# MACHINE LEARNING E FRAUDE DE CARTÃO DE CRÉDITO: UMA REVISÃO BIBLIOGRÁFICA SISTEMÁTICA

Machine Learning and Credit Card Fraud: a systematic review

**SILVA, GABRIEL FERREIRA DOS SANTOS**
Escola Superior de Agricultura “Luiz de Queiroz” – Universidade de São Paulo

**LAMARCA, DANIEL SÁ FREIRE**
Escola Superior de Agricultura “Luiz de Queiroz” – Universidade de São Paulo

**SARRIÉS, GABRIEL ADRIAN**
Escola Superior de Agricultura “Luiz de Queiroz” – Universidade de São Paulo

**Resumo:** A Inteligência Artificial (IA) está cada vez mais presente na vida humana, indicando um futuro integrado entre o real e o virtual. Inserido como um campo da IA, o Machine Learning opera com um conjunto de ferramentas que permitem a execução de atividades nas mais diversas áreas do conhecimento. Uma das aplicações dos algoritmos é na área de detecção de fraudes de cartão de crédito, que causam perdas bilionárias para que fazem instituições financeiras e a sociedade. Neste sentido, este trabalho se propôs a identificar de que forma o Machine Learning tem contribuído para este problema financeiro e social, utilizando-se, para tanto, da Revisão Bibliográfica Sistemática, a partir da qual obteve-se diagnósticos primários sobre as áreas do Machine Learning, Fraude e Fraude de Cartão de Crédito. Como fonte de pesquisa, foi selecionado o portal Web of Science, com as buscas centradas no período de 2008 a 2018. Os resultados apontam que, tanto no tema de Machine Learning, quanto no de fraude, grande parte dos trabalhos referem-se às áreas de Medicina & Biomedicina. Na integração entre Machine Learning e fraude de cartão de crédito, foram encontrados cinco trabalhos que, ao serem avaliados integralmente, revelaram-se com um bom poder de detecção de fraudes. Há, no entanto, um caminho a ser percorrido, que permita comparar os métodos empregados a partir de um banco de dados comum.

**Palavras-chave:** Inteligência Artificial; Algoritmos; Detecção.

**Abstract:** Artificial Intelligence (AI) has become increasingly present in human life, pointing to an integrated future with the real and the virtual walking side by side. Inserted as an AI field, Machine Leaning operates with a set of tools, called algorithms, that allow performing activities in almost every area of knowledge, whether in Biology, Math and Science or Humanities. An application of the algorithms is in the area of credit card fraud detection, which causes financial institutions and society to lose billions of dollars every year. In this sense, this work aimed to identify how Machine Learning has contributed to this financial and social problem. For this proposal, it was used the Systematic Bibliographic Review, from which it was obtained primary diagnoses on the

areas of Machine Learning, Fraud and Credit Card Fraud, in order to arrive at a thorough portrait of the subject. As a source of research, it was used in the Web of Science portal, with searches centered on the period from 2008 to 2018. The results show that, both in the subject of Machine Learning and fraud, most of the works refer to areas of Medicine & Biomedicine. In the integration between “Machine Learning” and credit card fraud, five papers were found that, when fully evaluated, proved to have good fraud detection power. There is, however, a way to go that allows comparing the methods employed from a common database.

**Key-words:** Artificial Intelligence; algorithms; Detection.

## INTRODUÇÃO

O Machine Learning ou Aprendizado de Máquina é um campo da Inteligência Artificial que estuda o reconhecimento de padrões, visando classificação e/ou predição de determinados comportamentos, com base em um conjunto de dados. Em meados da década de 2000, o Machine Learning passou a ser cada vez mais difundido, de modo a se tornar, na década seguinte, uma ferramenta capaz de auxiliar desde atividades mais simples, como a filtragem Anti-Spam de e-mails, até em questões de maior complexidade, como a segurança de dados na internet (DOMINGOS, 2012).

O Machine Learning trabalha com duas formas básicas de aprendizagem: a supervisionada e a não supervisionada. Na aprendizagem supervisionada, é dada uma predefinição para o programa, ou seja, o cientista indica que determinado padrão se refere a determinado comportamento, de modo que o algoritmo saiba reconhecer os novos dados e classificá-los conforme o que foi supervisionado. Na aprendizagem não supervisionada, o programa não possui conhecimento inicial sobre os dados, podendo encontrar padrões por si só, ou seja, não há uma supervisão que ligue um padrão a um determinado comportamento, não há uma indicação prévia (ALPAYDIN, 2009)

Um campo de aplicação em que o aprendizado supervisionado tem sido utilizando é da detecção de fraudes, ou seja, situações em que pessoas, cenários e/ou organizações são manipuladas, com o intuito de se obter vantagem ilícita, em prol de benefício próprio, seja ele individual ou corporativo. Existe uma extensa

aplicabilidade do tema fraude: na ciência, por exemplo, pode ocorrer por plágio ou manipulação de resultados; no ambiente empresarial, se configura por alteração de balanços contábeis, caixa-dois e apropriações indevidas; no governo, a partir desvios de verba e propinas; e na sociedade, desde simples ações, como furar a fila em um banco, até falsas pirâmides e golpes financeiros.

