

人工智能在支付风险控制中的应用研究

徐 寅

杭州快速网络科技有限公司 浙江 杭州 310000

摘 要：随着支付行业发展，支付风险防控至关重要。人工智能以强大数据处理分析能力，为支付风险控制提供新路径。本研究聚焦其应用，先阐述支付风险控制基础理论，明晰风险类型与传统方法；再介绍人工智能技术原理及优势。着重探讨其在风险识别上，经特征提取、异常挖掘构建模型；在防控策略制定中，实现实时预警、动态策略生成与优化。研究显示，人工智能可提升支付风险控制精准性和时效性，助力支付行业安全运行，推动风险控制技术升级。

关键词：人工智能；支付风险控制；风险识别；防控策略

1 引言

在数字化经济推动下，支付领域变革深刻，新型支付方式普及，支付便捷性提升，风险却更趋多样复杂。传统支付风险控制方法在处理海量动态数据时，局限性渐显。人工智能以机器学习、深度学习为核心，凭借强大模式识别、数据分析与预测能力，为支付风险控制带来新途径。它能深度挖掘分析支付数据，精准识险并及时定策。当下，虽已有不少人工智能与支付风险控制融合的探索，但技术融合不深、模型泛化不足等问题仍存。故而，深入探究人工智能在支付风险控制中的应用，对增强支付安全性、推动金融科技发展有着关键意义。

2 支付风险控制基础理论

2.1 支付系统架构与流程

支付系统架构是实现支付功能的基础框架，涵盖了从用户端发起支付请求，到银行、第三方支付机构等中间环节的处理，再到资金最终结算的全过程。在架构方面，包括了账户体系、支付接口、清算系统等核心组件。账户体系用于管理用户资金和交易记录；支付接口负责与各类应用场景对接，实现便捷支付；清算系统则处理银行间、机构间的资金清分结算。其流程一般为用户选择支付方式，输入支付信息，系统验证后，经支付网关传输至银行或第三方支付机构进行资金划转，最终反馈支付结果给用户。不同的支付系统，如线上支付、线下移动支付等，在架构和流程细节上会有所差异，但都围绕着安全、高效完成资金转移这一核心目标构建。

2.2 支付风险类型与特征

支付风险类型多样。信用风险是指交易对手因信用状况不佳，无法按时足额履行支付义务，如商家无法提供约定商品或服务，用户拖欠款项等。欺诈风险表现为不法分子通过伪造身份、盗取信息等手段，骗取资金，像盗刷银行卡、网络钓鱼诈骗支付等。操作风险源于系统故障、人

员失误或内部管理不善，例如支付系统漏洞导致资金被盗取，员工操作失误造成转账错误等。市场风险则受宏观经济环境、汇率波动等影响，使支付涉及的资金价值发生变动。这些风险具有隐蔽性，初期不易察觉；突发性，可能在毫无预警时发生；以及传染性，个别风险事件可能引发连锁反应，影响整个支付生态的稳定^[1]。

2.3 传统支付风险控制方法

传统支付风险控制主要从制度和技术两方面着手。制度层面，建立严格的身份认证制度，要求用户提供身份信息并通过多种方式核验，如密码、短信验证码、生物识别等，以确认交易主体身份。同时，制定交易限额规则，限制单笔和单日交易金额，降低大额损失风险。在技术方面，采用加密技术，对支付信息进行加密传输和存储，防止信息泄露和篡改，如SSL/TLS加密协议。还运用规则引擎，设定一系列交易规则，如交易地点、时间、金额范围等，一旦交易不符合规则，系统自动预警或拦截。但随着支付业务的创新发展和技术迭代，传统方法在应对复杂多变的风险时，逐渐暴露出局限性，亟需新的技术手段赋能。如图一所示。

3 人工智能技术原理及优势

3.1 机器学习算法基础

机器学习是实现人工智能的关键路径。它运用各类算法解析大量数据并学习，以决策和预测现实事件^[2]。传统算法中，决策树以树形结构分类决策，依特征划分样本；聚类算法按相似性划分数据对象；贝叶斯分类基于贝叶斯定理，依据概率分类；支持向量机找最优超平面区分数据类别。从学习方式看，监督学习用有标签数据训练模型；无监督学习在无标签数据中找模式；半监督学习结合少量有标签与大量无标签数据；集成学习融合多模型提性能；深度学习借深层神经网络自动提特征；强化学习靠智能体与环境交互、依奖励学最优策略。

