BOCA
BOLETIM DE CONJUNTURA

USO DE APRENDIZADO DE MÁQUINA NA DETECÇÃO DE FRAUDES FINANCEIRAS

THE USE OF MACHINE LEARNING IN DETECTING FINANCIAL FRAUD

EL USO DEL APRENDIZAJE AUTOMÁTICO EN LA DETECCIÓN DEL FRAUDE FINANCIERO

10.56238/bocav25n78-020

Yann Benedito Araújo Penha
Bacharel em Sistemas de Informação
Instituição: Faculdade Santa Terezinha (CEST)
Endereço: Maranhão, Brasil

Nathaniel Luiz Cordeiro Moraes
Bacharel em Sistemas de Informação
Instituição: Faculdade Santa Terezinha (CEST)
Endereço: Maranhão, Brasil

Dadilton Bastos Melo
Esp. Ciência de Dados e Big Data Analytics
Instituição: Centro Universitário Santa Teresinha (CEST)

RESUMO
Introdução: A crescente digitalização dos serviços financeiros tem ampliado a ocorrência de fraudes, tornando sua detecção um desafio relevante para instituições financeiras. Nesse contexto, o uso de técnicas de aprendizado de máquina destaca-se como uma abordagem eficiente, capaz de analisar grandes volumes de dados e identificar padrões suspeitos com maior precisão. Objetivo: Analisar o uso de técnicas de aprendizado de máquina na detecção de fraudes financeiras, destacando os principais algoritmos, aplicações e desafios envolvidos. Materiais e Método: Trata-se de uma pesquisa qualitativa, desenvolvida por meio de revisão de literatura. O levantamento identificou 186 estudos, dos quais 12 compuseram a amostra final após aplicação dos critérios de inclusão e exclusão. A análise foi realizada por meio de leitura exploratória, seletiva e analítica, organizando os dados em categorias temáticas. Resultados: Os estudos evidenciaram que algoritmos como Random Forest e Gradient Boosting apresentam alto desempenho na detecção de fraudes. Observou-se também a eficácia de modelos híbridos e técnicas de balanceamento de dados. No entanto, desafios como dados desbalanceados, falsos positivos e necessidade de atualização contínua dos modelos ainda persistem. Contribuição Científica: O estudo contribui ao sistematizar e analisar criticamente as principais abordagens da literatura, identificando tendências, desafios e lacunas no uso do aprendizado de máquina na detecção de fraudes financeiras. Conclusão: Conclui-se que o aprendizado de máquina é uma ferramenta essencial no combate às fraudes financeiras, embora ainda apresente desafios que exigem aprimoramento contínuo, especialmente diante da evolução constante das estratégias fraudulentas.

Palavras-chave: Aprendizado de Máquina. Fraudes Financeiras. Detecção de Fraudes.

ABSTRACT
Introduction: The growing digitization of financial services has led to an increase in fraud, making its detection a significant challenge for financial institutions. In this context, the use of machine learning techniques stands out as an efficient approach, capable of analyzing large volumes of data and identifying suspicious patterns with greater accuracy. Objective: To analyze the use of machine learning techniques in the detection of financial fraud, highlighting the main algorithms, applications, and challenges involved. Materials and Methods: This is a qualitative study conducted through a literature review. The survey identified 186 studies, of which 12 comprised the final sample after applying the inclusion and exclusion criteria. The analysis was performed through exploratory, selective, and analytical reading, organizing the data into thematic categories. Results: The studies showed that algorithms such as Random Forest and Gradient Boosting perform well in fraud detection. The effectiveness of hybrid models and data balancing techniques was also observed. However, challenges such as imbalanced data, false positives, and the need for continuous model updates still persist. Scientific Contribution: This study contributes by systematizing and critically analyzing the main approaches in the literature, identifying trends, challenges, and gaps in the use of machine learning for financial fraud detection. Conclusion: It is concluded that machine learning is an essential tool in combating financial fraud, although it still presents challenges that require continuous improvement, especially in light of the constant evolution of fraudulent strategies.

Keywords: Machine Learning. Financial Fraud. Fraud Detection.

RESUMEN
Introducción: La creciente digitalización de los servicios financieros ha incrementado la incidencia del fraude, lo que convierte su detección en un desafío significativo para las instituciones financieras. En este contexto, el uso de técnicas de aprendizaje automático se destaca como un enfoque eficiente, capaz de analizar grandes volúmenes de datos e identificar patrones sospechosos con mayor precisión. Objetivo: Analizar el uso de técnicas de aprendizaje automático en la detección del fraude financiero, destacando los principales algoritmos, aplicaciones y desafíos involucrados. Materiales y Métodos: Esta es una investigación cualitativa, desarrollada a través de una revisión de la literatura. La encuesta identificó 186 estudios, de los cuales 12 conformaron la muestra final tras aplicar los criterios de inclusión y exclusión. El análisis se realizó mediante lectura exploratoria, selectiva y analítica, organizando los datos en categorías temáticas. Resultados: Los estudios mostraron que algoritmos como Random Forest y Gradient Boosting tienen un alto rendimiento en la detección de fraude. También se observó la efectividad de los modelos híbridos y las técnicas de balanceo de datos. Sin embargo, persisten desafíos como el desequilibrio de datos, los falsos positivos y la necesidad de actualizaciones continuas del modelo. Contribución científica: Este estudio contribuye al sistematizar y analizar críticamente los principales enfoques de la literatura, identificando tendencias, desafíos y deficiencias en el uso del aprendizaje automático para la detección del fraude financiero. Conclusión: Se concluye que el aprendizaje automático es una herramienta esencial para combatir el fraude financiero, si bien aún presenta desafíos que requieren mejora continua, especialmente dada la constante evolución de las estrategias fraudulentas.

Palabras clave: Aprendizaje Automático. Fraude Financiero. Detección de Fraude.

