UNIVERSIDADE NOVE DE JULHO – UNINOVE
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA E GESTÃO DO CONHECIMENTO

ROGER WILLIAN JOEL LEONARDIS

DETECÇÃO DE FRAUDES EM TRANSAÇÕES COM CARTÃO DE CRÉDITO: UMA COMPARAÇÃO DO DESEMPENHO DE TÉCNICAS INTELIGENTES COM BASE NA AVALIAÇÃO DA FUNÇÃO DE CUSTO

SÃO PAULO
2023

UNIVERSIDADE NOVE DE JULHO – UNINOVE
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA E GESTÃO DO CONHECIMENTO

ROGER WILLIAN JOEL LEONARDIS

DETECÇÃO DE FRAUDES EM TRANSAÇÕES COM CARTÃO DE CRÉDITO: UMA COMPARAÇÃO DO DESEMPENHO DE TÉCNICAS INTELIGENTES COM BASE NA AVALIAÇÃO DA FUNÇÃO DE CUSTO

Dissertação de mestrado apresentada ao Programa de Pós-graduação em Informática e Gestão de Conhecimento da Universidade Nove de Julho – UNINOVE, como requisito parcial para a obtenção do grau de Mestre em Informática e Gestão do Conhecimento

Prof. Orientador: Dr. Renato José Sassi

SÃO PAULO
2023

Leonardis, Roger Willian Joel.
Detecção de fraudes em transações com cartão de crédito: uma comparação do desempenho de técnicas inteligentes com base na avaliação da função de custo. / Roger Willian Joel Leonardis. 2023.
75 f.
Dissertação (Mestrado) - Universidade Nove de Julho - UNINOVE, São Paulo, 2023.
Orientador (a): Prof. Dr. Renato José Sassi.

1. Fraudes em cartão de crédito. 2. Função de custo. 3. Custo de classificação. 4. Inteligência artificial. 5. Base de dados desbalanceada
I. Sassi, Renato José. II. Título.

CDU 004

PARECER – EXAME DE DEFESA

Parecer da Comissão Examinadora designada para o exame de defesa do Programa de Pós-Graduação em Informática e Gestão do Conhecimento a qual se submeteu o aluno Roger Willian Joel Leonardis.

Tendo examinado o trabalho apresentado para obtenção do título de "Mestre em Informática e Gestão do Conhecimento", com Dissertação intitulada "DETECÇÃO DE FRAUDES EM TRANSAÇÕES COM CARTÃO DE CRÉDITO: UMA COMPARAÇÃO DO DESEMPENHO DE TÉCNICAS INTELIGENTES COM BASE NA AVALIAÇÃO DA FUNÇÃO DE CUSTO", a Comissão Examinadora considerou o trabalho:

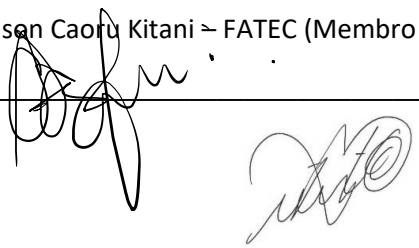
(X) Aprovado **( ) Aprovado condicionalmente**

( ) Reprovado com direito a novo exame **( ) Reprovado**

EXAMINADORES

Prof. Dr. Renato Jose Sassi - Uninove (Orientador)

Prof. Dr. Edson Caoru Kitani – FATEC (Membro Externo)



Prof. Dr. Fabio Henrique Pereira - UNINOVE (Membro Interno)

São Paulo, 26 de junho de 2023

Dedico este trabalho a minha esposa Margarete Nobilo Leonardis

AGRADECIMENTOS

Aos meus pais, Solange e Vanderlei Leonardis (in memoriam) e irmãos, Carla e André Leonardis (in memoriam) que sempre me apoiaram e me ensinaram a buscar sempre mais conhecimentos baseados no esforço e nos estudos, me incentivaram a leitura, a saber ouvir música, abrindo as portas para as outras áreas de conhecimento.

Em especial à minha esposa Margarete Leonardis pela paciência, carinho, compreensão e ajuda em todas as aventuras que inventamos.

Ao meu orientador Prof. Dr. Renato José Sassi, pela ajuda nas horas difíceis, por me trazer ao chão quando levitava nas minhas ideias, pela paciência em acertar os eixos nos momentos que se encontravam desalinhados. E acima de tudo pelo respeito e contribuições, não só neste trabalho, como também no aprendizado diário em nossas reuniões.

Aos colegas João Rafael Evangelista, Marcio Romero, Domingos Napolitano, Dacyr Gatto, Amanda Moura e Cintia Pinho pelas contribuições, auxílios, críticas e muito trabalho conjunto. Também a Prof. Dra. Daniela Biasotto-Gonzalez pelo incentivo contínuo à pesquisa na nossa família.

A Universidade Nove de Julho pela bolsa e apoio à pesquisa, também aos seus docentes e funcionários, pela oportunidade, respeito e profissionalismo, representado aqui pelo Prof. Dr. André Felipe Henriques Librantz.

Aos membros da banca, Prof. Dr. Edson Caoru Kitani e Prof. Dr. Fabio Henrique Pereira por aceitarem o convite e pelas contribuições neste trabalho.

People think of education as something that they can finish.
Issac Asimov

RESUMO

A detecção de fraudes em cartões de crédito enfrenta um problema relativo ao número de casos de fraudes ser menor do que o de não fraudes, dificultando a detecção por parte de técnicas inteligentes. A solução passa pela aplicação de dois métodos que tratam este desbalanceamento, o *Oversampling* e o *Undersampling*. Para avaliar e comparar o desempenho das técnicas, utiliza-se a Matriz de Confusão (MC), o Coeficiente de Correlação de Matthew (MCC), a Área sob a Curva (AUC) e a Função de Custo (FC). O resultado da FC quantifica o impacto financeiro causado por uma classificação incorreta e, por se tratar de custo, quanto menor o seu valor, melhor o desempenho da técnica. O objetivo geral deste trabalho foi comparar o desempenho de técnicas inteligentes com base na avaliação da Função de Custo para detectar fraudes em transações com cartões de crédito em base de dados desbalanceada. A base de dados utilizada contém informações sobre transações realizadas com cartões de crédito europeus coletadas no ano de 2013. Foram aplicadas as seguintes técnicas: Regressão Logística (RL), *Decision Trees* (DT), *Random Forest* (RF), *Support Vector Machine* (SVM), *Deep Learning* (DL) e XGBoost (XG), sobre as bases de dados desbalanceada e balanceada com Oversampling e Undersampling. Para avaliar e comparar os resultados foram utilizadas a MC, o MCC, a AUC e a FC. O melhor desempenho para a AUC foi da RL com Oversampling, para o MCC foi da RF aplicada à base desbalanceada e para a FC, novamente a RL com Oversampling foi a melhor. A justificativa para a RL com Oversampling apresentar o melhor desempenho em duas das três métricas avaliadas pode residir no fato de ser uma técnica tradicionalmente aplicada em problemas de detecção de fraudes e, por isto, apresentou mais aderência à base de dados utilizada. No estudo do Aprendizado de Máquina, o princípio da Navalha de Occam recomenda que, diante de vários modelos, o mais simples deve ser escolhido, como ocorreu com a RL com Oversampling. Ao considerar o custo de uma predição incorreta, não basta avaliar somente os resultados obtidos com as métricas AUC e MCC, deve-se considerar também a aplicação da FC para apoiar a escolha de uma técnica inteligente.

Palavras-chave: Fraudes em Cartão de Crédito, Função de Custo, Custo de Classificação, Inteligência Artificial, Base de Dados Desbalanceada.

ABSTRACT

Credit card fraud detection faces an issue with the number of the fraud transactions being lower than non-fraud, making it difficult for machine learning models to effectively detect them. There are different types of solution to fix this imbalance, Oversampling and Undersampling can be used to deal with it. To evaluate and compare the performance of the machine learning models, metrics like the Confusion Matrix (CM), the Matthew Correlation Coefficient (MCC), the Area under the Curve (AUC) and the Cost Function (FC) can be applied. The FC result quantifies the financial impact caused by a real fraud misclassification and, because it is cost related, the lower its value the better its performance. The objective of this experiment was to compare the performance of machine learning models using the FC to detect fraud in credit card transactions in an unbalanced dataset. The dataset contains information about European credit cards transactions collected in 2013. The following models were applied: Logistic Regression (RL), Decision Trees (DT), Random Forest (RF), Support Vector Machine (SVM), Deep Learning (DL) and XGBoost (XG), over the unbalanced and balanced databases with Oversampling and Undersampling. To evaluate and compare the results, CM, MCC, AUC and FC were used. The best performance for AUC was RL with Oversampling, for MCC was for RF applied to the unbalanced base and for FC also RL with Oversampling presented the best performance. The reasons why RL with Oversampling outperformed the other models in two out of the three metrics may be connected to the common use of this model in fraud detection problems, therefore presented more adherence to the database used. As stated in the principle of Occam's Razor the recommendation for Machine Learning models use is to adopt the simplest one: RL with Oversampling. When considering the cost of an incorrect prediction, it is not enough to evaluate only the results obtained with the AUC and MCC metrics, one should also consider the results of the FC to support of a machine learning model definition.

