浙 江 大 学 学 报（工学版）
Journal of Zhejiang University (Engineering Science)

金融行为欺诈检测技术综述

沈韵泓

（浙江大学 工程师学院，浙江 杭州 310058）

摘 要：随着电子商务、在线支付和移动金融的快速发展，越来越多的交易活动被转移到线上渠道。这种无现金、无接触的交易方式虽然便利，但也为针对金融产业的欺诈行为提供了更多的机会和便利条件。为此，研究人员在过去的几十年中向金融欺诈检测模型中引入各种统计学与机器学习方法。然而，随着互联网和大数据技术的发展，金融欺诈的手段也逐渐变得多样化、智能化，传统的欺诈检测技术已不能提供足够的安全保障、对先进欺诈检测系统的需求显得尤为迫切。本文旨在对现有的金融欺诈检测技术及评估指标进行全面调研综述，并对该领域的前景进行展望。

关键词：金融欺诈；异常检测；机器学习；深度学习；神经网络

中图分类号：TP 391　　**文献标识码：**A　　**文章编号：**

A Survey of Financial Fraud Detection Techniques

SHEN Yunfeng

(*College of Engineers*, *Zhejiang University*, *Hangzhou 310058*, *China*)

Abstract: The rapid development of e-commerce, online payments, and mobile finance has led to a significant shift of transaction activities to online channels. While convenient, this cashless, contactless method has also provided more opportunities for fraud in the financial sector. Various statistical and machine learning methods have been introduced into financial fraud detection models by researchers over the past few decades. As internet and big data technologies have advanced, financial fraud methods have become more diversified and intelligent, making traditional detection techniques insufficient in ensuring security, and thus, the need for advanced systems has been highlighted. A comprehensive review of existing financial fraud detection technologies and evaluation metrics is provided, and an outlook on the field's future is offered.

Key words: Financial Fraud; Anomaly Detection; Machine Learning; Deep Learning; Neural Network

1 研究背景与意义

随着金融科技的快速发展和全球金融体系的日益复杂化，金融欺诈行为呈现出高发性、隐蔽性和多样化的特点。数字化支付的普及、金融产品的创新以及跨境交易的增加，为欺诈者提供了新的可乘之机。根据国际金融犯罪执法网络的报告，金融欺诈每年造成的经济损失高达数千亿美元，严重威胁金融机构和消费者的利益。因此，开发高效、智能的金融欺诈检测技术成为当前金融领域亟待解决的重要问题。

金融欺诈不仅导致金融机构的直接经济损失，还损害消费者信心，影响金融市场的稳定性。普华永道发布的《2022 年全球经济犯罪调查报告》指出，超过 50%的金融机构在过去两年内遭受了严重的欺诈攻击[1]。此外，各国政府和监管机构对金融行业的合规性和反欺诈要求日益严格。例如，《反洗钱法》和《通用数据保护条例》要求金融机构必须采取有效措施防范和检测欺诈行为，否则将面临巨额罚款和法律诉讼。与此同时，金融欺诈手段不断升级，传统的基于规则的检测方法已无法应对高维、非线性和动态变化的新型欺诈行为。因此，研究先进的金融欺诈检测技术不仅是金融机构的迫切需求，也是满足监管要求和维护金融市场稳定的重要手段。

本文将对金融欺诈检测技术领域的研究现状进行回顾，并提供结构化的概述。第二节将以使用的主要机器学习为分类依据，对不同的金融欺诈检测技术进行介绍，第三节将介绍金融欺诈检测领域常用的数据集与评估指标，第四节将对该领域发展现状进行总结，并为未来的研究方向进行展望。

2 国内外研究现状

2.1 基于传统机器学习算法

2.1.1 支持向量机 支持向量机（Support Vector Machine，SVM）是一种强大的监督学习算法。该方法利用核函数（kernel function）将数据映射到更高维度以处理非线性可分数据，使其既能处理非线性可分数据，又无需实际进行复杂的高维计算。此外，通过调节正则化参数，SVM 还能选取最大化两类间隔的超平面、有效减少过拟合。

Sahin 等[2]首次将 SVM 算法应用于信用卡欺诈检测任务，在采样自国有银行的数据集上将其性能与决策树方法进行对比。研究人员首先通过特征工程技术选取用以区分欺诈与合法交易的最优特征，随后基于选取特征对样本进行分层。由于实验数据集中的合法交易样本远多于欺诈样本，研究人员通过分层抽样对合法交易样本进行欠采样，使其数量变得有意义。其实验结果表明 SVM 在小样本场景下倾向于过拟合数据，该现象将随数据量上升得到缓解。