1 INTRODUÇÃO

O avanço das tecnologias digitais e a crescente utilização de serviços financeiros eletrônicos têm proporcionado maior conveniência e agilidade nas transações. Contudo, esse cenário também ampliou significativamente as oportunidades para a ocorrência de fraudes, tornando a detecção de fraudes financeiras um dos principais desafios enfrentados por instituições bancárias, empresas de tecnologia financeira (fintechs) e órgãos reguladores (Paulino; Silva; Florian, 2025).

Segundo Stojanović et al. (2021), o aumento do volume de dados gerados por transações digitais exige métodos cada vez mais sofisticados para identificar comportamentos suspeitos em tempo real, uma vez que técnicas tradicionais já não conseguem acompanhar a complexidade e a velocidade das fraudes modernas. A crescente digitalização dos meios de pagamento, como cartões de crédito, transferências eletrônicas e sistemas instantâneos, como o Pix, tem contribuído para a ampliação da superfície de ataque explorada por fraudadores (Santos, 2025).

Nesse contexto, o uso de técnicas de aprendizado de máquina (machine learning) tem se destacado como uma abordagem promissora, por possibilitar a análise de grandes volumes de dados e a identificação de padrões complexos associados a atividades fraudulentas. O aprendizado de máquina compreende um conjunto de métodos computacionais capazes de aprender a partir de dados históricos, permitindo a realização de previsões e a identificação de comportamentos anômalos sem a necessidade de programação explícita para cada situação (Souza; Novais; Calumby, 2025).

Algoritmos supervisionados, como regressão logística, árvores de decisão e Random Forest, apresentam bons resultados na detecção de fraudes, especialmente quando combinados com técnicas de tratamento de dados desbalanceados (Araújo, 2022; Oliveira, 2025). Além disso, abordagens mais recentes, como modelos híbridos e técnicas baseadas em ensemble, têm sido exploradas com o objetivo de melhorar o desempenho dos sistemas antifraude (Silva; Roma, 2025).

Apesar dos avanços observados, a literatura evidencia desafios importantes, tais como o desbalanceamento dos dados, a ocorrência de falsos positivos, a necessidade de atualização contínua dos modelos e questões relacionadas à interpretabilidade dos algoritmos (Místico, 2023; Souza; Bordin Jr., 2023). Esses fatores demonstram que, embora o aprendizado de máquina represente uma ferramenta relevante na detecção de fraudes financeiras, ainda existem limitações que impactam sua aplicação em cenários reais.

Diante desse contexto, torna-se necessário compreender, de forma sistematizada, como as diferentes técnicas de aprendizado de máquina têm sido aplicadas na detecção de fraudes financeiras, bem como identificar suas principais vantagens, limitações e desafios. Assim, este estudo busca responder à seguinte questão de pesquisa: como as principais técnicas de aprendizado de máquina utilizadas na detecção de fraudes financeiras se diferenciam quanto às suas vantagens, limitações e desafios, segundo a literatura recente?

Para responder a essa questão, este trabalho adota como abordagem metodológica uma revisão integrativa da literatura, que permite reunir, analisar e sintetizar estudos com diferentes delineamentos metodológicos, proporcionando uma visão ampla e crítica sobre o estado da arte do tema. Esse tipo de revisão possibilita não apenas a identificação de tendências e lacunas, mas também a construção de um panorama teórico que contribui para o avanço do conhecimento científico na área.

Dessa forma, o objetivo geral deste estudo é analisar o uso de técnicas de aprendizado de máquina na detecção de fraudes financeiras, destacando os principais algoritmos empregados, suas aplicações, vantagens, limitações e desafios, com base na literatura científica recente.

A realização deste estudo justifica-se pela crescente incidência de fraudes financeiras e pela necessidade de desenvolvimento de soluções tecnológicas mais eficazes para seu combate. Considerando os impactos econômicos e sociais dessas práticas, bem como a constante evolução das estratégias utilizadas por fraudadores, torna-se essencial investigar criticamente o papel do aprendizado de máquina nesse contexto, contribuindo tanto para o avanço acadêmico quanto para o aprimoramento de práticas aplicadas no setor financeiro.

2 MATERIAIS E MÉTODO

O presente estudo caracteriza-se como uma pesquisa de natureza qualitativa, desenvolvida por meio de uma revisão integrativa da literatura. Esse tipo de abordagem tem como finalidade reunir, analisar e sintetizar resultados de pesquisas sobre um determinado tema, permitindo a construção de um panorama teórico abrangente e sistematizado, bem como a identificação de lacunas no conhecimento científico. A revisão integrativa distingue-se por possibilitar a inclusão de estudos com diferentes delineamentos metodológicos, proporcionando uma análise mais ampla e crítica do fenômeno investigado.

De acordo com Gil (2019), a pesquisa bibliográfica é elaborada a partir de materiais já publicados, sendo especialmente útil para investigar fenômenos amplamente discutidos na literatura científica. Complementarmente, a revisão integrativa, conforme destacado por Whittemore e Knafl (2005), segue um processo estruturado que envolve etapas como definição do problema, busca na literatura, seleção dos estudos, avaliação dos dados e síntese do conhecimento.

