如用静态代码分析工具审计生物特征识别软件代码，修复潜在漏洞[3]。（2）硬件安全加固：对生物特征识别设备等硬件安全检测和维护，采用硬件加密模块加密数据，如在指纹识别设备集成加密芯片，加密存储和传输指纹数据。（3）操作系统安全加固：对地铁AFC系统所用操作系统加固，

关闭不必要服务和端口，设置强密码策略，限制用户权限，定期更新升级，安装安全补丁，如对Linux操作系统关闭Telnet、FTP等服务，设置复杂root密码。

4.5 入侵检测与防御技术

（1）基于网络的入侵检测系统（NIDS）：在地铁AFC系统网络部署NIDS，实时监测流量，分析数据包异常行为，设置规则库检测常见攻击（如端口扫描、IP欺骗、DDoS攻击），检测到异常发出警报并防御。（2）基于主机的入侵检测系统（HIDS）：在服务器和终端设备部署HIDS，监测主机运行状态和文件变化，检测异常进程、文件篡改等，如黑客修改生物特征数据文件时及时警报。（3）入侵防御系统（IPS）：主动网络安全设备，实时监测流量，集成多种检测和防御策略，检测到攻击立即阻断流量，防止系统受损。

4.6 管理防护策略

4.6.1 建立完善的安全管理制度

地铁运营方应建立完善的生物特征支付安全管理制度，明确各部门和人员在生物特征数据管理、支付安全等方面的职责和权限。制定详细的安全操作规程，规范生物特征数据的收集、存储、使用和共享等环节的操作流程。例如，规定生物特征数据的收集必须获得用户的明确授权，数据存储必须采用加密技术，数据共享必须签订严格的数据共享协议等。

4.6.2 加强人员培训与管理

加强对地铁AFC系统相关人员的安全培训，提高人员的安全意识和安全技能。培训内容包括生物特征支付安全知识、系统操作规范、应急处理流程等。同时，对人员进行严格的管理，实行权限分级管理，限制人员对生物特征数据的访问权限，防止内部人员泄露生物特征数据。例如，对系统管理员、操作员等不同岗位的人员设置不同的访问权限，只有经过授权的人员才能访问和处理生物特征数据。

4.6.3 定期进行安全评估与审计

定期对地铁AFC系统中的生物特征支付功能进行安全评估和审计，及时发现系统中存在的安全隐患和问题[4]。安全评估可以委托专业的安全评估机构进行，评估内容包括系统的安全性、合规性等方面。安全审计则可以对系统的操作记录、数据访问记录等进行审查，及时发现异常行为和安全事件。例如，每月对系统的操作日志进行审计，检查是否有未经授权的访问和操作行为。

4.7 法律防护策略

4.7.1 完善法律法规

政府应加快完善关于生物特征数据保护和生物特征支付的法律法规，明确生物特征数据的收集、存储、使用和共享等方面的规则和标准。加强对生物特征支付违法行为的处罚力度，提高违法成本，保障用户的合法权益。例如，制定专门的《生物特征数据保护法》，对生物特征数据的保护进行详细规定，明确数据收集者的责任和义务，对数据泄露等违法行为给予严厉的处罚。

4.7.2 加强监管合作

加强不同领域和行业监管部门之间的合作与协调，建立统一的生物特征支付监管体系。明确各监管部门的职责和分工，加强对生物特征支付全过程的监管，确保生物特征支付的安全、合规运行。例如，交通部门、金融部门、信息产业部门等可以建立联合监管机制，共同对地铁AFC系统中的生物特征支付进行监管。

4.7.3 推动行业标准制定

鼓励行业协会和相关企业制定生物特征支付的行业标准和规范，统一生物特征数据的格式、加密方式、安全要求等。行业标准的制定可以提高生物特征支付系统的兼容性和互操作性，促进生物特征支付行业的健康发展。例如，中国城市轨道交通协会可以组织相关企业和专家制定地铁AFC系统中生物特征支付的行业标准，规范生物特征支付的技术要求和应用场景。

结语

地铁AFC系统中生物特征支付具便捷、唯一、高效等优势，但也面临数据泄露、伪造欺诈、系统漏洞及法规监管等安全风险。为保障其安全稳定运行，需从技术、管理、法律层面采取防护策略。技术上，用数据加密、活体检测等手段提升安全性；管理上，完善制度、加强培训与评估、制定应急预案；法律上，完善法规、加强监管合作、推动标准制定。全方位防护可降低风险，促进地铁智能化发展。

参考文献

[1]张新曼,基于生物特征识别的移动支付安全系统.广东省,广东顺德西安交通大学研究院,2021-05-14.

[2]马怀清,曾庆宁.人脸识别与信用支付在AFC系统中的应用研究[J].现代城市轨道交通,2021,(S1):100-104.

[3]董文斌.重庆轨道交通AFC系统移动支付改造研究与应用[J].都市快轨交通,2020,33(03):138-143.

[4]李皓东.移动支付在城市轨道交通自动售检票系统中的应用探讨[J].通讯世界,2019,26(04):12-13.