Uma categoria de fraude que tem crescido nos últimos anos é o golpe de cartão de crédito, principalmente por clonagem. Até as décadas passadas, os cartões eram clonados por leitores óticos adulterados, que transmitiam informações aos fraudadores. Atualmente, no entanto, a exposição maior está no ambiente virtual, devido ao intenso volume de transações comerciais e pagamentos “online”. Segundo estudo realizado pela consultoria The Nilson Report (2016), no ano de 2015, os valores perdidos com a fraude de cartão de crédito atingiram, mundialmente, 21,84 bilhões de dólares, o que representa, em Reais, R$ 85,26 bilhões, valor superior ao Produto Interno Produto de 46% dos países do mundo (FMI, 2019).

Por esta razão, o desenvolvimento de mecanismos que permitam a identificação destes cenários fraudulentos é essencial, ao passo que possibilita o direcionamento dos esforços para o combate destes golpes. No entanto, para que se possa avançar, é fundamental entender quais são os mecanismos que a literatura já dispõe, ou seja, o que se sabe sobre o papel do Machine Learning na detecção de fraude de cartão de crédito. E avanços nesta área de estudo são importantes tanto para a sociedade, sendo diretamente atingida pelos golpes, quanto para as empresas de cartão de crédito, ao passo que desejam oferecer aos seus clientes uma maior segurança nas transações comerciais e reduzir as perdas ocasionadas pelas fraudes.

Nesse sentido, o objetivo deste trabalho é investigar quais são as ferramentas atuais utilizadas na detecção de fraude de cartão de crédito, avaliando suas assertividades por análise bibliográfica sistemática dos trabalhos publicados no Brasil e no mundo, entre os anos de 2008 e 2018.

## DESENVOLVIMENTO

### Metodologia

A metodologia utilizada neste estudo foi a Revisão Bibliográfica Sistemática (RBS), ferramenta que permite uma análise criteriosa da literatura, caracterizando quantitativa e qualitativamente o desenvolvimento científico de determinada área, e identificando, conforme Conforto et al. (2011), seu “estado da arte”, ou seja, aquilo que se tem de mais recente, inovador e eficaz em relação ao assunto destacado.

A RBS carrega o caráter sistemático pelo fato de exigir um roteiro de execução. Não se trata de uma revisão bibliográfica narrativa, onde é apresentada uma descrição, geralmente histórica, sobre determinado tema, destacando-se artigos relevantes ao longo do tempo. Ao adotar-se um método criterioso de revisão bibliográfica, é possível reduzir vieses, aumentar a confiabilidade, analisar o comportamento e identificar tendências do tema investigado (DE MEDEIROS ET AL., 2015).

Neste sentido, para a execução da RBS, foi adotado o procedimento sugerido por Conforto et al. (2011), a partir do qual foram realizadas algumas adaptações, para o cumprimento dos objetivos deste trabalho. O método empregado consiste em três etapas: entrada, processamento e saída. A estrutura de análise foi definida da seguinte forma:

*Etapa de Entrada*

- Definição do Problema: o que tem sido discutido academicamente na área de intersecção entre o Machine Learning e a detecção de fraude de cartão crédito, no período de 2008 a 2018?
- Levantamento de fontes primárias: As buscas foram realizadas na base Web of Science, com artigos de livre acesso, brasileiros ou internacionais, no período de 2008 a 2018. A seleção de trabalhos exclusivamente de livre acesso se deu não só pela limitação da quantidade de artigos, mas também pela necessidade ocasional de consulta da íntegra dos trabalhos.
- Definição das strings de busca: “Machine Learning” (1), “Fraud OR Fraude” (2), “Fraude de Cartão de Crédito OR Credit Card Fraud” (3) e

“Machine Learning AND Fraude de Cartão de Crédito OR Machine Learning AND Credit Card Fraud” (4).

- Definição dos critérios de inclusão: para a análise das strings (1) e (2), foram avaliados artigos com livre acesso e no mínimo cinco citações, com o intuito de caracterizar os respectivos campos de estudos. Para a string (3), devido à restrição numérica de trabalhos encontrados, avaliaram-se todos, independentemente do número de citações. Na string (4), foram incluídos na análise apenas os artigos que apresentaram a aplicação de pelo menos um algoritmo de “Machine Learning” para a detecção de cenários de fraude de cartão de crédito.
- Definição dos critérios de qualificação: nas strings (1), (2) e (3), foram avaliados os títulos, os resumos e as palavras chaves dos artigos. Na string (4), os artigos foram avaliados integralmente.
- Definição dos métodos e ferramentas de análise: as buscas foram realizadas na base Web of Science, no período definido de janeiro de 2008 a dezembro de 2018.