Lu 等[3]提出了一种适用于信用卡欺诈检测任务的不平衡类别加权 SVM（Imbalance Class Weighted SVM，ICW-SVM）方法。为解决数据集的大规模、高维度挑战，作者引入主成分分析（Principal Component Analysis，PCA）技术以捕捉原始特征中的五个关键特征（账户负面信息、客户持卡情况、交易频率、交易频率、客户基本信息），从而实现降维。不同于以往的工作，ICW-SVM 并没有采用欠采样技术解决数据不平衡问题，而是通过调整合法类和欺诈类的权重改变 SVM 提取的超平面位置。作者在采样自一家商业银行的不平衡信用卡数据集上将 ICW-SVM 与标准 SVM 算法、决策树算法进行比较，取得了最优的准确率与召回率，并证明基于 PCA 的 ICW-SVM 具有更高的执行效率。

Hejazi 等[4]引入了单类支持向量机（One-Class SVM，OCSVM）[5]方法。不同于标准 SVM 算法，再将数据通过核函数映射到特征空间后，OCSVM 仅在数据点与原点间选取一个超平面，并将所有未归入该类的数据划分为异常类。作者在由加州大学欧文分校提供的德国信用卡数据集上对比了标准 SVM 与 OCSVM 方法，并证明后者拥有更好的准确率与泛化性。

在此基础上，Sundarkumar 等[6]将 OCSVM 与 K-逆近邻（k- Reverse Nearest Neighbours，kRNN）算法结合，提出了一种新型的混合欠采样方法。其中，kRNN 用于从训练集的多数类中识别并去除离群点，而 OCSVM 则用于数据降维、隐式完成欠采样。最终的训练集由全部少数类样本与去除离群点后的多数类样本合并后得到。作者在 Phua 等[7]提出的汽车保险索赔欺诈数据集上将此欠采样技术与 SVM、LR、决策树等方法进行融合，成功提高了所有种类分类器的整体预测性能。

Ryali 等[8]则在信用卡欺诈检测任务中将随机森林（Random Forest，RF）算法与 SVM 结合的方法。其中，RF 算法通过重要性得分选取非冗余鲁棒特征，从而实现数据降维。相较于决策树、局部离群因子（Local Outlier Factor，LOF）等方法，该 RF+SVM 方法成功在来自 Kaggle 的欧洲信用卡交易数据集上取得了最优的预测准确率与鲁棒性。

2.1.2 *孤立森林算法*　孤立森林（Isolation Forest，IF）算法是 Liu 等[9]于 2008 年提出的一种无监督方法。该方法通过构建由多棵孤立树（iTree）构成的集合检测异常点，其核心原理是利用随机选择特征和分割值递归地划分数据，使得异常点因特征较少而易被隔离。通过计算数据点在所有孤立树中的平均路径长度，得出异常评分以筛选异常点。IF 在计算效率、抗噪能力及处理无标注数据上存在优势，适用于处理高维和大规模数据集。

Ounacer 等[10]首次将 IF 算法用于信用卡欺诈检测任务。该方法首先使用 PCA 算法除交易时间与金额以外的所有输入特征，随后计算测试样本在所有隔离树中的路径长度，进而预测值域介于 0 到 1 之间的异常得分、以 0.5 为阈值对样本进行分类。在 Kaggle 提供的欧洲信用卡数据库上进行的实验证明 IF 具有比 OCSVM、LOF 等方法更强的预测性能。

Stripling 等[11]则将 IF 算法用于工人保险赔偿欺诈任务。不同于文献 10 中将 IF 直接作为分类器的做法，该方法将 IF 计算得到的异常分数作为新的特征加入训练集以实现数据增强。在采集自真实欧洲组织工人保险索赔数据上进行的实验表明，引入 IF 预测的异常分数能支持模型从无标注数据中发现被人类专家忽略的欺诈样例。

2.1.3 *朴素贝叶斯算法*　朴素贝叶斯（Naïve Bayes，NB）算法通过学习每个特征在给定类别标签下的条件概率实现分类，其前提假设为“特征间相互独立”。尽管该假设对于多数领域而言过于严苛，但 NB 分类器在多数不符合独立性假设的场景下仍表现出色，且在小规模数据集上仍能取得良好表现。