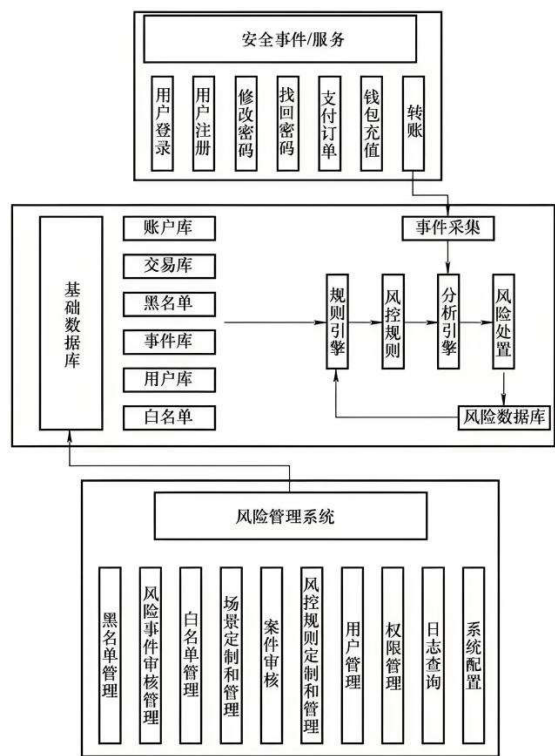


图1 传统风险管理系统架构图

3.2 深度学习模型架构

深度学习属于机器学习的范畴，其核心是深度神经网络。神经网络由大量神经元相互连接构成，神经元模仿生物神经元功能，对输入进行加权求和并通过激活函数输出。深度神经网络包含输入层、多个隐藏层和输出层。以多层感知机为例，它通过全连接层堆叠，可处理复杂的非线性映射问题。卷积神经网络（CNN）在图像、语音处理等领域表现卓越，利用卷积层提取局部特征，池化层进行降维，全连接层完成分类或回归任务。循环神经网络（RNN）及其变体长短时记忆网络

（LSTM）、门控循环单元（GRU），擅长处理序列数据，如时间序列、自然语言等，通过记忆单元捕捉序列中的长期依赖关系。生成对抗网络（GAN）由生成器和判别器组成，二者相互博弈，在图像生成、数据增强等方面有广泛应用。如表一所示：

表1 深度学习模型类型表

模型类型	结构特点	优势
卷积神经网络（CNN）	包含卷积层、池化层、全连接层等，通过卷积核提取数据特征	对图像、序列数据特征提取能力强
循环神经网络（RNN）及其变体（LSTM、GRU等）	具有记忆单元，能处理时间序列数据	适合分析随时间变化的交易数据
Transformer	基于注意力机制，不依赖循环结构，能并行处理数据	对长序列数据处理效果好，计算效率高

3.3 人工智能应用于支付风险控制的优势

人工智能在支付风险控制中优势显著。首先，具备强大的数据处理能力，能实时处理海量支付交易数据，从庞大且复杂的数据中快速提取关键信息，挖掘潜在风险模式。其次，具有高度的准确性，通过不断训练和优化模型，可精准识别欺诈交易、异常账户行为等风险，降低误判和漏判概率。再者，人工智能系统可实现 7×24 小时不间断运行，不受人为因素干扰，持续监测支付流程，及时响应风险事件。此外，其具有良好的适应性，能根据新出现的风险特征和欺诈手段，自动更新和优化模型，迅速适应支付风险环境的动态变化^[3]。最后，人工智能可通过综合多维度数据进行分析，提供全面的风险评估，为制定更有效的防控策略提供有力支持。如表二所示：

表2 人工智能应用于支付优势表

优势方面	描述	提升效果（与传统方法对比）	应用案例
处理速度	能快速处理海量交易数据，实现实时风险监测	风险监测延迟从分钟级缩短至秒级	某支付机构采用人工智能后，交易处理速度提升5倍
准确性	通过复杂算法和模型学习，精准识别风险	风险识别准确率从70%提升至90%	某银行利用人工智能，欺诈交易识别准确率大幅提高
适应性	可根据新数据和风险模式自动更新模型，适应变化	模型更新周期从月缩短至周	某金融科技公司的风控模型能快速适应新的欺诈手段

4 人工智能在支付风险识别中的应用

4.1 基于特征提取的风险识别

支付交易数据蕴含着海量信息，基于特征提取的风险识别是关键环节。首先，从交易金额、时间、地点、频率等基础维度入手，分析异常大额交易、高频短时间交易以及跨地域异常交易等情况。例如，在极短时间内出现多笔超出用户常规消费习惯的大额交易，可能存在盗刷风险。其次，关注交易主体特征，包括用户历史交易行为习惯、信用评级等^[4]。新用户或信用不良用户的异常交易需重点排查。再者，提取设备特征，如交易使用的设备类型、设备位置变动等。若一台设备频繁在不同地理位置登录进行支付操作，可能是设备被盗用。通过全面、细致地提取这些特征，构建特征向量，为后续风险判断提供依据。