Keywords: Credit Card Fraud, Cost Function, Classification cost, Artificial Intelligence, Imbalanced dataset

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE SIGLAS

ADASYN	–	*Adaptative Synthetic Sampling*
ANN	–	*Artificial Neural Network*
AUC	–	*Area Under the Curve*
Cadm	–	Custo Administrativo
Ctrans	–	Custo de Transação
DL	–	*Deep Learning*
DLor	–	*Deep Learning* aplicada à base de dados original
DLov	–	*Deep Learning* aplicada à base com *Oversampling*
DT	–	*Decision Trees* (Árvores de Decisão*)*
DTor	–	Árvores de Decisão aplicada à base de dados original
DTov	–	Árvores de Decisão aplicada à base com *Oversampling*
DTun	–	Árvores de Decisão aplicada à base com *Undersampling*
FC	–	Função de Custo
FN	–	Falso Negativo
FP	–	Falso Positivo
IA	–	Inteligência artificial
KNN	–	*K-Nearest Neighbor*
LSTM	–	*Long Short-Term Memory*
MC	–	Matriz de Confusão
MCC	–	*Mathew Correlation Coefficient*
NB	–	*Naïve Bayes*
POS	–	*Point of Sale*
RF	–	*Random Forest*
RFor	–	*Random Forest* aplicada à base de dados original
RFov	–	*Random Forest* aplicada à base com *Oversampling*
RFun	–	*Random Forest* aplicada à base com *Undersampling*
RL	–	Regressão Logística
RLor	–	Regressão Logística aplicada à base de dados original
RLov	–	Regressão Logística aplicada à base com *Oversampling*
RLun	–	Regressão Logística aplicada à base com *Undersampling*
RNN	–	*Recurrent Neural Networks*
ROC	–	*Receiver Operating Characteristic*
SMOTE	–	*Synthetic Minority Oversampling Technique*
SVM	–	*Support Vector Machine* (Máquina de vetores de suporte)
SVor	–	SVM aplicada à base com dados originais
SVov	–	SVM aplicada à base com *Oversampling*
SVun	–	SVM aplicada à base com *Undersampling*
VP	–	Verdadeiro Positivo
VN	–	Verdadeiro Negativo
XG	–	*XGboost*
XGor	–	*XGboost* aplicada à base de dados original

SUMÁRIO

1 INTRODUÇÃO

Os primeiros cartões de crédito foram criados em 1950, contando com apenas 200 clientes e com uma finalidade exclusiva de serem utilizados em bares e restaurantes da cidade de Nova Iorque (*Diners club*). No Brasil, os primeiros cartões de crédito foram introduzidos no ano de 1954 (DINERS, 2021).

Na década de 1970, as transações eram puramente manuais, com sistema de consulta de validade em listas físicas, entregues diariamente. Na década de 1980, com a introdução da tarja magnética nos cartões, a identificação de sua validade ficou instantânea, e a consulta da existência de crédito para a transação realizada em alguns segundos. No final do século XX os cartões de crédito receberam uma proteção adicional, os *chips*, dificultando a cópia do cartão e trazendo mais segurança para os clientes e lojistas (VISA, 2021).

Segundo Lorey (2008), o funcionamento do mercado de cartões de crédito no Brasil é caracterizado por 5 entidades envolvidas no processo de emissão de cartões: as Bandeiras, os Emissores, os Estabelecimentos Comerciais, os Clientes e os Adquirentes.

Bandeiras são as empresas responsáveis pela estrutura e as normas operacionais, que estão presentes nos sistemas de cartões de crédito. Emissores são as empresas que emitem e mantém o relacionamento com os Clientes dos cartões de crédito, são responsáveis pela concessão, uso e a coleta de pagamento das despesas utilizadas pelos Clientes.

O Emissor pode ser uma instituição financeira ou uma loja de departamento, que neste caso é chamada de Administradora. Adquirentes são as entidades que repassam o dinheiro dos emissores para os comerciantes no prazo que é determinado em contrato. Os Estabelecimentos Comerciais contratam as máquinas de ponto de venda, *Point Of Sale* (POS), junto aos Adquirentes para atender aos clientes (LOREY, 2008).

No período de pandemia, os níveis de transações de cartão de crédito foram afetados pelo uso de cartões pré-pagos e cartões de débito do auxílio emergencial fornecidos pelo governo federal. Mesmo assim, os valores transacionados ultrapassaram 1,18 trilhões de reais (ABECS, 2021). Em 2021 os valores de transações de cartão de crédito tiveram um crescimento de 6,4%, durante o primeiro trimestre do ano (ABECS, 2021).

Com o avanço dos modelos digitais de pagamentos, a forma de utilização dos cartões ganhou uma nova dimensão. Porém, em termos de segurança, o modelo presencial tradicional e o modelo *online* apresentam uma disparidade nos níveis de confiança das transações. Nas operações *online* apenas os dados do cartão são necessários para a compra. Já nas lojas físicas, a apresentação do cartão com *chip* e a entrada de uma senha são obrigatórias (FANG; ZHANG; HUANG, 2019).

Diante do cenário com a coexistência dos modelos presencial e online, o aumento constante do volume de transações e a ocorrência constante de exposição de dados, fraudadores tem diversas oportunidades para se aproveitarem desta situação.

Destaca-se, que em 2020, no Brasil ocorreram graves casos de vazamentos de informações, com 2.84 milhões de cartões de crédito e débito expostos na *internet*, um valor que representa mais de 45% do total dos casos mundiais (AXUR, 2021).

Para atender aos requisitos de segurança de seus clientes e para se protegerem de golpes, as empresas do mercado de cartão de crédito não tem outra alternativa, a não ser investirem em sistemas antifraude (FANG; ZHANG; HUANG, 2019).

Bolton e Hand (2001) definem a ocorrência de fraude em duas categorias: fraudes por comportamento e por aplicação. As fraudes por aplicação se referem a indivíduos que solicitam um novo cartão de crédito, utilizando documentos falsos ou roubados. As fraudes por comportamento estão relacionadas ao roubo ou clonagem de cartões de crédito já existentes.

Devido ao crescimento contínuo de fraudes combinado com a crescente utilização de cartões de crédito, são necessários investimentos em prevenção para atender a demanda de uso, seja *online* ou *offline* (OLOWOOKERE; ADEWALE, 2020).

O desenvolvimento da capacidade computacional e de novas formas de comunicação com os clientes, geraram novas opções para os emissores e seus clientes. Identificar formas eficientes de detectar fraudes em cartões de crédito, sobretudo com o emprego de técnicas baseadas em Inteligência Artificial (IA), também denominadas técnicas inteligentes, é uma necessidade de mercado (LIU; GU; SHANG, 2020; TRISANTO et al., 2020). (LIU; GU; SHANG, 2020; TRISANTO et al., 2020).

Técnicas inteligentes já foram aplicadas para a detecção de fraudes em bases de dados de cartões de crédito. Segundo Al-Hashedi e Magalingam (2021), as técnicas mais aplicadas foram: *Support Vector Machines* (SVM); *Decision Trees*; Regressão Logística; Redes Neurais Artificiais; Naive Bayes; *K-Nearest Neighbor* (KNN).

Os resultados obtidos com a aplicação destas técnicas podem ser comparados, utilizando métricas de desempenho. Isto pode ser feito pela análise da aplicação das técnicas à base de dados em uma tabela, denominada Matriz de Confusão (MC).

Desta forma diferentes métricas podem ser extraídas, tais como: Acurácia, Precisão, *Recall* ou Recuperação, Especificidade, Taxa de Erro, F1 *Score*, Característica de Operação do Receptor (ROC), Área sob a Curva do gráfico ROC (AUC) e Coeficiente de Correlação de Matthew (MCC) (TAE; HUNG, 2019).

Outro método de comparação que pode ser utilizado é a chamada Função de Custo (FC). A FC apresentada por Hand et al., (2007), utiliza o custo atrelado ao erro de detecção de uma fraude por parte da aplicação da técnica inteligente, coletando as informações oriundas da MC. A consequência direta é que o pagamento da transação que foi realizada, por ser fruto de uma fraude, terá o seu valor associado a uma perda financeira.

A importância da aplicação da FC reside em ser uma métrica adicional às métricas mais utilizadas na comparação do desempenho de técnicas inteligentes, a visão monetária/financeira do uso da técnica (DAL POZZOLO *et al.*, 2014).

O estudo das características e forma de abordagem do problema pode trazer impacto positivo no serviço fornecido aos usuários de cartão de crédito. Em uma primeira observação no volume das transações de crédito, em geral, destaca-se a desproporcionalidade dos casos identificados como fraude e os de não fraude, chamado de desbalanceamento (DAL POZZOLO *et al.*, 2014).