Viaene 等[12]首次将 NB 分类器应用于汽车保险欺诈任务，提出了 ABWOE 模型。通过分阶段扰动数据，NB 分类器可以逐渐聚焦于更难以学习的数据；而 AdaBoost[13]方法则令每个 NB 分类器的投票可以根据其分类质量自适应加权，使预测结果更加可解释。在马萨诸塞州汽车保险索赔数据集上进行的实验证明 ABWOE 模型在所有指标上均超过了单独的 NB、AdaBoost 方法。

2.1.4 *隐式马尔可夫模型*　隐式马尔可夫模型（Hidden Markov Models，HMM）通过建模隐状态序列与观测序列间的概率关系完成对时序数据的建模。该模型假设系统为马尔可夫过程、且

当前观测值仅依赖于当前的隐状态，通过状态转移矩阵、观测概率矩阵和初始状态分布刻画系统。

Srivastava 等[14]通过多项式 HMM 对用户的信用卡操作序列进行建模，从而实现信用卡欺诈检测。该方法基于每个持卡人的合法交易记录为其训练一个单独的 HMM 作为用户消费行为画像，并将未被 HMM 以足够高概率接受的交易视为欺诈。研究人员首先通过 K-means 聚类算法确定当前用户的高、中、低消费范围，随后根据用户购买的商品类型构建状态转移矩阵。该研究的验证实验在虚拟数据集上进行，研究人员通过构建不同长度的交易序列以训练具有不同状态数量的 HMM 模型，并验证了方法的有效性。之后的研究（如，文献[15]和文献[16]）则在真实信用卡交易数据集上验证了基于 HMM 方法的有效性，并进行了适当扩展（如，支持实时监测）。

Lucas 等[17]则提出了一种结合了 RF 算法的自动化信用卡欺诈检测方法。该方法从三个角度对信用卡交易序列进行建模：当前交易序列与完全合法序列及至少包含一次欺诈交易序列的相似性、持卡人与客户终端的交易序列特征、两次交易间间隔与交易金额，并根据上述角度训练了 8 个 HMM 模型，用于根据之前的交易序列为当前交易分配似然值。这些似然值随后将作为附加特征以增强 RF 分类器结果。在来自行业合作伙伴的真实数据集上进行的实验证明该方法能有效提高模型的预测性能。

2.2 基于深度神经网络算法

2.2.1 *多层感知机* 多层感知机（MultiLayer Perceptron，MLP）是最简单的神经网络模型，通过多层非线性变换学习输入数据的复杂表示。

Maes 等[18]首次将 MLP 应用于信用卡欺诈检测任务，尽管相关实验显示 MLP 的效果要逊色于贝叶斯网络，但其在训练耗时上的优势还是引发了相关研究人员的关注。其后的相关研究（如，文献[19]、文献[20]）也在多个数据集上验证了 MLP 在信用卡欺诈检测任务中的有效性。

随后的研究则更加注重于对标准 MLP 进行改进，从而获得更优的预测性能。Behera 等[21]提出了将模糊聚类与 MLP 相结合的混合模型 FCM-MLP。其中，模糊聚类（Fuzzy c-means，FCM）是一种允许每个样本同时属于多个类别的聚类形式。该模型共分为两个阶段：模型将首先根据交易金额与购买物品对交易进行 FCM 聚类，并根据与各类质心的欧式距离计算怀疑分数；随后分别基于阈值和 MLP 模型分别对交易进行粗筛和细分。该模型在较大规模的交易数据集上取得了较好的表现。Gómez 等[22]通过连接一组神经网络集合和一个 MLP 分类器构建了一个级联过滤模型。其中，神经网络集合被用于尽可能多的分类合法交易并拒绝，同时保留欺诈样本；MLP 则用于进一步判定欺诈样本的真实性。

2.2.2 *长短期记忆网络* 长短期记忆网络（Long Short-Term Memory，LSTM）是循环神经网络（Recurrent Neural Network，RNN）的扩展，解决了 RNN 在长序列训练中遇到的梯度消失和梯度爆炸问题，同时通过引入门控机制和细胞状态实现了对长距离依赖关系的有效捕捉，已被广泛应用于各种时序数据处理任务。