*Etapa de Processamento*

- Realização das buscas: as buscas foram realizadas no portal da base de dados Web of Science, visando apenas artigos com acesso aberto, diante da necessidade de consulta da íntegra dos materiais.
- Leitura e Análise dos Resultados: a partir dos filtros estabelecidos previamente, foram realizadas as leituras. Parcialmente, 9.346 artigos foram analisados, distribuídos nas strings (1), (2), (3) e (4). Integraram-se cinco artigos, identificados com aplicação de algoritmos para a detecção de fraude de cartão de crédito.
- Documentação e arquivamento dos artigos selecionados: os artigos foram todos documentados, em planilha de MS Excel®, conforme extração do Web of Science. Os artigos analisados foram integralmente arquivados e salvos em pasta específica.

*Etapa de Saída*

- Síntese e Resultados: por fim, a síntese de resultados foi realizada, contemplando a interpretação da leitura dos artigos e dos gráficos elaborados. Nas strings (1), (2) e (3), as informações analisadas referem-se ao conteúdo dos títulos, através de mineração de texto, expressa a partir de word clouds elaboradas com auxílio do software R/RStudio e do pacote adicional “wordcloud”. Os campos de aplicação foram separados, inicialmente, entre Ciências Naturais, Exatas e Humanas. Em seguida, as informações foram desagregadas por áreas temáticas, como Medicina e Biomedicina, Química & Biologia e Engenharia & Robótica. Analisaram-se, a partir disso, a evolução das publicações por área durante o período entre 2008 e 2018 e os principais meios de publicação dos trabalhos, como revistas, jornais, periódicos, em geral. Na string (4), foram avaliadas as publicações por ano, os algoritmos e as abordagens utilizadas, a descrição dos bancos de dados e as variáveis disponíveis e, por fim, os algoritmos de melhor desempenho entre os cinco artigos. As análises foram dispostas de forma condensada na seção de Resultados.

## Resultados

### *Machine Learning*

Ao se pesquisar pelo tema Machine Leaning no portal Web of Science, no período de 2008 a 2018, obteve-se um retorno de 95.304 resultados, dos quais 20.102 são de acesso aberto, distribuídos em diversos campos de conhecimento. Destes, 16.011 são classificados como artigos científicos. Aplicando-se o filtro de cinco ou mais citações, restaram 8.943 artigos. A primeira classificação destes trabalhos foi realizada com base na grande área de conhecimento. O tema Machine Learning foi amplamente aplicado no campo das Ciências Naturais, com cerca de 75% das publicações. Em seguida, aparecem as Ciências Exatas, com 22% e as Ciências Humanas, com 3%.

Ao avaliar-se a evolução de cada campo ao longo do período estabelecido, é possível inferir, a partir da Figura 1, que as aplicações em Ciências Humanas se

mantiveram relativamente estáveis, enquanto nas Ciências Exatas e Naturais, houve aumento considerável no número publicações. Destaca-se, no entanto, que os três campos apresentaram uma queda no ano de 2018, fato associado à filtragem realizada, que selecionou artigos com cinco ou mais citações. Muitos artigos do ano de 2018 não atingiram o índice mínimo para sua inclusão na análise, porém isso se deve ao aspecto temporal, e não a uma questão de queda de publicações.

Outra inferência importante é o distanciamento que o campo das Ciências Naturais apresenta em relação aos demais. No ano de 2008, os três campos estavam relativamente próximos, ainda pelo fato do Machine Learning ser um tema novo, à época. Já no ano de 2017, com os algoritmos mais popularizados, observa-se uma disparidade entre os campos, demonstrando como o Machine Learning se tornou familiar com maior velocidade nas Ciências Naturais.

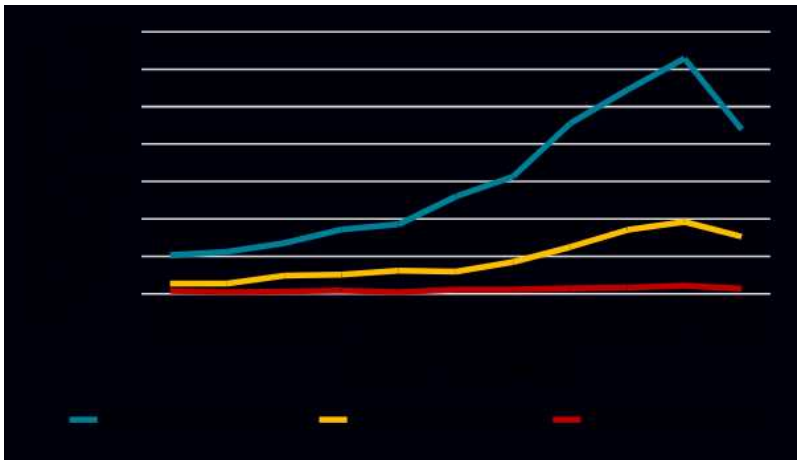


Figura 1 - Evolução da quantidade de publicações com aplicação de Machine Learning por campo de conhecimento, de 2008 a 2018, com base no portal Web of Science.

