

doi:10.1631/FITEE.1800580

题目：通过机器学习实现移动设备支付中绑定银行卡环节的欺诈侦测

概要：移动互联网技术的快速增长促进了移动支付的增长，也带来更多移动交易欺诈。作为移动交易的第一步，移动设备上的银行卡绑定已成为欺诈尝试的主要目标。虽然该环节的欺诈成功尝试不会立即造成资金损失，但直接导致后续的快速欺诈交易，且可以欺骗现有欺诈侦测系统。近年来，金融机构和服务提供商通过实施基于规则的专家系统，并采用短消息服务（SMS）认证用户身份解决这个问题。但是，上述解决方案不足以应对数据泄漏和社会工程的挑战。在本研究中，我们介绍了几种传统机器学习算法，最后选择改进的梯度增强决策树(GBDT)算法软件库用于实际系统，即XGBoost。基于对绑卡行为的分析进一步扩展了多个特征，并计划在未来研究中添加历史交易数据进行分析。使用了由全球支付处理商提供的2017年全年真实绑定银行卡的数据集，研究结果和框架已被上述全球支付处理商的移动支付欺诈侦测系统的新设计方案采纳。

关键词：欺诈侦测；移动支付；银行卡绑定；移动设备；梯度增强决策树（GBDT）；XGBoost