Wiese 等[23]是最早将 LSTM 用于信用卡欺诈检测的研究者，认为将交易序列作为整体进行的 LSTM 网络能捕捉更多的时序联系、并对合法消费行为中存在的微小扰动具有更强的鲁棒性。此外，作者还提出了用于衡量特定时间间隔内发生的交易数量的额外特征“交易速度”。相较于 SVM 和 MLP 方法，基于 LSTM 的检测方法具有更高的检测准确度与预测速度，但训练速度稍逊。在该研究的 LSTM 模型中，作者仅设置了两个仅包含两个记忆细胞的记忆块，参数量极小。作者认为这样的设置为将初步欺诈检测模型部署在支付卡芯片上提供了可能性，有助于构建真正的实时在线欺诈检测系统。

Jurgovsky 等[24]将 LSTM 模型与 Bahnsen[25]等转为信用卡欺诈模型设计的特征聚合策略相结合。该策略会根据卡号、交易类型、国家等标准对交易进行分组、并统计交易总量，同时提出了将交易时间建模为周期性变量以确定周期平均值的方法。此外，作者在面对面交易和电子交易两种数据集上对比了 RF 与 LSTM 模型的性能，并指出前者的检测结果一致性更高，而后者能覆盖更多的欺诈行为种类。

2.2.3 卷积神经网络　由于卷积神经网络（Convolutional Neural Network，CNN）的输入通常为矩阵格式，CNN 通常被应用于基于图像的模式识别任务。但通过适当调整输入数据结构，CNN 也可被应用于其他领域（如，语音处理、推荐系统、自然语言处理等）。一个 CNN 模型通常包括卷积层、池化层和全链接层三部分，其中：卷积层通过不同的卷积核提取不同角度的输入特征，池化层则用于降低特征图维度以减少参数量、控制过拟合，全连接层则基于池化层输出对样本进行更细致的分类。

CNN 在金融欺诈检测中的应用起步较迟，直至 2016 年 Fu 等[26]才首次将 CNN 应用于信用卡欺诈检测任务，以应对 MLP 造成的过拟合困境。该模型通过将一维交易序列切分为多个时间窗口的方式将其转化为特征矩阵，以满足 CNN 对输入格式的要求。此外，研究者还提出了一种被称为交易熵的新特征以描述单个用户与一段时间内总交易金额间的关系。在真实商业银行信用卡数据集上的实验证明使用交易熵的 CNN 模型的性能优于 MLP、SVM 等其他方法。

Heryadi 等[27]进一步对比了 CNN、LSTM 及混合模型的欺诈预测性能。在混合模型中，样本将首先通过 CNN 的处理，再送入 LSTM 进行分类，以同时利用二者在捕捉短期和长期时序关系中的优势。实验结果表明，仅 CNN 模型取得了最高的 AUC 得分，作者将其归结于信用卡欺诈交易的短期特质与 CNN 在捕捉短期趋势上优势的一致性。

2.2.4 生成对抗网络　生成对抗网络（Generative Adversarial Network，GAN）由两个相互竞争的神经网络构成。其中，生成模型用于捕捉训练数据分布，并输出尽可能贴合真实数据的合成数据；判别模型则通过最小化判别误差以更准确的对真实数据与生成数据作出区分。在大多数场景中，GAN 作为过采样方法应用于金融欺诈检测任务。

Chen 等[28]首次将 GAN 引入金融欺诈检测领域。该方法通过稀疏自编码器（Sparse Auto Encoder，SAE）提取合法交易表征以训练 GAN 模型，其中的判别网络需要对真实合法交易与生成合法交易作出区分。在欧洲信用卡数据集上的实验表明，基于 GAN 的模型拥有比 OCSVM 更优的预测性能，且预测精度随 SAE 中隐藏层神经元数量的增加而提高。类似的，Charitoud 等[29]将 SAE-GAN 结构应用于反洗钱任务，在 F1 得分与准确性上均优于其他模型。

此外，Ba[30]将使用以推土机距离（Wassertein Distance）为度量误差的 Wasserstrin GAN 模型应用于信用卡欺诈检测，在 F1 得分与 AUC 指标上取得了较优表现。Zheng 等[31]则提出了一种基于自编码器的单类对抗网络 AE-OCAN，通过训练两个互补的 GAN 模型检测信用卡欺诈交易，性能优于其他单类方法。