A partir da Tabela 1, é possível obter o desmembramento dos três campos apresentados. Cerca de 38% do total dos artigos está aplicado na área de Medicina & Biomedicina, enquanto 30% está centro na área Química & Biologia, demonstrando como o Machine Learning tem sido explorado nessas duas áreas. Em seguida, com cerca de 5,6%, aparecem Engenharia & Robótica. Ressalta-se, no entanto, a discrepância entre o segundo e o terceiro colocado, em torno de 24 pontos percentuais. Física & Astronomia aparecem em quarto lugar, com 4% de participação, seguidas por Data Science, Tecnologia, Agricultura e Psicologia &

Comportamento Humano. A área com menor participação foi a Gestão Pública, com apenas 4 artigos publicados, o equivalente a 0,04%. Além disso, outros 4 artigos não apresentaram informações suficientes para sua classificação.

Tabela 1. Quantidade de artigos publicados com aplicações de Machine Learning por área de conhecimento, de 2008 a 2018, com base no portal Web of Science.

| Área de Conhecimento | Quantidade de Artigos | Participação (%) |
|---|---|---|
| Medicina & Biomedicina | 3380 | 37,79% |
| Química & Biologia | 2650 | 29,63% |
| Engenharia & Robótica | 500 | 5,59% |
| Física & Astronomia | 355 | 3,97% |
| Data Science | 354 | 3,96% |
| Tecnologia | 339 | 3,79% |
| Agricultura & Pecuária | 331 | 3,70% |
| Psicologia & Comportamento Humano | 192 | 2,15% |
| Matemática & Estatística | 169 | 1,89% |
| Geografia & Meteorologia | 136 | 1,52% |
| Tecnologia da Informação | 129 | 1,44% |
| Linguística | 100 | 1,12% |
| Farmácia | 95 | 1,06% |
| Economia & Administração | 83 | 0,93% |
| Educação Física & Esporte | 47 | 0,53% |
| Transporte & Logística | 20 | 0,22% |
| Educação & Ciência | 19 | 0,21% |
| Música | 16 | 0,18% |
| Direito | 13 | 0,15% |
| Comunicação & Jornalismo | 7 | 0,08% |
| Gestão Pública | 4 | 0,04% |
| Não Classificado | 4 | 0,04% |
| Total | 8943 | 100,00% |

Fonte: Web of Science (2019). Elaborado pelos autores

Com base na ferramenta wordcloud (Figura 2), foi possível observar que palavras como "câncer", “disease”, “human”, “clinical” e “diagnosis” são as mais frequentes nos títulos dos artigos, demonstrando, novamente, a supremacia das áreas da Medicina e Biomedicina. Verificou-se também, que o “Machine Learning” tem sido utilizado como ferramenta para a detecção de doenças, como o câncer, além de outras identificadas nos trabalhos, como Parkinson, Alzheimer e Demência. Por meio das palavras “gene” e “protein”, há indícios de que outro uso aplicado do "machine learning" é na área da genética e microbiologia.



Figura 2 - Wordcloud dos títulos dos artigos com aplicação de Machine Learning, no período de 2008 a 2018, com base no portal Web of Science.

*Fraude*

Em fraude, a pesquisa, realizada nos parâmetros estabelecidos, apresentou 8.953 resultados, dos quais 1.506 são de acesso aberto. Deste total, 1.101 são classificados como artigos científicos. Ao realizar a filtragem das citações, restaram 362 artigos para análise. A análise revelou que, mesmo quando o tema é fraude, as Ciências Naturais ainda levam vantagem na quantidade de publicações, contempladas com 43% do total de artigos. Em relação ao Machine Learning, há uma troca de posição nos demais campos. As Ciências Humanas aparecem em segundo lugar, com 33%, enquanto as Ciências Exatas foram responsáveis por 24% das publicações.