O desbalanceamento pode provocar dificuldade para a técnica inteligente, que irá, por exemplo, classificar os casos ou exemplos. Isto pode ocorrer porque numa base de dados do mundo real, a quantidade de exemplos de fraudes é, consideravelmente menor do que os exemplos de não fraude, podendo ocasionar o enviesamento dos resultados, o que levará a erros de classificação.

A fim de tratar o problema de desbalanceamento, Fang, Zhang e Huang (2019) utilizaram com sucesso o método de balanceamento sintético, do inglês *Synthetic*

Minority Oversampling Technique (SMOTE) ou, simplesmente *Oversampling*. O objetivo foi aumentar sinteticamente a chamada classe minoritária, geralmente os casos de fraudes, para reduzir o desbalanceamento e apresentar à técnica inteligente, um conjunto de treinamento que facilite a detecção de fraudes.

Outra forma de correção do desbalanceamento é chamada de *Undersampling*. Este método consiste em eliminar aleatoriamente instâncias da classe majoritária, geralmente casos de não fraude, alterando artificialmente a proporcionalidade com a classe minoritária, os casos de fraude (TRISANTO et al., 2020).

Diante deste cenário, considera-se relevante a realização de estudos que aplicam técnicas inteligentes na detecção de fraudes em transações com cartões de crédito com o desempenho avaliado pela FC.

1.1 JUSTIFICATIVA DA PESQUISA

A análise e prevenção de fraudes é um conceito estritamente ligado a valores e à ética na sociedade como um todo. Identificar e evitar este comportamento tem um efeito positivo na confiança e postura das pessoas frente a novas tecnologias e adoção de meios eletrônicos de pagamento (SLADE *et al.*, 2015).

A identificação de fraudes em transações de cartões de crédito tem utilidade para instituições financeiras, para as operadoras de cartão de crédito, além de prestar um serviço de proteção aos usuários clientes. Para os detentores de cartão de crédito são tentativas de uso indevido barradas e danos financeiros evitados.

As técnicas e conceitos aplicados podem ser utilizados por empresas financeiras que controlam as aprovações de cartão de crédito de seus clientes, visto que hoje estas empresas têm acesso a capacidade computacional em nuvem, com possibilidade de explorar o seu uso eficaz em tempo real.

Existe uma variedade de técnicas disponíveis com capacidade de detecção de fraudes. O levantamento bibliográfico realizado neste trabalho revelou que as Redes Neurais Artificiais (RNAs), a Regressão Logística (RL), as árvores de Decisão ou Decision Trees (DT), a Random Forest (RF), a Support Vector Machine (SVM) e a Naive Bayes (NB) são as técnicas mais utilizadas para este identificar se uma transação é fraudulenta ou não (RAUDHA; SAEEDI, 2019). Deep Learning (DL) e

XGboost (XG) aparecem com mais frequência, a partir do ano de 2020 aplicadas na identificação de fraudes em transações com cartões de créditos (THEJAS *et al.*, 2021).

Considera-se a aplicação da FC na avaliação do desempenho das técnicas inteligentes como um ponto de lacuna na literatura por ser pouco explorada. Seu uso leva em consideração a importante característica da justificativa financeira da adoção de um sistema que possibilite a detecção de fraudes.

Olowookere e Adewale (2020) indicam que boa parte dos artigos exploram métricas padrão para avaliação de técnicas inteligentes, como Precisão ou Taxa de Erro, mas dificilmente medem o impacto financeiro direto, que é o caso da aplicação da FC.

Considera-se então, justificável a aplicação da FC porque traz consigo a medição da efetividade do uso de uma técnica inteligente, tanto em ambiente de testes quanto na produção regular, podendo ser calculada em determinado período de tempo e comparada com o previsto, além de identificar a necessidade de uma recalibração ou reavaliação da técnica inteligente.

A contribuição reside na possibilidade de se aplicar a FC em conjunto com as métricas comumente utilizadas, com o intuito de avaliar o custo atrelado ao erro de uma detecção de fraude. Outro ponto relevante é que nem sempre a técnica com o melhor desempenho obtido nas métricas mais utilizadas é a que terá o melhor desempenho na FC. Este fato abre um precedente sobre como considerar qual técnica deverá ser adotada em um ambiente de produção nas organizações.

1.2 OBJETIVOS GERAL E ESPECÍFICO

O objetivo geral deste trabalho foi comparar o desempenho de técnicas inteligentes com base na avaliação da Função de Custo para detectar fraudes em transações com cartões de crédito em base de dados desbalanceada.

Os objetivos Específicos são:

- Realizar a análise exploratória dos dados da base selecionada;
- Utilizar os métodos de correção de desbalanceamento da base;
- Aplicar as técnicas inteligentes selecionadas na base de dados balanceada e desbalanceada;
- Aplicar as métricas MC, AUC, MCC e FC para avaliar os resultados.

1.3 DELIMITAÇÃO DO TEMA

A base de dados selecionada neste trabalho contém dados reais, apesar da possibilidade de utilização de transações geradas artificialmente. Esta base está disponível para download na internet e possui uma quantidade de instâncias e atributos que possibilitou realizar os experimentos com as técnicas selecionadas, além de conter dados relevantes como, o valor da transação e as fraudes identificadas.

As técnicas inteligentes aplicadas neste trabalho foram selecionadas com base nos resultados do levantamento bibliográfico realizado, que apontou como as mais utilizadas para detecção de fraudes com cartões de crédito: a Regressão Logística (RL), a *Decision Trees* (DT), a *Random Forest* (RF), a XGboost (XG), a *Deep Learning* (DL) e a *Support Vector Machine* (SVM).

Destaca-se que os resultados apresentados buscaram analisar o contexto contido nos registros que compõem a base de dados. Assim, não foi contemplada a utilização de históricos de uso ou isolar as transações por usuário. O treinamento das técnicas buscou a identificação de casos de fraudes pelo aprendizado de conhecimento da base como um todo.

Todos os resultados e análises estão diretamente ligados às características da base de dados, às versões das bibliotecas utilizadas e aos parâmetros utilizados nas técnicas inteligentes.

1.4 ESTRUTURA DO TRABALHO

Além do capítulo 1, este trabalho está estruturado da seguinte forma: o capítulo 2 contém a fundamentação teórica com detalhamento dos pontos principais abordados, o levantamento bibliográfico que sustenta as argumentações e bases da dissertação e a análise gráfica e dados que nortearam a busca pelos artigos selecionados. No capítulo 3 são apresentados os métodos e instrumentos de pesquisa utilizados e a estrutura adotada na realização dos experimentos computacionais. No capítulo 4, são apresentados e discutidos os resultados dos experimentos computacionais e no capítulo 5, apresenta-se a conclusão deste trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, apresenta-se a Fundamentação Teórica sobre Fraudes com Cartões de Crédito, Técnicas Inteligentes, Métricas de Desempenho, Função de Custo e por fim, o Levantamento Bibliográfico.

2.1 FRAUDES COM CARTÕES DE CRÉDITO

Fraude pode ser entendida como uma ação intencional com o objetivo de benefício próprio em detrimento de outra instituição ou indivíduo. Fraudes financeiras causam perdas de bilhões de dólares a cada ano e é um foco de atenção das instituições do mercado financeiro para prevenir e detectá-las (SINGH; JAIN, 2019).

Al-Hashedi e Magalingam (2021) indicam que as fraudes financeiras podem ser classificadas da seguinte maneira: fraudes corporativas, fraudes relacionadas a seguros, fraudes em criptomoedas e fraudes financeiras.

A fraude corporativa ocorre quando uma empresa forja os resultados financeiros em seus demonstrativos públicos. O objetivo é causar uma impressão melhor da empresa para que ela, seus acionistas ou seus gestores possam obter vantagens em obtenção de crédito, valorização indevida para uma venda ou atrair novos investidores (AL-HASHEDI; MAGALINGAM, 2021).

As fraudes relacionadas a seguros ocorrem quando fraudadores tentam se beneficiar de companhias de seguro, forjando acidentes, de forma a coletar o prêmio estabelecido em suas apólices (AL-HASHEDI; MAGALINGAM, 2021).

As fraudes em criptomoedas são consideradas mais recentes devido ao advento desta nova tecnologia e ao baixo nível de conhecimento de seu funcionamento pelo público geral. Assim os fraudadores se aproveitam para iludir indivíduos com falsas promessas de ganhos (GUPTA; LOHANI; MANCHANDA, 2021).

A falta de regulamentação e sua característica descentralizada de controle favorece o uso ilegal. Já as fraudes financeiras são as mais evidenciadas no Brasil, e se caracterizam pela lavagem de dinheiro e fraudes com cartões de crédito (AXUR, 2021).

O ambiente online também apresenta oportunidades para fraudadores, que se utilizam de e-mails para tentar coletar informações de cartões de crédito, por meio,

por exemplo, da prática de *phishing*, que consiste no uso de e-mails, solicitando informações pessoais, o que inclui dados de cartões de crédito. Estas mensagens normalmente oferecem grandes descontos em produtos cobiçados, às vezes até direcionando para sites clonados de lojas conhecidas (BASIT *et al.*, 2021).