2.3 基于图的方法

由于洗钱、保险等金融欺诈场景往往涉及多个与用户相关的实体，基于图的模型在此类问题的建模上具有天然的优势：图模型可以通过不同类型的节点和边对异构数据进行建模。此外，结合时序特征构建的动态图可以对用户行为及关系的时序变化进行建模，为其未来动向预测提供更鲁棒且可解释的结果。因此，基于图的金融欺

诈检测技术的流行度不断上升。

在汽车保险索赔欺诈任务中，Šubelj 等[32]提出了一种基于社交网络图结构的专家系统。作者分别为司机、乘客与车辆构建了三个独立的网络，以观察不同个体和群体间的潜在联系。此外，作者还提出了一种新型的迭代评估算法以实现对单个实体节点是否涉嫌欺诈的预测，但需要领域专家根据先验知识设置阈值。该模型无需数据标注，亦不要求大量数据，具备极高的适用性。

在反洗钱任务中，Dreżewski 等[33]提出了社交网络分析（Social Network Analysis，SNA）算法，以检测潜在的洗钱活动。作者认为金融欺诈者通常会构建复杂的社会组织，而这类组织结构及每个成员的细分角色都可以通过 SNA 进行识别。为此，作者基于从银行对账单和法院登记册等多种数据源获取的数据为部分节点分配角色，并根据节点接近度模块的预测结果为未知节点分配角色类别。在此基础上，Colladon 等[34]探究了 SNA 在预防洗钱上的应用，重点考虑了债务人与保理公司间的资金动向、并构建了用以反应四种不同维度风险的关系图：经济活动种类、特定地理位置、交易金额及相同所有者持有的不同公司。经过滤后，这些图可以帮研究者重点关注具有更高交易风险的集群。在特定集群的任一节点涉及可疑操作时、立刻检查集群中的其他节点将有助于预防尚未发生的洗钱活动。

3 常用数据集与评估指标

3.1 真实数据的缺失

金融数据（如交易记录、用户信息）通常包含用户的个人隐私和财务信息、具有高度敏感性。一旦泄露，可能导致用户隐私被侵犯、财产损失甚至法律纠纷。金融数据同时也是金融机构的核心资产，具有极高的商业价值。公开数据可能削弱其竞争优势，甚至被竞争对手利用。

此外，各国对金融数据的隐私保护有严格的法律要求。例如，欧盟的《通用数据保护条例》（GDPR）和美国的《金融服务现代化法案》（GLBA）都对金融数据的收集、存储和使用提出了严格要求。即使对数据进行匿名化处理，仍可能通过数据关联分析还原用户身份，这使得金融机构在数据共享方面持谨慎态度。

因此，现有研究大多选择不公开其使用的数据集，或在合成数据集[35,36,37]上进行验证。

3.2 常用评估指标

多数金融欺诈检测研究会将任务定义为二分类任务，其常用评估指标如下：

准确率（Accuracy）用于衡量模型预测结果与真实标签的一致性，定义为正确预测样本数在总样本中所占的比例：

$$\text{Accuracy}=\frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \tag{1}$$

式中：TP（True Positive）为模型正确预测为正类的样本数，TN（True Negative）为模型正确预测为负类的样本数，FP（False Positive）为模型错误预测为正类的样本数，FN（False Negative）为模型错误预测为负类的样本数。

召回率（Recall）用于衡量模型是否能尽可能多的捕捉所有正样本：

$$\text{Recall}=\frac{\text{TP}}{\text{TP}+\text{FN}} \tag{2}$$

精确率（Precision）用于衡量模型预测为正类中真正正类样本所占的比例，特别适用于需要减少误报的场景：

$$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}} \tag{3}$$

F1 得分（F1 Score）是召回率与精确率的调和平均数，特别适用于数据不平衡、或需要平衡精确率与召回率的场景：

$$\text{F1 Score}=2\times\frac{\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \tag{4}$$

曲线下面积（Area Under Curve，AUC）是以真正例率（True Positive Rate，TPR）为纵轴、以假正例率（False Positive Rate，FPR）为横轴的 ROC 曲线（Receiver Operating Characteristic Curve）下的面积，用于衡量模型在不同分类阈值下的整体性能。取值范围介于 0 至 1 之间，且越接近 1 时，模型的分类性能越优异。

类似的，我们可以用 PR 曲线（Precision-Recall Curve）下的面积定义参数 **AUPRC（Area Under the Precision-Recall Curve）**在不同分类阈值下模型对召回率和精确率的平衡能力。AUPRC 的取值范围同样介于 0 至 1 之间，且越接近 1 时，模型越能准确的分辨正负样本。