Em termos da evolução das publicações, os três campos apresentaram comportamento oscilante, porém crescente ao longo do tempo. Assim como no caso do Machine Learning, no ano de 2008 os campos estavam próximos em número de publicações. No decorrer do período, é possível observar vantagem das Ciências Naturais, porém em menor grau de discrepância. Por fim, nos anos de 2017 e 2018, observa-se um comportamento de queda, mas fruto de dois fatores: a oscilação presente na série (2017) e o filtro de citações que retirou considerável quantidade de artigos, pelo curto tempo para que o trabalho seja citado (2018).

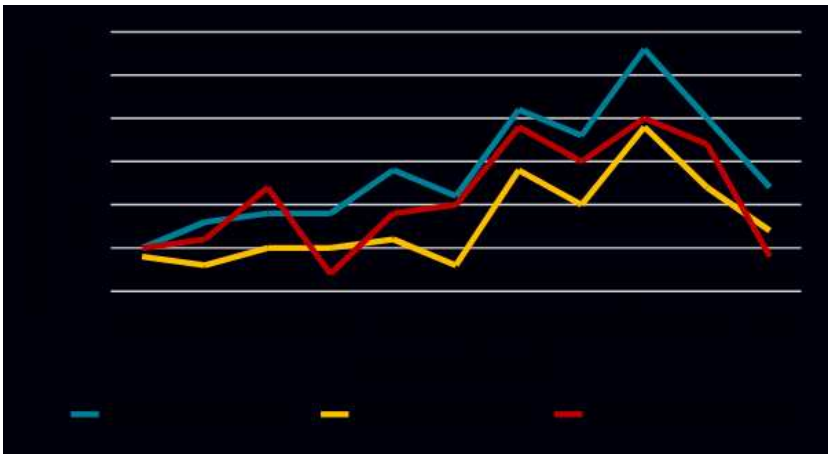


Figura 3 - Evolução da quantidade de publicações com abordagens relativas a fraudes, por campo de conhecimento, de 2008 a 2018, com base no portal Web of Science.

De modo similar ao comportamento observado no tema Machine Learning, as áreas Medicina & Biomedicina e Química & Biologia lideram o número de publicações relacionadas à fraude, sendo responsáveis, juntas, por cerca de 38,4% do total de artigos. Em seguida, Tecnologia da Informação e Economia & Administração aparecem, ambas, com 12,15%.

Tabela 2. Quantidade de artigos publicados com abordagens relativas a fraudes por área de conhecimento, no período de 2008 a 2018, com base no portal Web of Science.

| Área de Conhecimento | Quantidade de Artigos | Participação (%) |
|---|---|---|
| Medicina e Biomedicina | 75 | 20,72% |
| Química & Biologia | 64 | 17,68% |
| Tecnologia da Informação | 44 | 12,15% |
| Economia & Administração | 44 | 12,15% |
| Engenharia & Robótica | 30 | 8,29% |
| Direito | 23 | 6,35% |
| Gestão Pública | 18 | 4,97% |
| Agricultura & Pecuária | 13 | 3,59% |
| Sociologia | 12 | 3,31% |
| Educação & Ciência | 12 | 3,31% |
| Matemática & Estatística | 9 | 2,49% |
| História & Filosofia | 4 | 1,10% |
| Física & Astronomia | 3 | 0,83% |
| Geografia | 3 | 0,83% |
| Outros | 8 | 2,21% |
| Total | 362 | 100,00% |

Fonte: Web of Science (2019). Elaborado pelos autores.

Por meio da ferramenta word cloud (Figura 4), observou-se, novamente, a presença de palavras relativas à Medicina e Biomedicina, como health, medical. Há, no entanto, palavras como food, meat e olive, relativos ao eixo da Agricultura & Pecuária. Ressalta-se, também, a presença da palavra financial, remetendo a questões de fraude financeira, grande grupo da fraude de cartão de crédito.




Figura 4 - Wordcloud dos títulos dos artigos com aplicações do tema Fraude, no período de 2008 a 2018, com base no portal Web of Science.

*Fraude de Cartão de Crédito*

Em relação ao tema fraude de cartão de crédito, a pesquisa inicial apresentou 381 resultados, dos quais apenas 29 eram de acesso aberto. Diante do número restrito de trabalhos, não foi realizada a filtragem subsequente. Portanto, os 29 artigos foram analisados. Conforme a Tabela 3, destes 29 trabalhos, 23 referem-se ao tema Cartão de Crédito, o que representa cerca de 79% do total de publicações. Além disso, os temas Cartão de Presente, Cheques, Dados Espaço-Temporais, Finanças, Passagens Aéreas e Cigarro completam os tópicos abordados, com uma publicação cada.