Um comportamento semelhante também ocorre em aplicativos de mensagens diretas, como WhatsApp ou SMS, contendo atalhos para redirecionar o usuário aos sites clonados ou mesmo instalar programas maliciosos com o intuito de furto de dados.

Existem duas formas de utilizar cartões de crédito: o cartão de crédito físico e o cartão de crédito virtual ou online. Pode-se citar como vantagens na utilização de cartão de crédito físico: o fácil acesso ao crédito em estabelecimentos comerciais que não aceitam pagamentos online; a possibilidade de realizar compras sem precisar andar com dinheiro em espécie, diversas formas de autenticação e a possibilidade do cartão pode ser bloqueado em caso de perda ou roubo (CHIGADA, 2020).

Pode-se citar as desvantagens do cartão de crédito físico: o risco de fraudes, já que as informações do cartão físico podem ser facilmente clonadas. Além da questão da limitação da disponibilidade de estabelecimentos, já que só é possível utilizá-lo naqueles em que aceitam pagamentos com cartão de crédito (CHIGADA, 2020).

Levando em conta as vantagens de se portar um cartão de crédito virtual ou online: pode-se citar mais comodidade, já que pode ser utilizado em qualquer lugar com acesso à internet. A possibilidade de fazer um melhor controle sobre as compras e gastos, já que é possível gerar uma numeração específica para cada transação, além de acessar a fatura e o extrato do cartão a qualquer momento (THIRUPATHI; VINAYAGAMOORTHI; MATHIRAJ, 2019).

Entre as desvantagens do cartão de crédito virtual/online: destaca-se a dependência de uma conexão estável com a internet para realizar compras, risco de fraudes por meio de *phishing* e outras técnicas de engenharia social e a possibilidade de compras não autorizadas, caso os dados do cartão sejam vazados (TANOUZ *et al.*, 2021).

Ainda assim, a quantidade de transações válidas é muito superior à quantidade das ocorrências de fraudes, pela própria natureza do produto de compras presenciais

ou eletrônicas. Este desbalanceamento relativo à ocorrência de fraudes, de acordo com Jain (2019), dificulta consideravelmente a identificação de uma fraude.

O aumento da confiança nos pagamentos eletrônicos, o crescimento constante do comércio digital e o efeito da pandemia nas atividades comerciais são fatores que demonstram a necessidade e a efetividade de sistemas que identifiquem e coíbam fraudes (OLOWOOKERE; ADEWALE, 2020).

O interesse sobre as fraudes em cartões de crédito se faz pelas características de volume das operações, sua simultaneidade e a necessidade de se ter uma rápida resposta pois as operações são praticamente em tempo real. Sendo uma tarefa muito desafiadora do ponto de vista da tecnologia empregada (FOROUGH; MOMTAZI, 2021).

Os sistemas de detecção de fraudes já vêm utilizando a Inteligência Artificial, para identificar padrões de fraudes em transações de cartão de crédito ao longo dos anos, especialmente empregados por empresas de tecnologia chamadas de *FinTechs*, provendo plataformas e ferramentas impulsionadas pela IA (LI, Zhenchuan *et al.*, 2021).

2.2 TÉCNICAS INTELIGENTES

Na literatura, encontram-se diversos tipos de técnicas inteligentes para identificar fraudes. O desempenho delas depende, entre outros itens dos tipos de dados apresentados para o possibilitar o aprendizado (ABDALLAH; MAAROF; ZAINAL, 2016).

Segundo Al-Hashedi e Magalingam, (2021), as quatro técnicas para detecção de fraudes em cartões de crédito mais utilizadas, encontradas na literatura entre os anos de 2009 e 2019 foram: Support Vector Machine (SVM) ou Máquinas de Vetores de Suporte, as Redes Neurais Artificiais do tipo *Multilayer Perceptron*, a Regressão Logística e Naive Bayes.

Nos trabalhos recentes aparecem a aplicação de técnicas baseadas em Redes Neurais Recorrentes ou em inglês *Recurrent Neural Networks* (RNN) (BENCHAJI; DOUZI; EL OUAHIDI, 2021) e XGBoost (FOROUGH; MOMTAZI, 2021).

Gupta, Lohani e Manchanda (2021) indicam em seu trabalho o uso de Naive Bayes como técnica viável para detecção de fraudes financeiras para os casos de

bases desbalanceadas. A comparação foi feita com *Random Forest*, Regressão Logística e Árvores de Decisão para demonstrar a efetividade de Naive Bayes.

Liu, Gu e Shang (2020) utilizam uma *Deep Learning* (DL) não supervisionada para extração de padrões, para em seguida combinar este conhecimento extraído com o treinamento supervisionado e criar um modelo classificador híbrido. Este modelo atingiu o percentual de 100% para identificação de novas fraudes, porém considera-se um modelo de alta complexidade operativa.

A detecção de fraudes em cartões de crédito apresenta um problema de variação com o tempo, do termo inglês *concept drift*, isto ocorre quando uma característica se altera ao longo do período de uso. Este ponto implica em uma necessidade de retreinamento do modelo com as novas características dos dados, sugerido por Dornadula e Geetha (2019).

Uma outra abordagem é apresentar à técnica inteligente um conjunto de treinamento formado por uma sequência cronológica. Lucas et al. (2020) segmentaram a base de dados pelo estabelecimento do ponto de origem da compra, e um segundo conjunto isolando o usuário do cartão de crédito. Numa tentativa de gerar um padrão de comportamento para cada estabelecimento e para cada consumidor.

Os trabalhos descritos acima possuem uma complexidade no sentido de existir uma necessidade de identificar uma janela de tempo para executar um novo treinamento. Tanto para encontrar uma alteração normal de perfil de gastos de um cliente quanto identificar uma irregularidade nas transações do estabelecimento. Importante notar que estabelecimentos ou clientes novos não teriam um histórico, e tentativas válidas que sejam invalidadas ou tentativas de fraude que não são capturadas podem ocorrer com maior frequência.

Considerando que pela frequência, uma fraude equivale a uma anomalia, pode-se utilizar uma técnica não supervisionada para identificar os casos de fraudes. O uso de DL se mostra eficaz para este tipo de problema (LIU; GU; SHANG, 2020).

O desbalanceamento de classes em base de cartões de crédito pode ocorrer, devido ao número de instâncias fraudulentas ser menor do que o número de não fraudulentas. Para solucionar este problema, Ileberi, Sun e Wang (2021) utilizam o método de *Oversampling* em diferentes técnicas para a detecção de fraudes. Para comparação de desempenho das técnicas, foram adicionadas as técnicas de Decision

Trees, k-Nearest Neighbor (kNN), Regressão Logística, XGBoost, Random Forest e Nayve bayes. No mesmo sentido, Naveen e Diwan (2020) adicionam a técnica de Análise de Discriminação Quadrática, que é capaz de identificar variações entre variáveis dependentes para uma identificação mais clara dos limites entre classes.

Apresenta-se a seguir as características das técnicas inteligentes mais aplicadas na detecção de fraudes: Regressão Logística; Decision Trees; Randon Forest; Support Vector Machine; Deep Learning e XGboost (NEGI; DAS; BODH, 2022; TANOUZ et al., 2021; TRISANTO et al., 2020).

a) Regressão Logística

A Regressão Logística (RL) é uma técnica que se utiliza de um modelo linear que tenta segregar as classes no espaço de hipóteses, a fim de estimar uma regra para classificação, a partir dos atributos de entrada fornecidos. Esta regra fornece um valor de probabilidade para a instância pertencer ou não a uma determinada categoria (ALENZI; ALJEHANE, 2020).

O resultado será uma informação binária sobre a classe, sendo a instância pertencente ou não a uma determinada classe. Apesar do cálculo ser uma probabilidade de pertencer ou não a uma classe, a saída da técnica é efetivamente binária e não o valor resultante da probabilidade.

A Equação 1, que representa a RL é obtida a partir da equação da Regressão Linear, sendo y o valor da probabilidade da variável de categorização que pode assumir valores entre 0 e 1, a RL é representada como uma sigmoide dos valores de uma classe y contra a classe alternativa (1-y), a_0 o valor da intersecção da reta linear com o eixo x e a_n, n>0, os pesos associados a cada variável independente x.

$$log\left(\frac{y}{1-y}\right) = a_0 + a_1\, x_1 + a_2 x_2 + a_k x_k \qquad (1)$$

b) *Decision Tree*

A *Decision Tree* (DT) ou Árvore de Decisão é uma técnica representada por meio de uma função-alvo com valores discretos, que se utiliza de treinamento supervisionado para predizer uma classe alvo.