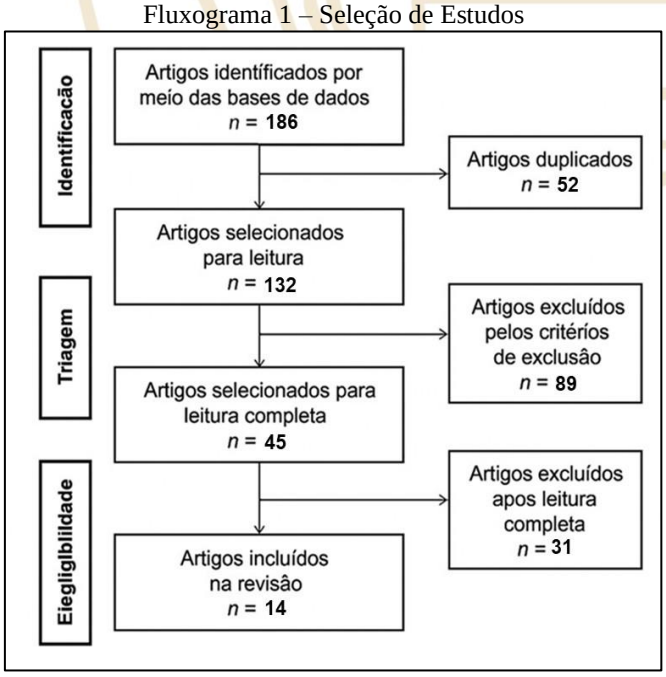
Nesse contexto, a presente revisão possui caráter descritivo e exploratório, uma vez que busca compreender como as técnicas de aprendizado de máquina têm sido aplicadas na detecção de fraudes financeiras, identificando suas principais abordagens, vantagens, limitações e desafios. Conforme Lakatos e Marconi (2021), pesquisas exploratórias têm como objetivo proporcionar maior familiaridade com o problema, tornando-o mais explícito e possibilitando a construção de interpretações mais aprofundadas.

O processo de coleta de dados foi realizado por meio de buscas em bases de dados acadêmicas e científicas, incluindo Google Acadêmico, SciELO, periódicos eletrônicos e repositórios institucionais. Para a recuperação dos estudos, foram utilizados descritores em português e inglês, tais como “aprendizado de máquina”, “machine learning”, “detecção de fraudes” e “fraudes financeiras”, combinados com operadores booleanos (AND, OR), de forma a ampliar a abrangência e a relevância dos resultados obtidos. Segundo Silva (2018), a definição adequada das estratégias de busca é fundamental para garantir a qualidade e a consistência do levantamento bibliográfico.

Como critérios de inclusão, foram considerados estudos publicados preferencialmente nos últimos anos, disponíveis na íntegra e que apresentassem relação direta com o tema proposto, abordando a aplicação de técnicas de aprendizado de máquina na detecção de fraudes financeiras. Foram excluídos trabalhos duplicados, estudos incompletos ou aqueles que não apresentavam rigor metodológico adequado ou aderência ao objetivo da pesquisa. Conforme Botelho, Cunha e Macedo (2011), a definição de critérios claros e objetivos de seleção contribui para a confiabilidade e a validade dos resultados em revisões integrativas.

A seleção dos estudos ocorreu em etapas. Inicialmente, foram identificados 186 trabalhos. Após a remoção de 52 registros duplicados, permaneceram 134 estudos para triagem. Desses, 89 foram excluídos por não atenderem aos critérios estabelecidos, resultando em 45 estudos selecionados para leitura na íntegra. Após a avaliação detalhada, 31 trabalhos foram excluídos por inadequações metodológicas ou baixa aderência ao tema, totalizando 14 estudos incluídos na amostra final. Esse processo de seleção está representado no Fluxograma 1.

Fluxograma 1 – Seleção de Estudos



Fonte: Autores (2026).

A análise dos dados foi realizada de forma qualitativa, com abordagem descritiva e interpretativa, buscando identificar padrões, convergências e lacunas na literatura. Os estudos selecionados foram organizados em categorias analíticas, como tipos de algoritmos utilizados, desempenho dos modelos, estratégias de tratamento de dados desbalanceados e desafios práticos na detecção de fraudes financeiras. Essa etapa permitiu a construção de uma síntese crítica do conhecimento, característica fundamental das revisões integrativas.

3 RESULTADOS E DISCUSSÃO

A sistematização dos achados identificados nos 12 estudos selecionados é apresentada no Quadro 1, o qual sintetiza os principais aspectos metodológicos e resultados relacionados ao uso de aprendizado de máquina na detecção de fraudes financeiras, destacando os algoritmos empregados, suas aplicações e os desafios encontrados nesse contexto.

Quadro 1 – Resultados dos Estudos Selecionados

Autor/Ano	Título	Tipo de estudo	Objetivo	Principais Resultados
Araujo (2022)	Estudo comparativo entre algoritmos de aprendizagem de máquina aplicados à detecção de fraudes de cartão de crédito	Estudo experimental	Comparar o desempenho de algoritmos de machine learning na detecção de fraudes	Modelos como *Random Forest* apresentaram melhor desempenho, especialmente com técnicas de balanceamento de dados.
Araújo; Vaz (2022)	Utilização de aprendizado de máquina para detecção de fraudes em cartão de crédito	Estudo experimental	Avaliar algoritmos de ML na identificação de fraudes em cartões	Algoritmos supervisionados mostraram alta eficiência, destacando-se na classificação de transações.
Místico (2023)	Aprendizado de máquina aplicado a fraudes em cartões	Estudo experimental	Aplicar modelos de ML para detectar fraudes em cartões	Resultados indicaram boa capacidade preditiva, com destaque para modelos ensemble.
Souza; Bordin Jr. (2023)	Detecção de fraude de cartão de crédito por meio de algoritmos de aprendizado de máquina	Estudo experimental	Investigar algoritmos de ML aplicados à fraude em cartões	Resultados apontaram boa precisão, com necessidade de ajuste para reduzir falsos positivos.
Ono; Silva; Molina (2024)	Comparação de três algoritmos de Machine Learning: adaboost, árvore de decisão e floresta aleatória	Estudo comparativo	Comparar diferentes algoritmos de ML	*Random Forest* apresentou melhor desempenho geral, equilibrando precisão e robustez.
Silva; Roma (2025)	Fraudes em Cartões de Crédito: Uma Abordagem Híbrida e Unificada com Machine Learning e GMM	Estudo aplicado	Desenvolver modelo híbrido para detecção de fraudes	A abordagem híbrida aumentou a capacidade de detecção em cenários complexos.
Souza; Novais; Calumby (2025)	Water Fraud Analytics – um modelo de Machine Learning para detecção de fraudes em consumo de água	Estudo aplicado	Desenvolver modelo de ML para detectar fraudes em consumo	Modelo apresentou eficácia na identificação de padrões anômalos em consumo.