Tabela 3. Quantidade de artigos publicados com a temática de Fraude de Cartão de Crédito, por assunto de aplicação, de 2008 a 2018, com base no portal Web of Science.

| Tópico | Quantidade de Artigos | Participação (%) |
|---|---|---|
| Cartão de Crédito | 23 | 79,31% |
| Cartão de Presente | 1 | 3,45% |
| Cheques | 1 | 3,45% |
| Dados Espaço-temporais | 1 | 3,45% |
| Finanças | 1 | 3,45% |
| Passagens Aéreas | 1 | 3,45% |
| Cigarro | 1 | 3,45% |
| Total | 29 | 100,00% |

Fonte: Web of Science (2019). Elaborado pelos autores.

Considerando apenas os trabalhos publicados com a temática “cartão de crédito”, observa-se, a partir do gráfico apresentado na Figura 5, a crescente produção de materiais publicados. No ano de 2008, apenas um trabalho foi publicado, enquanto, em 2018, o número chegou a sete. Neste caso, diferentemente do comportamento observado com as strings “Machine Learning” e “Fraude/Fraud”, não se observa a queda no último ano do período, pelo fato do filtro de citações não ter sido aplicado.

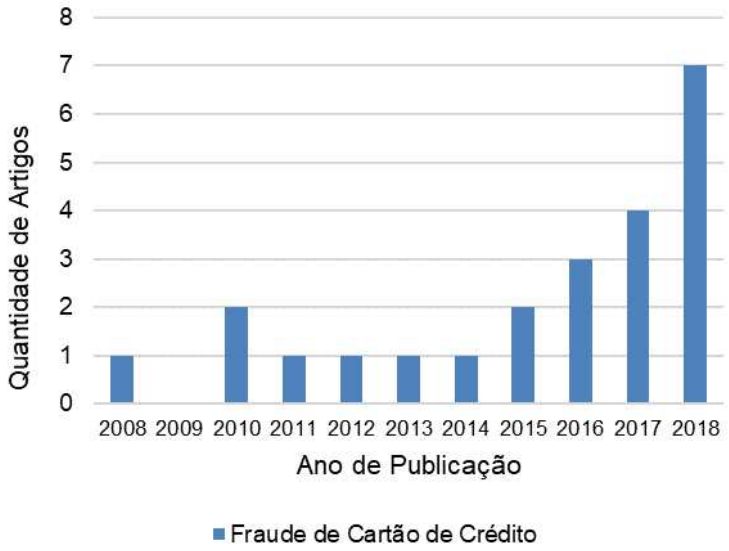



Figura 5 - Evolução da quantidade de publicações com abordagens exclusivamente relativas ao tema Fraude de Cartão de Crédito, por campo de conhecimento, de 2008 a 2018, com base no portal Web of Science

*Machine Learning & Fraude de Cartão de Crédito*

Por fim, foi avaliada a intersecção entre os temas Machine Learning e Fraude de Cartão de Crédito. A partir da string (4), foram encontrados 149 trabalhos, sendo 12 de acesso aberto. Deste total, segundo a Tabela 4, 5 são relacionados à detecção de fraude de cartão de crédito, enquanto os demais trabalham com Data Science e Detecção de Outliers.

Tabela 4. Quantidade de artigos publicados envolvendo “Machine Learning” e Fraude de Cartão de Crédito, por tópico

de aplicação, de 2008 a 2018, com base no portal “Web of Science”

| Tópico | Quantidade de Artigos | Participação (%) |
|---|---|---|
| Fraude de Cartão de Crédito | 5 | 41,67% |
| “Data Science” | 4 | 33,33% |
| Detecção de “Outliers” | 3 | 25,00% |
| Total | 12 | 100,00% |

Fonte: “Web of Science” (2019). Elaborado pelos autores

Após a filtragem destes 5 artigos, realizou-se uma análise de seus respectivos conteúdos. De maneira sintética, observa-se, a partir da Figura 6, que os cinco artigos avaliados utilizaram, ao todo, dezessete algoritmos distintos, sendo que Logistic Regression e Random Forest apresentaram maior reincidência, com abordagem em três trabalhos. Em seguida, aparecem Multi-Layer Perceptron, Naive Bayes, C4.5 e Neural Network, com duas aplicações cada. Com apenas uma utilização, aparecem Linear Regression, K-Nearest Neighbor, Support Vector Machine, Gradient Boost Tree, Random Tree, Parenclitic Network, Deep Learning, Bagging e Decision Stump.