Com isso, um problema considerado composto é dividido em vários problemas menores e que são resolvidos de maneira recursiva (GAMA, 2004). Com conjunto de

algoritmos para o processamento de dados, DT traz consigo inferências para aplicação em múltiplas áreas, como na área médica, de avaliação de crédito por setores financeiros, sendo assim é possível inferir regras de fácil interpretação (MITCHELL, 1997).

c) *Random Forest*

A *Random Forest* (RF) se utiliza de várias árvores de decisão, combinando as suas saídas, após a randomização dos dados de treinamento (VADAKARA; KUMAR, 2019).

Para cada árvore de decisão utilizada, um conjunto de dados de probabilidade fixa é utilizado. Uma vez, utilizando-se de várias árvores de decisão, a quantidade de atributos da base de teste é distribuída entre as árvores. Ao final da construção de cada árvore, os dados são combinados por uma votação de maioria.

Boost e *Bagging* são variações de Random Forest, na aleatoriedade ou construção da distribuição das árvores. *Boost* utiliza probabilidade variável em função da dificuldade de classificação de um exemplo de teste. *Bagging* utiliza exemplos aleatórios na construção de seus exemplos, mantendo a distribuição de probabilidades uniforme (TRISANTO et al., 2021).

d) *Support Vector Machine*

A *Support Vector Machine* (SVM) ou Máquina de Vetores de Suporte é uma técnica cujo principal objetivo é encontrar um hiperplano ideal que separe, de forma mais eficiente, as diferentes classes de dados no espaço dimensional (NAVEEN; DIWAN, 2020).

Para isso, a SVM tenta maximizar a distância entre os pontos de dados mais próximos de diferentes classes (os chamados vetores de suporte). A SVM funciona transformando os dados de entrada em um espaço de alta dimensão por meio de uma função de mapeamento linear ou não linear, dependendo da estratégia adotada.

e) *Deep Learning*

A *Deep Learning* (DL) é uma técnica baseada em processamento não linear com funcionamento em camadas. Cada saída de camada alimenta uma nova camada e assim sucessivamente. O termo “aprendizagem profunda” identifica a técnica como

tendo um número de camadas ocultas, ou profundidade, maior do que as técnicas que utilizam redes neurais artificiais tradicionais (SHRESTHA; MAHMOOD, 2019).

No treinamento da DL, os dados segregados para o treinamento são apresentados ao conjunto de camadas de neurônios por diversas vezes. A cada passagem de dados pelos neurônios é dado o nome de época. (SHRESTHA; MAHMOOD, 2019)

A *Recurrent Neural Networks* (RNN) é um dos algoritmos mais eficazes em *Deep Learning* quando se está analisando sequências de transações, especialmente para identificar anomalias como, por exemplo, fraude em cartão de crédito. Isto se dá pela capacidade desta técnica conseguir utilizar as informações utilizadas em épocas já utilizadas pelo algoritmo (SHRESTHA; MAHMOOD, 2019).

No caso das transações com cartões de crédito, as ocorrências entram numa fila de verificação onde RNN poderá identificar a fraude dentro das demais operações, fazendo a classificação com mais precisão (BENCHAJI; DOUZI; EL OUAHIDI, 2021)

A RNN utiliza a saída de uma iteração anterior no próximo ciclo, em unidades ocultas. Isto cria uma memória que é mais bem aproveitada em séries temporais. Para detectar uma fraude, que é um evento diferente que ocorre esporadicamente, a técnica deve guardar as entradas preliminares para estabelecer um comparativo com as entradas atuais. Isto é primordial para que a técnica possa estabelecer uma correlação entre eventos ao longo do tempo (JURGOVSKY *et al.*, 2018).

f) XGBoost

XGboost é uma técnica que se mostra eficaz na identificação de fraudes. A técnica é baseada em *boosting* (VICTORIA PRISCILLA; PADMA PRABHA, 2020). Este é um procedimento iterativo que atribui pesos a cada instância de treinamento, em função da dificuldade do treinamento, criando modelos sequenciais.

No caso dos gradientes de *boosting* os valores residuais dos modelos pré-existentes são usados para gerar o próximo, capacitando o modelo para encontrar as instâncias de fraude. XGBoost ou *extreme gradiente boosting* utilizam este conceito. A XGBoost têm indicação de uso para bases desbalanceadas e uso em detecção de fraudes por tratar a questão de desbalanceamento de bases de forma nativa (THEJAS *et al.*, 2021)

2.3 MÉTRICAS DE DESEMPENHO

Os tipos de aprendizado ou treinamento das técnicas inteligentes podem ser: Supervisionado, Não Supervisionado ou por Reforço. O Aprendizado Supervisionado é o tipo de treinamento em que os dados apresentados são rotulados com a variável alvo, para realizar uma classificação. No caso do Aprendizado Não Supervisionado, os dados não precisam ser rotulados. O objetivo é gerar agrupamentos com base na similaridade de padrões (DAL POZZOLO *et al.*, 2014).

O Aprendizado por Reforço usa um mecanismo de tentativa e erro em vez de uma coleção de exemplos conhecidos como aprendizado supervisionado. Nesse mecanismo, cada tentativa resulta em recompensa ou penalidade. O objetivo é aumentar a recompensa acumulada ao longo do tempo e aprender a agir de formas que produzam melhores resultados (ZHININ-VERA *et al.*, 2020).

O resultado de um treinamento pode ser avaliado, por meio de métricas de desempenho. Elas são fundamentais para apoiar a tomada de decisão sobre qual técnica pode ser a mais eficaz para identificar fraudes (DAL POZZOLO *et al.*, 2014).

Ao analisar os resultados das técnicas aplicadas, pode-se utilizar as seguintes métricas: a Matriz de Confusão (MC); a Precisão, a Sensibilidade, a Recuperação, a Medida-F, o Coeficiente de Correlação De Matthew (MCC) e a Área Sob a Curva (AUC), calculada a partir da Curva Característica de Operação do Receptor ou *Receptor Operating Characteristic* (ROC).

Para cada aplicação, pode-se utilizar um certo parâmetro específico para avaliar o desempenho das técnicas inteligentes. No caso das fraudes em cartões de crédito, pode-se utilizar a Função de Custo (FC), que avalia em valores monetários o impacto dos erros previstos cometidos pelas técnicas na fase de treinamento. Hand et al. (2007) indicam que existe uma necessidade de se utilizar uma métrica específica que faça sentido para o objetivo do negócio, no caso a FC.

A seguir, apresenta-se as características principais da MC, MCC, AUC e a Função de Custo (FC):

a) Matriz de Confusão

É basicamente formada por uma tabela, onde os resultados da técnica de podem ser avaliados. Nas colunas são representados os valores previstos e nas linhas

os valores reais. O resultado de uma MC é a contagem das ocorrências verdadeiras e falsas realizadas pela técnica, em função do cruzamento das instâncias verdadeiras com as previstas.

Desta forma é possível determinar as taxas de Verdadeiros Positivos (VP), Falsos Negativos (FN), Verdadeiros Negativos (VN) e Falsos Positivos (FP), como pode ser visualizado na Figura 1 (HAND *et al.*, 2008).

Figura 1: Matriz de Confusão

		PREVISTO	
		Normal	Fraude
REAL	Normal	Verdadeiro Negativo (VN)	Falso Negativo (FN)
	Fraude	Falso Positivo (FP)	Verdadeiro Positivo (VP)

Fonte: adaptado de (HAND *et al.*, 2008).

Os valores de VP e VN são os casos em que a técnica acerta a previsão. No caso de FN e FP são os casos em que a técnica erra a previsão.

b) Coeficiente de Correlação de Matthew

Quando se trata de bases desbalanceadas, as instâncias consideradas positivas são predominantes, sendo que o valor calculado da precisão, que é o número de decisões corretas divido pelo total de decisões, sempre será alto, não sendo parâmetro para aplicação em fraudes.

O uso do Coeficiente de Correlação de Matthew ou em inglês *Matthew Correlation Coefficient* (MCC) é uma alternativa por utilizar todos os valores da MC de modo a contemplar a questão das classes de diferentes tamanhos. O cálculo do MCC é apresentado, conforme a Equação 2 (TRISANTO et al., 2020).