Lee et al. (2025)	Evaluating Machine Learning Algorithms for Financial Fraud Detection: Insights from Indonesia	Estudo experimental comparativo	Avaliar o desempenho de algoritmos de ML na detecção de fraudes financeiras	Algoritmos como *Random Forest* e *Gradient Boosting* apresentaram melhor desempenho, com alta precisão na detecção de fraudes.
Sousa (2021)	Estudo comparativo entre modelos para detecção de fraudes em cartões de crédito	Estudo experimental	Comparar diferentes modelos de ML na detecção de fraudes em cartões	Modelos supervisionados apresentaram melhores resultados, destacando a importância do tratamento de dados desbalanceados.
Varmedja et al. (2019)	*Credit Card Fraud Detection – Machine Learning methods.*	Estudo experimental comparativo	Comparar diferentes algoritmos de aprendizado de máquina na detecção de fraudes em cartões de crédito.	Modelos ensemble, especialmente *Random Forest*, apresentaram melhor desempenho em bases de dados desbalanceadas, alcançando maior precisão e capacidade de identificação de transações fraudulentas em comparação a modelos tradicionais.
Alarfaj et al. (2022)	*Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms.*	Estudo experimental comparativo	Avaliar o desempenho de algoritmos de machine learning e deep learning na detecção de fraudes financeiras.	Modelos de *deep learning* e *ensemble* apresentaram maior eficiência na detecção de fraudes, especialmente quando associados a técnicas de balanceamento de dados e otimização de hiperparâmetros.
Sadgali; Sael; Benabbou (2019)	*Performance of Machine Learning Techniques in the Detection of Financial Frauds*	Revisão comparativa e experimental	Analisar o desempenho de diferentes técnicas de machine learning aplicadas à detecção de fraudes financeiras.	Técnicas de aprendizado supervisionado apresentam melhores resultados que métodos tradicionais, destacando a importância do pré-processamento dos dados e da seleção adequada de atributos.
Carcillo et al. (2019)	*Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy*	Estudo experimental aplicado	Propor uma estratégia mais realista para detecção de fraudes em cartões de crédito considerando cenários reais de operação.	Foi identificado limitações em avaliações tradicionais e demonstraram que fatores como atraso na rotulação dos dados e *concept drift* impactam diretamente o desempenho dos modelos em ambientes reais.
Mienye; Sun (2023)	*A Deep Learning Ensemble With Data Resampling for Credit Card Fraud Detection*	Estudo experimental	Desenvolver um modelo baseado em deep learning e reamostragem de dados para melhorar a detecção de fraudes.	O modelo proposto apresentou melhora significativa na detecção de fraudes em bases altamente desbalanceadas, reduzindo falsos negativos e aumentando a

				capacidade preditiva dos sistemas antifraude.

Fonte: Autores (2026).

A análise dos estudos selecionados evidencia que o uso de técnicas de aprendizado de máquina tem se consolidado como uma das principais estratégias para a detecção de fraudes financeiras, especialmente em cenários caracterizados por grande volume de dados e necessidade de respostas em tempo real. Nesse contexto, observa-se que diferentes abordagens têm sido propostas e avaliadas, variando desde modelos supervisionados tradicionais até métodos híbridos e mais sofisticados.

Araujo (2022) demonstra, por meio de um estudo comparativo, que algoritmos como Random Forest apresentam desempenho superior na detecção de fraudes em cartões de crédito, principalmente quando associados a técnicas de balanceamento de dados. O autor destaca que o problema do desbalanceamento, comum em bases de dados financeiras, impacta diretamente a performance dos modelos, exigindo estratégias específicas para garantir maior precisão na identificação de fraudes.

Contudo, embora o Random Forest tenha apresentado melhores resultados, o estudo não aprofunda situações em que esse algoritmo pode falhar, como em cenários com elevada dimensionalidade ou necessidade de interpretabilidade, aspectos relevantes em aplicações financeiras reguladas.

De forma semelhante, Araújo e Vaz (2022) evidenciam que algoritmos supervisionados, como regressão logística e árvores de decisão, são eficazes na classificação de transações fraudulentas. No entanto, os autores ressaltam que a qualidade dos dados e o pré-processamento adequado são determinantes para o sucesso dos modelos, especialmente em cenários reais, onde os dados podem apresentar ruídos e inconsistências.

Apesar disso, o estudo apresenta limitação metodológica ao não detalhar suficientemente os critérios de balanceamento utilizados, dificultando comparações mais robustas com pesquisas que utilizam técnicas como SMOTE ou *undersampling*.

Místico (2023) reforça essa perspectiva ao aplicar diferentes técnicas de aprendizado de máquina na detecção de fraudes em cartões. O estudo aponta que modelos ensemble, como Random Forest, tendem a apresentar melhor desempenho devido à sua capacidade de reduzir *overfitting* e lidar com variabilidade nos dados.

O autor destaca a importância da engenharia de atributos na melhoria da capacidade preditiva dos modelos. Entretanto, embora os resultados sejam positivos, a pesquisa não discute aspectos relacionados à interpretabilidade do modelo, um fator relevante em sistemas financeiros que demandam justificativas para bloqueios ou recusas de transações. Essa discussão amplia o debate ao demonstrar que métricas isoladas, como acurácia, podem mascarar falhas importantes em conjuntos de dados desbalanceados, reforçando críticas presentes em outros estudos analisados.