4.2 异常交易行为模式挖掘

异常交易行为模式挖掘旨在发现支付过程中偏离正常模式的行为。一方面，利用聚类算法对大量正常交易行为进行聚类分析，确定正常交易行为的模式范围。例如，将用户日常消费的商品类别、消费时段等进行聚类，若出现明显不属于该聚类范围的交易，如平时只购买生活用品的用户突然大量购买奢侈品，可能存在异常。另一方面，运用序列模式挖掘算法，分析交易行为的先后顺序和关联规则。如某些特定商品组合的交易顺序异常，或在特定促销活动期间出现不符合常规逻辑的交易顺序，可能是欺诈行为。此外，结合时间序列分析，观察交易行为随时间的变化趋势，对于突然出现的异常波动，如短时间内交易数量或金额的大幅增长，深入挖掘背后原因，精准识别异常交易行为模式。

4.3 风险识别模型构建与评估

构建风险识别模型时，依据提取特征和异常交易模式，选用合适机器学习算法，如决策树、支持向量机、神经网络等。像决策树，通过逐层划分交易数据特征构建分类模型判断风险。构建后严格评估，用交叉验证划分数据集为训练集和测试集，在训练集训练、测试集验证。以准确率、召回率、F1值等指标评估，准确率看正确识别比例，召回率关注识别全部风险交易能力，F1值综合二者。通过调整参数、优化算法，提升模型泛化能力与风险识别准确性，保障其在支付风险控制中有效运作^[5]。

5 人工智能在支付风险防控策略制定中的应用

5.1 实时风险预警机制

人工智能通过对支付系统中实时产生的海量交易数据进行高速处理与分析。借助机器学习算法，持续学习

正常交易行为模式，一旦监测到交易数据偏离已建立的正常模式，如交易地点异常变动、交易时间不符合常规规律、交易金额短时间内大幅波动等情况，能迅速触发预警。例如，当用户习惯在本地消费，却突然出现一笔远在国外的大额交易时，人工智能系统可及时识别并发出警报，提醒支付机构采取进一步措施，如暂停交易、要求用户进行身份二次验证等，有效降低欺诈等风险发生的可能性，为支付风险防控争取宝贵的应对时间。

5.2 动态防控策略生成

依据人工智能对支付风险的实时识别结果，能够动态生成针对性的防控策略。不同类型的风险，如账户被盗用风险、欺诈交易风险、洗钱风险等，其防控策略各不相同。针对账户被盗用风险，系统可自动采取临时冻结账户、更改登录密码等措施；对于欺诈交易风险，可能会限制交易额度、要求提供更多交易凭证等。同时，人工智能还能结合支付场景、用户信用等级等多维度信息，灵活调整防控策略。例如，对于高信用等级用户，在风险较小时可能仅采取提醒措施；而对于信用等级较低或风险较高的情况，则采取更为严格的管控手段，确保防控策略的科学性与有效性。

5.3 防控策略效果评估与优化

通过对支付风险防控策略实施后的效果进行持续评估，人工智能可以判断策略是否达到预期的风险降低目标。评估指标包括风险识别准确率是否提升、欺诈交易损失是否减少、用户对防控措施的接受程度等。若发现当前防控策略效果不佳，如误报率过高影响用户体验，或漏报导致部分风险未被有效拦截，人工智能可基于评估结果，自动调整相关算法参数、优化模型结构，或引入新的数据维度进行分析，从而对防控策略进行优化。持续的评估与优化过程，能使支付风险防控策略不断适应复杂多变的支付环境，始终保持良好的防控效果。

6 结语

本研究围绕人工智能在支付风险控制中的应用展开深入剖析。明确了人工智能凭借强大的数据处理与分析能力，显著提升支付风险识别精准度与防控效率，能通过实时风险预警、动态策略生成以及策略效果评估优化，有效应对复杂多变的支付风险。然而，当前人工智能在支付风险控制中的应用仍存在一些不足，如模型的可解释性有待提升，数据隐私保护面临挑战等。未来，随着技术的不断发展，应着力解决现存问题，进一步挖掘人工智能潜力，持续完善支付风险控制体系，为支付行业的稳健发展提供更坚实的保障，推动支付风险控制

迈向新高度。

参考文献

[1]苏小坡.人工智能技术在电力安全风险控制中的应用[J].计算机应用文摘,2025,41(5):76-78.

[2]贺育斌.人工智能技术在电商平台风险控制中的应用与实践研究[J].商展经济,2024(22):67-70.

[3]包俊先,洪虹.生成式人工智能在电商行业中的应用现状和风险研究[J].老字号品牌营销,2024(7):55-57.

[4]唐滴.人工智能在网络支付数据处理和隐私保护中的应用研究[J].电子商务评论,2024,13(4):4402-4407.

[5]范玉民.人工智能在支付清算风险管理中的设计研究[J].北方金融,2022(7):96-99.