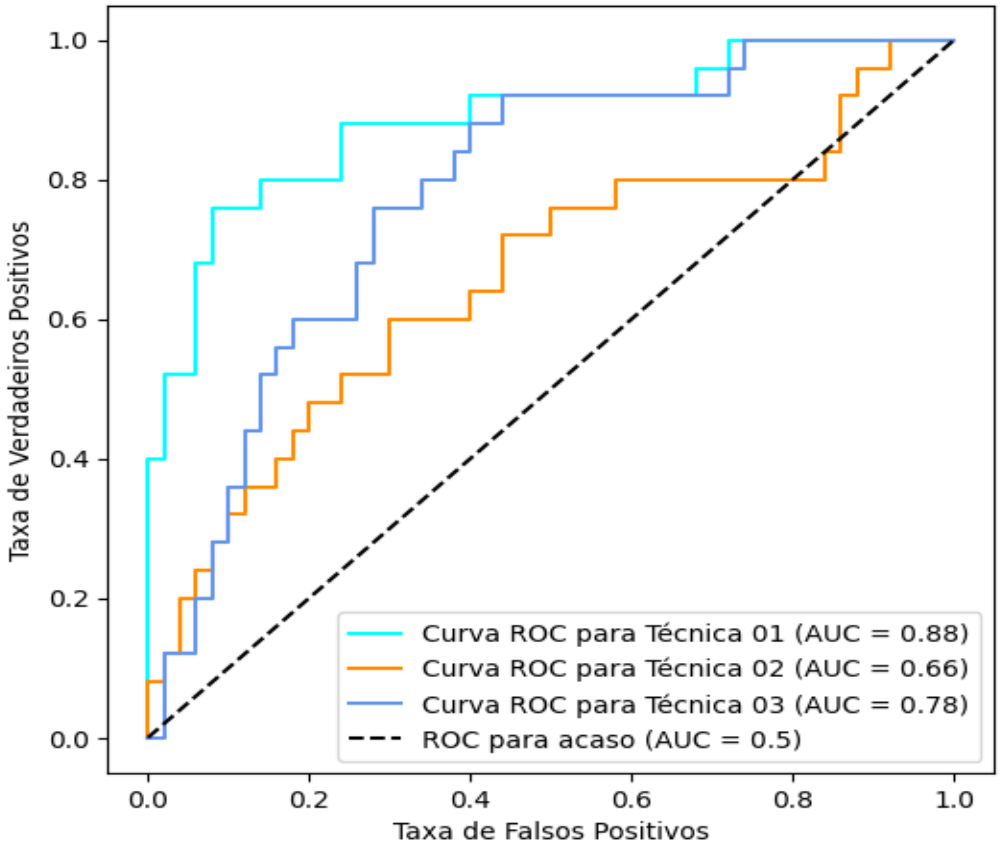
$$MCC = \frac{VP\ x\ VN - FP\ x\ FN}{\sqrt{(VP+FP)(VP+FN)(VN+FP)(VN+FN)}} \qquad (2)$$

c) Área sob a curva

A outra forma de medir o desempenho é a utilização do gráfico das Características de Operação do Receptor ou em inglês *Receptor Operating Characteristic* (ROC), que é a representação das taxas de FP versus VP, contribuindo para a visualização do desempenho da técnica (FANG; ZHANG; HUANG, 2019). Para uma visão numérica representativa do entendimento da ROC, utiliza-se a área calculada sob esta curva, em inglês *Area Under the Curve* (AUC) (FAYZRAKHMANOV; KULIKOV; REPP, 2018).

Apresenta-se, na Figura 2, um exemplo das curvas ROC e os valores das AUC para um experimento comparativo, aplicando três técnicas inteligentes identificadas como 01, 02 e 03.

Figura 2: Exemplo de curva ROC e AUC



Fonte: adaptado de FANG, ZHANG e HUANG (2019).

Pode-se verificar na Figura 2 o comportamento das curvas ROC para as três técnicas aplicadas. Os valores contidos na legenda, referem-se às AUC. O melhor

desempenho com AUC igual a 0,88 é para a Técnica 01 e o de pior desempenho para a Técnica 02 com AUC igual a 0,66 (FAYZRAKHMANOV; KULIKOV; REPP, 2018).

Figura 2 apresenta o desempenho de cada técnica frente à variação de falsos positivos e verdadeiros positivos, considera-se que uma reta entre os pontos (0,0) e (1,1) equivale à probabilidade de se jogar uma moeda, o resultado ser cara ou coroa, sendo a AUC igual a 0,5, identificada como ROC para o acaso. Valores acima e mais próximos de 1 sugerem que o classificador teve melhor desempenho para identificar fraudes.

d) Função de Custo

A Função de Custo (FC) estabelece uma relação entre as predições realizadas pela técnica com o valor da transação. A relação entre elas é representada em uma Matriz de Custo, conforme a Figura 3 (BAHNSEN *et al.*, 2013).

Figura 3: Matriz de Custo

		PREVISTO	
		Normal	Fraude
REAL	Normal	Nulo	Cadm
	Fraude	Ctrans	Nulo

Fonte: adaptado de Bahnsen et al. (2013).

A Matriz de Custo mostra que a previsão de uma transação normal para uma fraude incorre em um custo de transação (Ctrans), equivalente ao valor da transação. O valor previsto como fraude, mas para uma transação normal incorre em um custo administrativo (Cadm).

Nos quadrantes onde o resultado previsto é igual ao valor real, o custo é considerado como sendo nulo ou zero. Para os valores onde o resultado previsto é diferente do real, a tratativa deve ser diferente (BAHNSEN *et al.*, 2013).

No caso de um resultado previsto pela técnica ser uma transação fraudulenta para uma transação normal, considera-se que a técnica foi protetiva e irá causar custos administrativos para lidar com a reclamação do cliente.

No caso de uma previsão normal para uma transação que seja efetivamente uma fraude, o custo será considerado como equivalente ao valor de cada transação *i*, pois o pagamento ao lojista será efetuado, porém sem a contrapartida do detentor do cartão de crédito. Assim, FC pode ser definida conforme a Equação 3.

$$\mathrm{F}C = \sum_{i=1}^{m} y_i \left(p_i C_{adm} + (1 - p_i) C_{trans}\right) + (1 - y_i) p_i C_{adm} \quad (3)$$

A FC avalia o custo de *m* transações selecionando entre y_i e p_i, considerando respectivamente os valores reais e previstos ao assumir os valores 0 e 1. Em linhas gerais, os custos administrativos são bem inferiores (da ordem de 100 vezes menor) aos custos que incorrem com os erros de transação. Desta forma, opta-se por considerar somente o C_{trans}.

Assim, esta alteração na FC está apresentada na Equação 4 (HAND *et al.*, 2008).

$$FC = \sum_{i=1}^{m} y_i \left((1 - p_i) C_{trans}\right) \quad (4)$$

O resultado desta métrica busca quantificar o impacto financeiro causado pela classificação incorreta e, por se tratar de custo, quanto menor seu valor, melhor será o desempenho da técnica (KIM *et al.*, 2019).

2.4 BASES DE DADOS DESBALANCEADAS

Uma base de dados pode ser considerada desbalanceada quando a quantidade de ocorrências de uma classe é, significantemente superior a quantidade de outras classes (MROZEK; PANNEERSELVAM; BAGDASAR, 2020).

Técnicas inteligentes podem ter dificuldade na identificação de casos da classe minoritária, em função do pequeno número de exemplos de treinamento apresentados a ela. Neste caso, a técnica pode não encontrar uma solução ideal para identificar uma fraude quando um novo valor for apresentado (MROZEK; PANNEERSELVAM; BAGDASAR, 2020).

Para estes casos específicos, existem métodos que podem ser utilizados para tentar auxiliar a técnica inteligente a melhorar o desempenho na identificação da

classe minoritária. De maneira geral, o objetivo é fazer com que a classe minoritária seja, artificialmente, equiparada à classe majoritária. Pode-se citar a sobre-amostragem, denominada *Oversampling* e a sub-amostragem, denominada *Undersampling* (CHEN *et al.*, 2021).

O *Oversampling* diz respeito ao aumento artificial da classe minoritária, criando instâncias a partir das existentes, a fim de balancear as quantidades entre as classes. Ao final do processo, todas as classes majoritárias são mantidas, mas existe um risco de causar *Overfitting*, condição em que a técnica inteligente tem bom desempenho no treinamento, porém mau desempenho nos dados utilizados para teste (TRISANTO et al., 2020).

Como o *Oversampling* adiciona instâncias à base de dados de teste, o custo computacional também aumenta, já que a técnica terá que analisar uma maior quantidade de dados.

Existem várias possibilidades de aplicação do *Oversampling* para realizar o balanceamento da base de dados, os principais são o *Oversampling* randômico e o *Oversampling* sintético ou do inglês *Synthetic Minority Oversampling Technique* (SMOTE), e o *Oversampling* adaptativo ADASYN, do inglês *Adaptative Synthetic Sampling*, entre outros (TRISANTO et al., 2020).

No *Oversampling* randômico, aplica-se a duplicação das instâncias minoritárias aleatoriamente. O SMOTE cria exemplos minoritários pela interpolação das instâncias existentes, criando novas entradas e mantendo a classe minoritária intacta (LI, W., 2019).

O *Undersampling* trabalha no sentido oposto, realizando o balanceamento da base de dados, eliminando instâncias da classe majoritária. Uma vez que a base de dados é reduzida pelo ajuste do balanceamento, a necessidade de esforço computacional também é refletida, resultando num processamento em menor tempo durante a aplicação das técnicas inteligentes (TRISANTO et al., 2020).

A forma mais comum de *Undersampling* é a randômica em que as instâncias da classe majoritária são removidas artificialmente. Neste processo existe a possibilidade de se extrair instâncias com informações importantes para a detecção das classes, considerada como uma desvantagem do método (TRISANTO et al., 2020).