Souza e Bordin Jr. (2023) corroboram essa análise ao afirmar que, embora os modelos apresentem boa precisão, ainda há necessidade de ajustes finos para reduzir erros de classificação. Os autores enfatizam que a detecção de fraudes não deve se basear apenas na acurácia, mas também em métricas como recall e precisão, que oferecem uma visão mais completa do desempenho dos modelos.

No estudo de Ono, Silva e Molina (2024), a comparação entre algoritmos como *AdaBoost*, árvore de decisão e *Random Forest* evidencia que este último apresenta melhor desempenho geral. Os autores destacam que o equilíbrio entre robustez e capacidade de generalização torna o Random Forest uma das opções mais eficientes para aplicações em ambientes financeiros.

Ainda assim, o estudo sugere implicitamente que algoritmos como *Gradient Boosting* podem superar o *Random Forest* em cenários mais complexos e com maior refinamento de hiperparâmetros, embora essa comparação não tenha sido explorada de forma aprofundada.

Oliveira (2025) amplia essa discussão ao analisar diferentes métodos de machine learning aplicados à detecção de fraudes. O autor aponta que não existe um algoritmo universalmente superior, sendo necessário considerar as características específicas do conjunto de dados e do problema em questão. Essa constatação reforça a importância de abordagens experimentais e comparativas na escolha dos modelos. O estudo evidencia um conflito recorrente na literatura: enquanto alguns trabalhos priorizam desempenho preditivo, outros defendem modelos mais interpretáveis, ainda que menos precisos.

No contexto de novas modalidades de fraude, Santos (2025) analisa a aplicação de algoritmos de aprendizado de máquina em transações Pix, destacando a eficiência dos modelos na identificação de padrões suspeitos em sistemas de pagamento instantâneo.

O estudo evidencia que a rapidez dessas transações exige modelos capazes de operar em tempo real, aumentando a complexidade dos sistemas de detecção, entretanto, a pesquisa não detalha os custos computacionais envolvidos, fator importante para implementação prática em larga escala.

Silva e Roma (2025) propõem uma abordagem híbrida que combina técnicas de aprendizado de máquina com modelos estatísticos, como o *Gaussian Mixture Model*. Os resultados indicam melhora significativa na capacidade de detecção, especialmente em cenários complexos, demonstrando que a integração de diferentes técnicas pode potencializar os resultados. Apesar disso, a metodologia utilizada apresenta limitações relacionadas à ausência de validação em bases públicas amplamente utilizadas pela comunidade científica, o que restringe comparações externas.

Souza, Novais e Calumby (2025) expandem a aplicação do aprendizado de máquina para além do setor financeiro tradicional, ao desenvolverem um modelo para detecção de fraudes no consumo de água. Os autores demonstram que técnicas de machine learning são eficazes na identificação de padrões anômalos, reforçando sua versatilidade e aplicabilidade em diferentes contextos, ainda assim,

o cenário analisado difere significativamente das fraudes financeiras em tempo real, o que limita a generalização direta dos resultados.

Pacheco Junior (2019) contribui com uma análise mais abrangente sobre modelos de detecção de fraudes, destacando a importância da escolha adequada das técnicas e da validação dos modelos. O autor ressalta que a combinação entre conhecimento de domínio e técnicas computacionais é essencial para o desenvolvimento de sistemas eficazes. Essa perspectiva diferencia-se de estudos mais recentes que priorizam exclusivamente métricas quantitativas, reforçando a necessidade de abordagens multidisciplinares.

Stojanović et al. (2021) abordam a aplicação de machine learning em fintechs, destacando a necessidade de modelos adaptativos capazes de acompanhar a evolução das estratégias de fraude. Os autores enfatizam que a detecção de fraudes é um problema dinâmico, exigindo atualização constante dos modelos. O estudo não detalha como ocorre esse processo de atualização contínua, tampouco os riscos associados ao *concept drift*, problema recorrente em ambientes financeiros dinâmicos.

Lee et al. (2025) reforçam essa perspectiva ao avaliar diferentes algoritmos em um contexto internacional, evidenciando que modelos como *Gradient Boosting* e Random Forest apresentam alto desempenho na detecção de fraudes financeiras. O estudo também destaca a importância da validação cruzada para garantir a confiabilidade dos resultados. Diferentemente de outros trabalhos, os autores demonstram que o *Gradient Boosting* pode superar o *Random Forest* em bases altamente complexas e menos ruidosas, especialmente quando há maior disponibilidade computacional para ajuste fino dos parâmetros.

Sousa (2021) analisa comparativamente diferentes modelos aplicados à detecção de fraudes em cartões de crédito, evidenciando que algoritmos supervisionados apresentam melhores resultados. O autor destaca, novamente, o impacto do desbalanceamento dos dados e a necessidade de técnicas específicas para seu tratamento. Apesar disso, o estudo limita-se a *datasets* tradicionais e não explora cenários de detecção em tempo real, o que reduz sua aderência às demandas atuais do mercado financeiro digital.

Socca Junior (2024) enfatiza o papel da mineração de dados na identificação de padrões suspeitos, destacando que a combinação entre técnicas de data mining e machine learning potencializa a capacidade de detecção. O autor aponta que a análise de grandes volumes de dados permite identificar comportamentos que não seriam detectados por métodos tradicionais. Entretanto, o estudo carece de maior detalhamento sobre a origem e disponibilidade dos dados utilizados, dificultando a replicabilidade dos experimentos.

Tosta e Dias (2025) discutem a aplicação de inteligência artificial na detecção de fraudes bancárias, destacando que o uso dessas tecnologias permite maior automação e eficiência nos processos de monitoramento. Os autores ressaltam que a integração de sistemas inteligentes é

fundamental para enfrentar a crescente sofisticação das fraudes. Ainda assim, o estudo pouco discute questões éticas e regulatórias relacionadas ao uso intensivo de dados sensíveis em sistemas automatizados.