其余将金融欺诈检测定义为聚类任务的研究则会采用样本与聚类中心间的欧氏距离、曼哈顿距离及距离的均方误差等参数，对模型的性能进行评估。

4 结　语

本文首先强调了在当前时代背景下金融欺诈检测技术的重要性，随后以使用的主要机器学习为分类依据，对不同的金融欺诈检测技术进行分类介绍，以帮助读者了解在信用卡欺诈、保险欺诈和洗钱领域的最新研究进展。

从综述的文献不难看出，相较于传统的机器学习方法，基于深度学习的金融欺诈检测架构正在不断变得流行、一些混合方法也不断涌现。然而，相较于传统机器学习算法，深度学习模型对数据质量有着更高的要求。这为大规模数据集的构建及数据的准确标注带来了巨大挑战，一些研究人员也因此开始了对无监督学习方法的探究。

此外，深度学习模型的黑箱特性使决策过程与决策依据变得不透明，在金融领域中不具备足够的可信度。因此，如何构建一种可解释的欺诈检测模型也将是该领域的一个重要研究方向。

随着自然语言处理技术的发展，通用大模型已被引入金融用户画像构建、金融智能客服、智能量化交易等金融领域，并证明其有效性。如何将大模型作为自动编码器，以从文本数据中自动抽取结构化用户数据以帮助欺诈检测；或帮助现有模型处理多模态用户数据，以提高预测准确性也将成为该领域未来需要探究的问题。

参考文献（References）：

[1] Pricewaterhouse Coopers. Global Economic Crime Survey 2022[EB/OL]. (2022-06-12). https://www.pwc.tw/zh/publications/global-insights/economic-crime-survey.html

[2] Sahin Y, Duman E. Detecting credit card fraud by decision trees and support vector machines[C]. Proceedings of the International MultiConference of Engineers and Computer Scientists. 2011, 1: 1-6.

[3] Lu Q, Ju C. Research on credit card fraud detection model based on class weighted support vector machine[J]. Journal of Convergence Information Technology, 2011, 6(1).

[4] Hejazi M, Singh Y P. One-class support vector machines approach to anomaly detection[J]. Applied Artificial Intelligence, 2013, 27(5): 351-366.

[5] Schölkopf B, Williamson R C, Smola A, et al. Support vector method for novelty detection[J]. Advances in neural information processing systems, 1999, 12.

[6] Sundarkumar G G, Ravi V. A novel hybrid undersampling method for mining unbalanced datasets in banking and insurance[J]. Engineering Applications of Artificial Intelligence, 2015, 37: 368-377.

[7] Phua C, Alahakoon D, Lee V. Minority report in fraud detection: classification of skewed data[J]. Acm

sigkdd explorations newsletter, 2004, 6(1): 50-59.

[8] Rtayli N, Enneya N. Selection features and support vector machine for credit card risk identification[J]. Procedia Manufacturing, 2020, 46: 941-948.

[9] Liu F T, Ting K M, Zhou Z H. Isolation forest[C]. 2008 eighth ieee international conference on data mining. IEEE, 2008: 413-422.

[10] Ounacer S, El Bour H A, Oubrahim Y, et al. Using Isolation Forest in anomaly detection: the case of credit card transactions[J]. Periodicals of Engineering and Natural Sciences, 2018, 6(2): 394-400.

[11] Stripling E, Baesens B, Chizi B, et al. Isolation-based conditional anomaly detection on mixed-attribute data to uncover workers' compensation fraud[J]. Decision Support Systems, 2018, 111: 13-26.

[12] Viaene S, Derrig R A, Dedene G. A case study of applying boosting Naive Bayes to claim fraud diagnosis[J]. IEEE Transactions on Knowledge and data Engineering, 2004, 16(5): 612-620.

[13] Freund Y, Schapire R E. Experiments with a new boosting algorithm[C]. icml. 1996, 96: 148-156.

[14] Srivastava A, Kundu A, Sural S, et al. Credit card fraud detection using hidden Markov model[J]. IEEE Transactions on dependable and secure computing, 2008, 5(1): 37-48.

[15] Dhok S S, Bamnote G R. Credit card fraud detection using hidden Markov model[J]. International Journal of Soft Computing and Engineering (IJSCE), 2012, 2(1): 231-237.