2.5 LEVANTAMENTO BIBLIOGRÁFICO

O levantamento bibliográfico foi realizado na base SCOPUS (www.scopus.com) e na base SCIENCE DIRECT (www.elsevier.com), pesquisando os seguintes termos em seus equivalentes em inglês: cartão de crédito (*credit card*), fraude (*fraud*), Aprendizado de Máquina (*Machine Learning*) e Inteligência Artificial (*Artificial Intelligence*). Concentrou-se a busca em artigos publicados entre o ano de 2016 até o mês de abril de 2023.

Apresenta-se na Figura 4 o filtro de busca aplicado às bases selecionadas para encontrar os artigos.

Figura 4: Filtro de busca aplicado às bases selecionadas

```
ABS ( credit AND card AND fraud AND ( ( machine AND learning )
 OR ( artificial AND intelligence ) ) ) AND ( LIMIT-
TO ( PUBSTAGE , "final" ) ) AND ( LIMIT-
TO ( DOCTYPE , "cp" ) OR LIMIT-TO ( DOCTYPE , "ar" ) OR LIMIT-
TO ( DOCTYPE , "cr" ) OR LIMIT-
TO ( DOCTYPE , "re" ) ) AND ( EXCLUDE ( SUBJAREA , "SOCI" ) OR E
XCLUDE ( SUBJAREA , "MEDI" ) OR EXCLUDE ( SUBJAREA , "ENVI" ) )
 AND ( LIMIT-TO ( PUBYEAR , 2023 ) OR LIMIT-
TO ( PUBYEAR , 2022 ) OR LIMIT-TO ( PUBYEAR , 2021 ) OR LIMIT-
TO ( PUBYEAR , 2020 ) OR LIMIT-TO ( PUBYEAR , 2019 ) OR LIMIT-
TO ( PUBYEAR , 2018 ) OR LIMIT-TO ( PUBYEAR , 2017 ) OR LIMIT-
TO ( PUBYEAR , 2016 ) ) AND ( LIMIT-TO ( LANGUAGE , "English" ) )
```

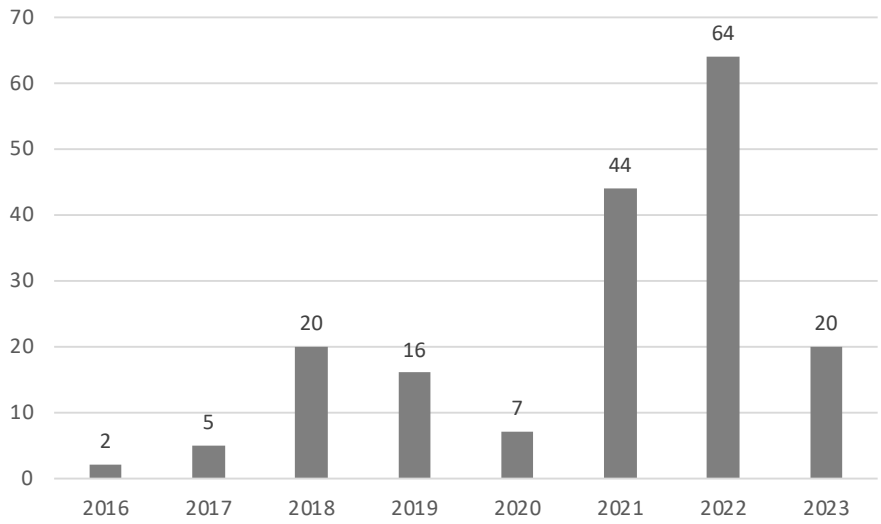
Fonte: o Autor.

O resultado da aplicação do filtro retornou 367 artigos nas áreas de computação, engenharia e finanças. Foram desconsiderados os artigos que citavam fraudes em cartões de crédito, mas o escopo do trabalho era voltado para outra área de estudo, como fraude, puramente financeira ou detecção de fraudes em seguros e concessão de crédito.

Após a remoção destes artigos fora do escopo deste estudo, foram selecionados os artigos entre o ano de 2016 até o mês de abril de 2023, resultando em 178 artigos para análise.

Apresenta-se na Figura 5 a distribuição dos 178 artigos selecionados por ano de publicação.

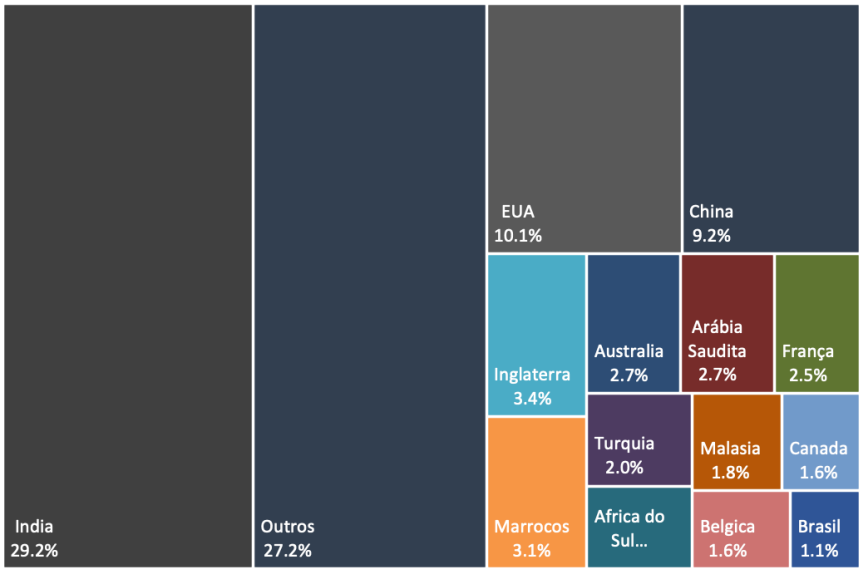
Figura 5: Distribuição de artigos por ano de publicação



Fonte: o Autor.

Pode-se verificar o aumento de frequência significativa de publicações, a partir de 2021, inclusive com 20 publicações contabilizadas até o mês de abril de 2023. Apresenta-se, na Figura 6 a distribuição de publicações por país de origem.

Figura 6: Distribuição de artigos por país de origem



Fonte: o Autor.

Verifica-se na Figura 6 que a Índia foi, significativamente o país com o maior número de publicações, seguida por Estados Unidos, China e Inglaterra. Pode-se considerar este ranking, devido a estas quatro nações investirem, pesadamente em *Big Data* e *Machine Learning*. Apenas 1,1% dos artigos foram identificados como realizados no Brasil.

Com relação aos termos centrais dos artigos relacionados, a ocorrência de cada termo pode ser verificada na nuvem de palavras apresentada na Figura 7. Destacam-se os seguintes termos de busca: detecção de fraudes (*fraud detection*), Aprendizado de máquina (*Machine Learning*), Fraudes em cartões de crédito (*credit card fraud*) e inteligência artificial (*Artificial Intelligence*). Na sequência identificou-se as técnicas mais utilizadas na detecção de fraudes: SVM, DL e DT.

Também, nota-se a questão do desbalanceamento de dados, representados pelos termos *class imbalance*, *imbalanced datasets*, SMOTE, *Oversampling*, *data imbalance*, *imbalanced classification* e *Undersampling*. Pela nuvem de palavras, pode-se notar uma menor ocorrência de XGBoost e principalmente da FC.

Figura 7: Nuvem de palavras-chave dos temas centrais

Fonte: o Autor.

No Quadro 1, estão listados os 16 artigos mais próximos ao tema deste trabalho.

Quadro 1: Lista de artigos próximos ao tema

Autores	**Título**	**Considerações**
Negi; Das; Bodh (2022)	*Credit Card Fraud Detection using Deep and Machine Learning (International Conference on Applied Artificial Intelligence and Computing)*	A utilização da mesma base de dados, da AUC e das técnicas RL e XGboost na detecção de fraudes em cartões de crédito.
Yuan (2022)	*A Transformer-based Model Integrated with Feature Selection for Credit Card Fraud Detection (ACM International Conference Proceeding Series)*	A aplicação da DL na detecção de fraudes em cartões de crédito sem comparação com outras técnicas.
Benchaji; Douzi e El Ouahidi (2021)	*Credit card fraud detection model based on LSTM recurrent neural networks (Journal of Advances in Information Technology)*	A aplicação da DL *Long Short-Term Memory* (LSTM) e da AUC na detecção de fraudes.
Asha e Suresh Kumar (2021)	*Credit card fraud detection using artificial neural network (Global Transitions Proceedings)*	Aplicou em comum uma SVM avaliada pelas seguintes métricas: precisão, acurácia e recall para detectar fraudes em cartões de crédito.
Al-Hashedi e Magalingam (2021)	*Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019 (Computer Science Review)*	Foi realizada uma revisão sistemática da literatura sobre o tema fraudes financeiras, que apoiou o levantamento bibliográfico realizado neste trabalho
Tanouz et al. (2021)	*Credit Card Fraud Detection Using Machine Learning (International Conference on Intelligent Computing and Control Systems)*	Utilizou a mesma base de dados para detecção de fraudes em cartões de crédito, aplicando DT, RF, RL e NB e para comparação de desempenho foram utilizadas a MC, F1 e AUC.
Forough e Momtazi (2021)	*Ensemble of deep sequential models for credit card fraud detection (Applied Soft Computing)*	Aplicou uma associação de técnicas em duas bases de dados, sendo a mesma utilizada neste trabalho e a outra base com dados brasileiros. Associou-se uma DL com um algoritmo baseado em votação. Os resultados apresentados foram avaliados segundo as seguintes métricas: precisão, recall, F1 e AUC.
Zhang et al. (2021)	*HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture (Information Sciences)*	Utilizou uma base de dados de fraudes de um banco chinês, aplicando *deep belief network* e redes convolucionais.
Li et al. (2021)	*A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection (Expert Systems with Applications)*	Abordou a questão das sobreposições das classes em bases desbalanceadas, avaliando o efeito dela em diversas técnicas de classificação aplicadas na base de dados utilizada neste trabalho.