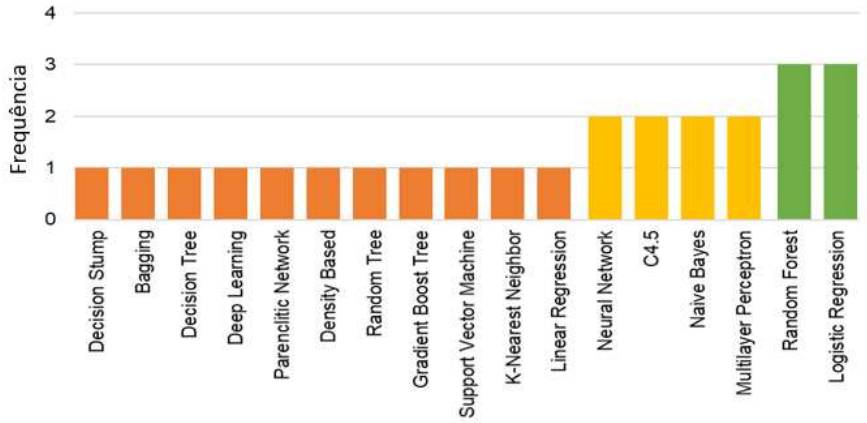



Figura 6 - Algoritmos utilizados para a detecção de cenários de fraude de cartão de crédito, de 2008 a 2018, com base no portal Web of Science.

A Tabela 5 apresenta dados condensados dos cinco artigos selecionados. O primeiro trabalho foi publicado apenas em 2013. Nos demais anos, houve publicação no ano de 2015, sendo que em 2014, 2016 e 2017 não foram encontrados trabalhos

com base nos critérios de busca estabelecidos. No ano de 2018, no entanto, foram publicados três trabalhos relacionados à detecção de fraude de cartão de crédito com base no Machine Learning, apresentando indícios de que o tema tem ganhado um pouco mais de destaque a partir deste ano.

Além disso, observa-se que os trabalhos operam com abordagens distintas. Apesar de todos apresentarem resultados individuais dos algoritmos, foram utilizadas algumas técnicas visando incrementar a qualidade dos resultados, como a Análise Combinada, o Majority Voting, Adaboost, Thresold Optimization, Bayesin Minimum Risk Classifier e Bayesian Minimum Risk Classifier com Probabilidade Ajustada. Em geral, os resultados apresentam melhoria de desempenho, como observado em Zanin et al. (2018) e Randhawa et al. (2018). Há casos, no entanto, em que ferramentas mais complexas tendem a piorar o desempenho dos algoritmos individuais (BAHNSEN ET AL., 2013).

Em relação aos bancos de dados utilizados para as análises, cada trabalho operou com um conjunto distinto, proveniente de Instituições Financeiras, como em Zanin (2018), Bahnsen et al. (2013) e Randhawa et al. (2018). Choi e Lee (2018) obtiveram as informações junto ao mercado de Internet of Things, enquanto Zareapoor et al. (2015) trabalharam com dados viabilizados a partir de uma competição na Universidade da Califórnia.

Em análise das principais variáveis componentes dos bancos de dados, observa-se que a informação sobre o montante da transação é a variável mais utilizada, presente em quatro trabalhos. Em seguida, a variável de maior incidência foi data da transação, abordada em três trabalhos. A bandeira do cartão, o horário da transação, o número do cartão, a identificação do vendedor e a variável binária indicativa de fraude foram utilizadas em 2 trabalhos, cada uma. Destaca-se, no entanto, que a presença da variável no banco de dados não implica que ela seja relevante para o desempenho do algoritmo. A relevância de cada variável está associada ao seu respectivo nível de significância, cuja métrica é definida pelos autores.

Por fim, dos cinco trabalhos analisados, o melhor desempenho de detecção de fraude foi observado em Randhawa et al. (2018), onde obteve-se 100% de

assertividade com os algoritmos Naive Bayes, Random Forest e Random Tree, a partir da abordagem de Adaboost, e aplicação de Decision Stump + Gradient Boost Tree, Decision Tree + Desision Stump, Decision Tree + Gradient Boost Tree, com o incremento do Majority Boosting.

Há, no entanto, de se destacar que, pelo fato dos trabalhos utilizarem bancos de dados distintos, não é possível firmar uma base comparativa em que se possa dizer quais algoritmos e quais métodos possuem melhores poder de detecção de fraudes financeiras.

Tabela 5. Informações condensadas dos artigos que aplicaram Machine Learning para fins de detecção de fraude de cartão de crédito, no período de 2008 a 2018, com base no portal Web of Science.

| Componente | Resultados observados |
|---|---|
| Anos de Publicação | 2013 (1), 2015 (1) e 2018 (3) |
| Abordagens Utilizadas | Algoritmos Individuais (5); Análise Combinada (1); Majority Voting (1); Adaboost (1); Thresold Optimization (1); Bayesin Minimum Risk Classifier (1); Bayesian Minimum Risk Classifier com Probabilidade Ajustada (1) |
| Bancos de Dados | Companhia de Cartão de Crédito Europeia (1); Registros de Transações disponibilizados em competição da Universidade da Califórnia (1); Instituição Financeira da Malásia (1); Transações de cartão de débito e crédito do banco espanhol BBVA (1); Dados de Pagamento no ambiente da Internet of Things, no mercado da Coreia do Sul (1) |
| Variáveis | Montante da Transação (4); Data da transação (3); Bandeira do cartão (2); Horário da transação (2); Identificação do número do cartão (2); Identificação do Vendedor (2); Presença de fraude (variável binária, 0 ou 1) (2); Tipo de Mercadoria (2); Tipo de transação (internet, cartão presente, etc) (2); Banco emissor do cartão (1); Código da moeda da fatura do titular (1); Código da moeda da transação (1); Código de Autenticação do Cliente (1); Código do grupo do vendedor (1); Companhia de Telecomunicação (1); Fatura do titular do cartão (1) |