Por outro lado, Brum e Reis (2025) destacam a importância de estratégias integradas que envolvam não apenas a detecção, mas também a prevenção e dissuasão de fraudes. As autoras apontam que o uso de tecnologias deve estar aliado a políticas institucionais e práticas organizacionais eficazes. Essa visão amplia o debate ao demonstrar que soluções puramente tecnológicas podem ser insuficientes diante da complexidade das fraudes contemporâneas.

A Experian (2024) reforça a relevância do uso de inteligência artificial e aprendizado de máquina em sistemas antifraude, destacando que modelos modernos são capazes de aprender continuamente com novos dados, aumentando sua eficácia ao longo do tempo. Esse aspecto é fundamental em um cenário onde os padrões de fraude estão em constante evolução.

Varmedja et al. (2019) analisam a aplicação de diferentes algoritmos de aprendizado de máquina na detecção de fraudes em cartões de crédito, destacando que modelos ensemble, especialmente o Random Forest, apresentaram desempenho superior em comparação a métodos tradicionais. Os autores apontam que a capacidade desses algoritmos em lidar com dados desbalanceados contribui significativamente para a melhoria na identificação de transações fraudulentas. Entretanto, o estudo também evidencia que o desempenho dos modelos depende diretamente da qualidade do pré-processamento dos dados e da escolha adequada das métricas de avaliação.

Alarfaj et al. (2022) investigam o uso de algoritmos de machine learning e deep learning na detecção de fraudes financeiras, demonstrando que modelos mais complexos, como redes neurais profundas, podem alcançar resultados superiores em cenários com grandes volumes de dados.

Os autores relatam que as técnicas de balanceamento e ajuste de hiperparâmetros são fundamentais para aumentar a precisão dos sistemas antifraude. Além disso, o estudo ressalta que modelos de *deep learning* apresentam maior capacidade de capturar padrões complexos, embora demandem maior custo computacional e menor interpretabilidade.

Sadgali, Sael e Benabbou (2019) realizam uma análise comparativa de diferentes técnicas de aprendizado de máquina aplicadas à detecção de fraudes financeiras. Os autores observam que métodos supervisionados tendem a apresentar melhores resultados na classificação de transações suspeitas, principalmente quando associados a estratégias adequadas de seleção de atributos.

O estudo também destaca que o desempenho dos modelos pode variar significativamente de acordo com as características da base de dados utilizada, evidenciando a inexistência de um algoritmo universalmente superior para todos os cenários.

Carcillo et al. (2019) propõem uma abordagem voltada para cenários reais de detecção de fraudes em cartões de crédito, destacando limitações frequentemente ignoradas em estudos experimentais tradicionais. Os autores demonstram que fatores como atraso na rotulação dos dados, atualização contínua dos modelos e *concept drift* impactam diretamente a eficiência dos sistemas antifraude em ambientes operacionais. O estudo reforça a necessidade de estratégias adaptativas capazes de acompanhar a evolução constante dos padrões de fraude.

Mienye e Sun (2023) apresentam um modelo baseado em *deep learning* combinado com técnicas de reamostragem de dados para melhorar a detecção de fraudes financeiras em bases altamente desbalanceadas. Os autores identificam que a integração entre modelos ensemble e técnicas de balanceamento reduz significativamente a ocorrência de falsos negativos, aumentando a capacidade preditiva dos sistemas. O estudo destaca que abordagens híbridas tendem a apresentar melhor desempenho em cenários complexos, especialmente quando comparadas a modelos supervisionados tradicionais.

Contudo, a literatura ainda apresenta lacunas importantes relacionadas à transparência dos modelos, à disponibilidade de bases públicas para validação e à comparação entre desempenho preditivo e interpretabilidade, indicando a necessidade de pesquisas futuras mais robustas e padronizadas.

4 CONCLUSÃO

O presente estudo permitiu compreender que o aprendizado de máquina tem desempenhado papel fundamental no aprimoramento dos sistemas de detecção de fraudes financeiras, respondendo à crescente complexidade das transações digitais e ao aumento do volume de dados processados pelas instituições financeiras.

A análise dos estudos revisados possibilitou responder ao problema central da pesquisa ao demonstrar que algoritmos de machine learning, especialmente modelos ensemble como *Random Forest* e *Gradient Boosting*, apresentam elevado potencial na identificação de padrões fraudulentos, sobretudo quando associados a técnicas adequadas de pré-processamento e balanceamento de dados.

Os resultados observados na literatura indicam que não existe um modelo universalmente superior para todos os cenários. Enquanto o Random Forest apresenta maior robustez e boa capacidade de generalização em bases heterogêneas e desbalanceadas, modelos como *Gradient Boosting* tendem a alcançar desempenho superior em contextos mais controlados e com maior refinamento de hiperparâmetros, verificou-se que fatores como qualidade dos dados, engenharia de atributos, validação adequada e capacidade de adaptação em tempo real influenciam diretamente a eficácia dos sistemas de detecção de fraudes.

A pesquisa também evidenciou limitações recorrentes nos estudos analisados. Muitos trabalhos utilizam bases de dados privados ou pouco detalhadas, dificultando a reprodutibilidade científica e a comparação entre modelos. Outro aspecto identificado refere-se à limitada discussão sobre interpretabilidade dos algoritmos, especialmente em modelos complexos classificados como "caixas-pretas", o que representa um desafio importante em ambientes financeiros regulados. Da mesma forma, observou-se que parte significativa das pesquisas prioriza métricas como acurácia, sem aprofundar suficientemente indicadores como recall, precisão e taxa de falsos positivos, fundamentais em sistemas antifraude reais.

Como contribuição científica, este estudo sistematizou criticamente diferentes abordagens aplicadas à detecção de fraudes financeiras, identificando convergências, conflitos metodológicos e lacunas presentes na literatura recente. Além disso, a pesquisa evidenciou a importância de análises comparativas mais aprofundadas entre algoritmos, considerando não apenas desempenho estatístico, mas também aspectos como interpretabilidade, custo computacional, capacidade de atualização contínua e aplicabilidade em cenários de detecção em tempo real.