[16] Robinson W N, Aria A. Sequential fraud detection for prepaid cards using hidden Markov model divergence[J]. Expert Systems with Applications, 2018, 91: 235-251.

[17] Lucas Y, Jurgovsky J. Credit card fraud detection using machine learning: A survey[J]. arXiv preprint arXiv:2010.06479, 2020.

[18] Maes S, Tuyls K, Vanschoenwinkel B, et al. Credit card fraud detection using Bayesian and neural networks[C]. Proceedings of the 1st international naiso congress on neuro fuzzy technologies. 2002, 261: 270.

[19] Ghosh S, Reilly D L. Credit card fraud detection with a neural-network[C]. System Sciences, 1994. Proceedings of the Twenty-Seventh Hawaii International Conference on. IEEE, 1994, 3: 621-630.

[20] Aleskerov E, Freisleben B, Rao B. Cardwatch: A neural network based database mining system for credit card fraud detection[C]. Proceedings of the IEEE/IAFE 1997 computational intelligence for financial engineering (CIFEr). IEEE, 1997: 220-226.

[21] Behera T K, Panigrahi S. Credit card fraud detection: a hybrid approach using fuzzy clustering & neural network[C]. 2015 second international conference on advances in computing and communication engineering. IEEE, 2015: 494-499.

[22] Gómez J A, Arévalo J, Paredes R, et al. End-to-end neural network architecture for fraud scoring in card payments[J]. Pattern Recognition Letters, 2018, 105: 175-181.

[23] Wiese B, Omlin C. Credit card transactions, fraud detection, and machine learning: Modelling time with LSTM recurrent neural networks[M]. Innovations in neural information paradigms and applications. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009: 231-268.

[24] Jurgovsky J, Granitzer M, Ziegler K, et al. Sequence classification for credit-card fraud detection[J]. Expert systems with applications, 2018, 100: 234-245.

[25] Bahnsen A C, Aouada D, Stojanovic A, et al. Feature engineering strategies for credit card fraud detection[J]. Expert Systems with Applications, 2016, 51: 134-142.

[26] Fu K, Cheng D, Tu Y, et al. Credit card fraud detection using convolutional neural networks[C]. Neural Information Processing: 23rd International Conference, ICONIP 2016, Kyoto, Japan, October 16–

21, 2016, Proceedings, Part III 23. Springer International Publishing, 2016: 483-490.

[27] Heryadi Y, Warnars H L H S. Learning temporal representation of transaction amount for fraudulent transaction recognition using CNN, Stacked LSTM, and CNN-LSTM[C]. 2017 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom). IEEE, 2017: 84-89.

[28] Chen J, Shen Y, Ali R. Credit card fraud detection using sparse autoencoder and generative adversarial network[C]. 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2018: 1054-1059.

[29] Charitou C, Garcez A A, Dragicevic S. Semi-supervised GANs for fraud detection[C]. 2020 International Joint Conference on Neural Networks (IJCNN). IEEE, 2020: 1-8.

[30] Ba H. Improving detection of credit card fraudulent transactions using generative adversarial networks[J]. arXiv preprint arXiv:1907.03355, 2019.

[31] Zheng P, Yuan S, Wu X, et al. One-class adversarial nets for fraud detection[C]//Proceedings of the AAAI Conference on Artificial Intelligence. 2019, 33(01): 1286-1293.

[32] Šubelj L, Furlan Š, Bajec M. An expert system for detecting automobile insurance fraud using social network analysis[J]. Expert Systems with Applications, 2011, 38(1): 1039-1052.

[33] Dreżewski R, Sepielak J, Filipkowski W. The application of social network analysis algorithms in a system supporting money laundering detection[J]. Information Sciences, 2015, 295: 18-32.

[34] Colladon A F, Remondi E. Using social network analysis to prevent money laundering[J]. Expert Systems with Applications, 2017, 67: 49-58.

[35] Kaggle. Credit Card Fraud Detection[EB/OL]. (2021-05-03). https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud

[36] Kaggle. Synthetic Financial Datasets For Fraud Detection[EB/OL]. https://www.kaggle.com/datasets/ealaxi/paysim1

[37] Altman E, Blanuša J, Von Niederhäusern L, et al. Realistic synthetic financial transactions for anti-money laundering models[J]. Advances in Neural Information Processing Systems, 2024, 36.