| | |
|---|---|
| Melhores Desempenhos | RANDHAWA, Kuldeep et al. (2018). Aplicação de Naive Bayes, Random Forest e Random Tree, sob a abordagem de Adaboost; Aplicação de Decision Stump + Gradient Boost Tree, Decision Tree + Desision Stump, Decision Tree + Gradient Boost Tree, sob a abordagem do Majority Boosting |

## CONSIDERAÇÕES FINAIS

O Machine Learning engloba um conjunto de ferramentas utilizadas em diversas áreas do conhecimento, para potencializar a tomada de decisão humana, reduzindo os riscos de erros e suas eventuais consequências. As Ciências Naturais são as principais utilizadoras dos recursos, no entanto, muito tem se trabalhado em demais campos do conhecimento aplicado, como a detecção de fraude de cartão de crédito. Nesta área, alguns algoritmos já apresentam desempenho satisfatório. Contudo, os resultados estão associados à qualidade dos bancos de dados. É notório, portanto, que o Machine Learning tem cooperado na detecção de transações de cartão de crédito fraudulento, mas que existem caminhos abertos para a evolução e melhoria, buscando cenários que comparem e contemplem diferentes algoritmos, sob abordagens distintas, mas que utilizem um banco de dados similar, destacando, também, quais as variáveis são de maior relevância para o melhor desempenho dos métodos.

## REFERÊNCIAS BIBLIOGRÁFICAS

ALPAYDIN, E. 2009. **Introduction to machine learning**. MIT press.

BAHNSEN, A. C., STOJANOVIC, A., AOUADA, D.,OTTERSTEN, B. 2013. Cost sensitive credit card fraud detection using Bayes minimum risk. In: **2013 12th international conference on "Machine Learning" and applications** (Vol. 1, pp. 333-338). IEEE. doi: 10.1109/ICMLA.2013.68

CHOI, Dahee; LEE, Kyungho. An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation. **Security and Communication Networks**, v. 2018, 2018. doi: 10.1155/2018/5483472

CONFORTO, Edivandro Carlos; AMARAL, Daniel Capaldo; SILVA, SL da. Roteiro para revisão bibliográfica sistemática: aplicação no desenvolvimento de produtos e gerenciamento de projetos. In**: 8º Congresso Brasileiro de Gestão de Desenvolvimento de Produto**, Porto Alegre, RS, Brasil. Anais. pages 1--12, 2011.

DE MEDEIROS, Ivan Luiz et al. Revisão Sistemática e Bibliometria facilitadas por um Canvas para visualização de informação. **InfoDesign-Revista Brasileira de Design da Informação**, v. 12, n. 1, p. 93-110, 2015.

[DOMINGOS, Pedro. A few useful things to know about machine learning. **Communications of the ACM**, v. 55, n. 10, p. 78-87, 2012. doi: 10.1145/2347736.2347755

Fundo Monetário Internacional [FMI]. *GDP, current prices* (2015), 2019.

RANDHAWA, Kuldeep et al. Credit card fraud detection using AdaBoost and majority voting. **IEEE access**, v. 6, p. 14277-14284, 2018. doi: 10.1109/ACCESS.2018.2806420

The Nilson Report. *Card Fraud Worldwide*, 2016.

ZANIN, Massimiliano et al. Credit card fraud detection through parenclitic network analysis. **Complexity**, v. 2018, 2018. doi: 10.1155/2018/5764370

ZAREAPOOR, Masoumeh et al. Application of credit card fraud detection: Based on bagging ensemble classifier. **Procedia computer science**, v. 48, n. 2015, p. 679-685, 2015. doi: 10.1016/j.procs.2015.04.201

## Sobre os autores

Gabriel Ferreira dos Santos Silva
Mestrando em Estatística e Experimentação Agronômica – ESALQ/USP
E-mail para contato: gabriel8.silva@usp.br

Daniel Sá Freire Lamarca
Doutorando em Engenharia de Biossistemas – ESALQ/USP
E-mail para contato: lamarca@usp.br

Gabriel Adrian Sarriés
Professor Doutor – Departamento de Ciências Exatas – ESALQ/USP
E-mail para contato: gasarrie@usp.br