No âmbito prático, os resultados reforçam que instituições financeiras e empresas do setor digital devem investir não apenas em modelos com alta capacidade preditiva, mas também em estratégias integradas que contemplem governança de dados, atualização contínua dos sistemas e redução de falsos positivos, visando minimizar impactos operacionais e melhorar a experiência do usuário. A adoção de abordagens híbridas e adaptativas mostra-se particularmente relevante diante da constante evolução das estratégias de fraude.

Portanto, sugere-se, como agenda para pesquisas futuras, o desenvolvimento de estudos voltados à interpretabilidade dos modelos de machine learning, à aplicação de técnicas de aprendizado contínuo para lidar com *concept drift* e à criação de benchmarks públicos que permitam maior padronização na comparação entre algoritmos. Também se recomenda investigar modelos capazes de operar eficientemente em ambientes de pagamento instantâneo, como o Pix, bem como explorar abordagens que conciliem alto desempenho preditivo, transparência algorítmica e viabilidade operacional em tempo real.

REFERÊNCIAS

ALARFAJ, Fawaz Khaled et al. Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms. **IEEE Access**, v. 10, p. 39700-39715, 2022. DOI: 10.1109/ACCESS.2022.3166891. Disponível em: https://ieeexplore.ieee.org/document/9755930. Acesso em: 02 mai. 2026.

ARAUJO, Danilo da Rocha Lira. **Estudo comparativo entre algoritmos de aprendizagem de máquina aplicados à detecção de fraudes de cartão de crédito** / Danilo Araujo. - Recife, 2022. 48 p. Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Informática, Sistemas de Informação - Bacharelado, 2022. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/47179/5/TCC%20Danilo%20da%20Rocha%20Lira%20Arau%CC%81jo%20-%202022.pdf. Acesso em: 24 abr. 2026.

ARAÚJO, Victor Santos Pimentel Rodrigues de; VAZ, Giovanna Castro. **Utilização de aprendizado de máquina para detecção de fraudes em cartão de crédito**. 2022. 52 f., il. Trabalho de conclusão de curso (Bacharelado em Engenharia de Redes de Comunicação) — Universidade de Brasília, Brasília, 2022. Disponível em: https://bdm.unb.br/bitstream/10483/34494/1/2022_VictorDeAraujo_GiovannaVaz_tcc.pdf. Acesso em: 18 abr. 2026.

BOTELHO, Louise de Lira Roedel; CUNHA, Cristiano Castro de Almeida; MACEDO, Marcelo. O método da revisão integrativa nos estudos organizacionais. **Gestão e Sociedade**, Belo Horizonte, v. 5, n. 11, p. 121–136, 2011.

BRUM, Laura Pianetti de. REIS, Luiza Santangelo. Tendências e aplicação de técnicas de dissuasão, detecção e prevenção no combate a fraudes financeiras. **Rev. Catarin. Ciênc. Contáb.,** Florianópolis/SC, v. 24, 1-21, e3538, 2025. ISSN 2237-7662, DOI: https://doi.org/10.16930/2237-7662202535381.

CARCILLO, Fabrizio et al. Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy. **IEEE Transactions on Neural Networks and Learning Systems**, v. 30, n. 12, p. 3784-3797, 2019. DOI: 10.1109/TNNLS.2018.2852630. Disponível em: IEEE Xplore. Acesso em: 01 mai. 2026.

EXPERIAN. **Fraud detection using machine learning and AI**. [S. l.], c. 2024. Disponível em: https://www.experian.co.uk/blogs/latest-thinking/guide/machine-learning-ai-fraud-detection/. Acesso em: 18 abr. 2026.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2019.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 9. ed. São Paulo: Atlas, 2021.

LEE, C.-W., et al. Evaluating Machine Learning Algorithms for Financial Fraud Detection: Insights from Indonesia. **Mathematics**, 13(4), 600. 2025https://doi.org/10.3390/math13040600. Disponível em: https://www.mdpi.com/2227-7390/13/4/600. Acesso em: 24 abr. 2026.

MIENYE, Ibomoiye Domor; SUN, Yanxia. A Deep Learning Ensemble With Data Resampling for Credit Card Fraud Detection. **IEEE Access**, v. 11, p. 30628-30638, 2023. DOI: 10.1109/ACCESS.2023.3262020. Disponível em: https://ieeexplore.ieee.org/document/10081315. Acesso em: 11 maio 2026.

MISTICO, Giovane Piola. **Aprendizado de máquina aplicado a fraudes em cartões**. 54p. 2023. Monografia (Graduação em Engenharia Mecatrônica) - Escola de Engenharia de São Carlos da Universidade de São Paulo, 2023. Disponível em: https://bdta.abcd.usp.br/directbitstream/f41a5ae8-4c56-4db9-b274-d794576d72cc/Mistico_Giovane_tcc.pdf. Acesso em: 24 abr. 2026.

OLIVEIRA, Vinicius Dias. Métodos de machine learning na detecção de fraude em cartão de crédito: um estudo comparado. **Revista Científica ACERTTE** - ISSN 2763-8928, [S. l.], v. 5, n. 9, p. e59265, 2025. DOI: 10.63026/acertte.v5i9.265. Disponível em: https://acertte.org/acertte/article/view/265. Acesso em: 24 abr. 2026.

ONO, Kaue T. L. SILVA, Kleberson dos S. MOLINA, Mariângela F. F. Comparação de três algoritmos de *Machine Learning*: adaboost, árvore de decisão e floresta aleatória para detecção de fraudes de cartão de crédito e seu impacto em clientes e instituições financeiras. **Revista Eletrônica Anima Terra**, Faculdade de Tecnologia de Mogi das Cruzes – FATEC-MC. Mogi das Cruzes-SP., n°19, ano IX, p.44-57, 2° semestre, 2024. ISSN 2526-1940.

PACHECO JUNIOR, João Carlos. **Modelos para detecção de fraudes utilizando técnicas de aprendizado de máquina**. 102 f. Dissertação (mestrado profissional MPFE) – Fundação Getúlio Vargas, Escola de Economia de São Paulo. 2019. Disponível em: https://repositorio.fgv.br/server/api/core/bitstreams/b4d9367d-712f-496e-8b15-ecb349671723/content. Acesso em: 25 abr. 2026.

PAULINO, Murilo Cabral. SILVA, André Luiz da. FLORIAN, Fabiana. A evolução dos modelos de inteligência artificial na detecção de fraudes financeiras. **Revista FT**. Ciências Exatas e da Terra, Volume 29, Edição 152, 2025. DOI: 10.69849/revistaft/ra10202511112333. Disponível em: https://revistaft.com.br/a-evolucao-dos-modelos-de-inteligencia-artificial-na-deteccao-de-fraudes-financeiras/. Acesso em: 24 abr. 2026.

SADGALI, Imane; SAEL, Nawal; BENABBOU, Faouzia. Performance of Machine Learning Techniques in the Detection of Financial Frauds. **Procedia Computer Science**, v. 148, p. 45-54, 2019. DOI: DOI:10.1016/j.procs.2019.01.007.

SANTOS, Andrei Camilo dos. **Aprendizagem de Máquina Aplicado na Detecção de Fraudes em Cartão de Crédito**. 42p. Universidade Federal de Ouro Preto – UFOP Departamento de Estatística – DEEST, Ouro Preto-MG. 2023. Disponível em: https://www.monografias.ufop.br/bitstream/35400000/6454/7/MONOGRAFIA_AprendizadoM%C3%A1quinaAplicado.pdf. Acesso em: 24 abr. 2026.

SANTOS, Daniele Chaves dos. **Detecção de fraudes em transações Pix com algoritmos de aprendizado de máquina**. 2025. 34 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) - Universidade Federal do Amazonas, Itacoatiara (AM), 2025. Disponível em: https://riu.ufam.edu.br/bitstream/prefix/8898/2/TCC_DanieleChaves.pdf. Acesso em: 24 abr. 2026.

SILVA, César Augusto Tibúrcio. **Metodologia da pesquisa científica**. Brasília: Universidade de Brasília, 2018.

SILVA, Martony Demes da; ROMA, Warleyson Costa. Fraudes em Cartões de Crédito: Uma Abordagem Híbrida e Unificada com Machine Learning e GMM. In: **Workshop de Sistemas de Informação** (WSIS), 16. 2025, Rio Paranaíba/MG. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2025. p. 89-96. DOI: https://doi.org/10.5753/wsis.2025.15731.

SOCCA JUNIOR, J. R. Técnicas de Mineração de Dados para Identificar Padrões Suspeitos em Transações Financeiras. **Revista Tópicos**, Rio de Janeiro, v. 2, n. 10, p. 1-31, 2024. ISSN: 2965-

6672. Disponível em: https://revistatopicos.com.br/artigos/te-cnicas-de-minerac-a-o-de-dados-para-identificar-padro-es-suspeitos-em-transac-o-es-financeiras. Acesso em: 23 abr. 2026.

SOUSA, Jocélio Silva de. **Estudo comparativo entre modelos para detecção de fraudes em cartões de crédito**. 2021. 41 f. Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Russas, Curso de Ciência da Computação, Russas, 2021. Disponível em: https://repositorio.ufc.br/bitstream/riufc/58056/1/2021_tcc_jssousa.pdf. Acesso em: 23 abr. 2026.

SOUZA, Daniel H.M. de. BORDIN JR., Claudio J. Detecção de fraude de cartão de crédito por meio de algoritmos de aprendizado de máquina. **Revista Brasileira de Computação Aplicada**, v. 15, n. 1, pp. 1–11, 2023. DOI: 10.5335/rbca.v15i1.13790. Homepage: seer.upf.br/index.php/rbca/index.

SOUZA, Márcio Nunes de. NOVAIS, Renato Lima. CALUMBY, Rodrigo Tripodi. *Water Fraud Analytics* – um modelo de *Machine Learning* para detecção de fraudes em consumo de água. **ABES - Associação Brasileira de Engenharia Sanitária e Ambiental**. 33º Congresso da ABES – FITABES, 2025. Disponível em: https://abes-dn.org.br/anaiseletronicos/33cbesa/242_tema_xi.pdf. Acesso em: 23 abr. 2026.

STOJANOVIĆ, B., et al. Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications. **Sensors**, 21(5), 1594. 2021. DOI: https://doi.org/10.3390/s21051594. Disponível em: https://www.mdpi.com/1424-8220/21/5/1594. Acesso em: 23 abr. 2026.

TOSTA, P. L. M. DIAS, J. C.; Detecção de fraudes em transações bancárias utilizando inteligência artificial. **Revista Processando o Saber**, [s. l.], v. 17, n. 01, 21-37, 6 jun. 2025. DOI 10.5281/zenodo.15477217. Disponível em: https://www.fatecpg.edu.br/revista/index.php/ps/article/view/341. Acesso em: 20 abr. 2026.

VARMEDJA, Dejan et al. Credit Card Fraud Detection – Machine Learning methods. In: **International Symposium Infoteh-Jahorina** (INFOTEH), 18., 2019. Proceedings [...]. IEEE, 2019. p. 1-5. DOI: 10.1109/INFOTEH.2019.8717766. Disponível em: https://ieeexplore.ieee.org/document/8717766. Acesso em: 01 mai. 2026.

WHITTEMORE, Robin; KNAFL, Kathleen. The integrative review: updated methodology. **Journal of Advanced Nursing**, v. 52, n. 5, p. 546–553, 2005.