Autores	Título	Considerações
Trisanto et al. (2020)	*Effectiveness Undersampling method and feature reduction in credit card fraud detection (International Journal of Intelligent Engineering and Systems)*	Propôs o uso de redução de dimensionalidade, associada a sub amostragem de dados para utilizar no treinamento das técnicas KNN, SVM, RL, Naive Bayes e RF. Usou como comparação de desempenho o MCC.
Liu, Gu e Shang (2020)	*Quantitative Detection of Financial Fraud Based on Deep Learning with Combination of E-Commerce Big Data (Complexity)*	Aplicou DL com diferentes abordagens. Desenvolveu um processo para gerar um modelo de classificação que envolveu o uso de treinamento não supervisionado na sequência de um supervisionado. Utilizou AUC para realizar comparações.
Lucas et al. (2020)	*Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs (Future Generation Computer Systems)*	Utilizou modelos cadeias de Markov, os autores executaram uma modelagem de dados de entrada separando em combinações com e sem fraude; por terminal e por cliente numa janela de tempo determinado.
Priscilla e Prabha (2020)	*Influence of Optimizing XGBoost to handle Class Imbalance in Credit Card Fraud Detection (International Conference on Smart Systems and Inventive Technology)*	Aplicou XGBoost em duas bases de dados. Realizou experimentos associados a diferentes métodos de amostragem e também a uma otimização do XGBoost.
HAND et al. (2007)	*Performance criteria for plastic card fraud detection tools (Journal of the Operational Research Society)*	Abordou com profundidade a forma como os resultados devem ser analisados. Introduziu a ideia da FC para comparação entre as técnicas aplicadas.
DAL POZZOLO et al. (2014)	*Learned lessons in credit card fraud detection from a practitioner perspective (Expert Systems with Applications)*	Utilizou a mesma base de dados de transações com cartões europeus. Destacou-se pela análise dos efeitos causados pelo desbalanceamento da base de dados. Estabeleceu que, ao invés de utilizar classificação pura, gerar um ranqueamento entre as transações e verificar qual deles consegue identificar uma fraude mais rapidamente. Concorda com Hand et al. (2007) na questão do uso da curva ROC, isoladamente na comparação da efetividade dos modelos, principalmente para este modelo de ranqueamento.

Autores	Título	Considerações
WHITROW et al. (2009)	*Transaction aggregation as a strategy for credit card fraud detection (Data Mining and Knowledge Discovery)*	Utilizou a FC como fator de comparação entre as técnicas aplicadas. Aplicou uma estratégia de agregação das transações por usuário e local de compra.

Fonte: o Autor.

Identifica-se no Quadro 1, que os artigos selecionados têm em comum com este trabalho, a detecção de fraudes em cartões de créditos, confirmando que o tema tratado é importante e atual.

Outro ponto em comum foi a aplicação de diversas técnicas inteligentes, das métricas utilizadas e em cinco artigos foi utilizada a mesma base de dados selecionada para este trabalho, o que indica a importância desta base.

Vale destacar que em somente três artigos foi aplicada a FC, na avaliação do desempenho de técnicas inteligentes, o que mostra que existe espaço para o desenvolvimento de pesquisas que abordem este tema e justifica a realização deste trabalho.

Os Materiais e Métodos utilizados neste trabalho são apresentados no próximo capítulo.

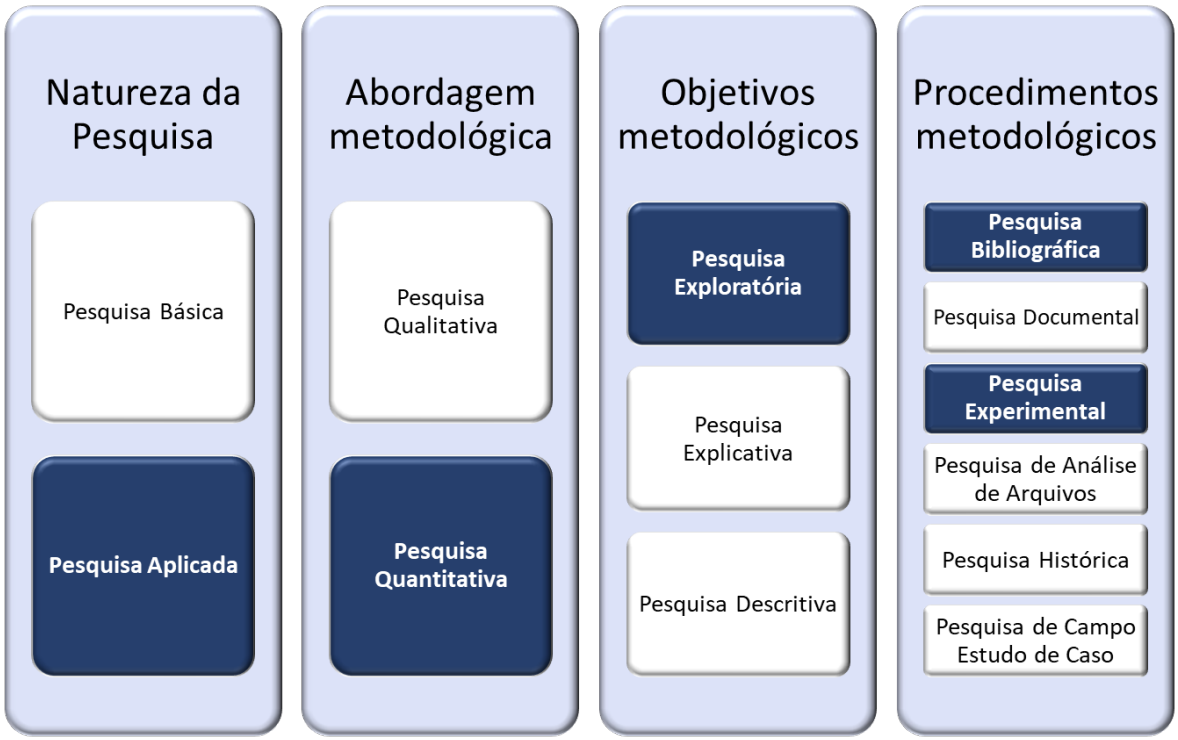
3 MATERIAIS E MÉTODOS

Neste capítulo, os materiais e métodos utilizados para desenvolvimento desta dissertação, a caracterização metodológica, a descrição dos experimentos computacionais, a base de dados e os softwares utilizados são apresentados.

3.1 CARACTERIZAÇÃO DA METODOLOGIA DE PESQUISA

Esta pesquisa se caracteriza por ser quantitativa e experimental, que procura avaliar o comportamento e desempenho de técnicas inteligentes para identificar a ocorrência de fraude em transações com de cartão de crédito. A Figura 8 apresenta a caracterização metodológica e os elementos destacados em azul escuro foram aplicados neste trabalho.

Figura 8: Caracterização metodológica



Fonte: O Autor.

3.2 PLATAFORMA DE ENSAIOS

Os experimentos foram desenvolvidos, utilizando a linguagem Python, com o uso das bibliotecas e as suas respectivas versões apresentadas no Quadro 2.

Quadro 2: Bibliotecas utilizadas nos ensaios

Biblioteca	**Finalidade**	**Versão**	**Url**
Python	Linguagem de programação, de código aberto interpretativo com aplicações diversas, incluindo Aprendizado de máquina.	3.9.5	https://www.python.org/
Numpy	Pacote para Python de computação científica que trabalha com vetores multidimensionais.	1.20.0	https://numpy.org/install/
Pandas	Pacote para Python de manipulação de dados em formato de tabela de dados.	1.2.4	https://pandas.pydata.org/pandas-docs/stable/getting_started/install.html
Scikit Learn	Pacote para Python para diferentes análises preditivas de dados	0.22.1	https://scikit-learn.org/stable/install.html#
TensorFlow	Pacote para Python, construído para uso em aplicações de aprendizado de máquina,	2.6.0	https://tensorflow.org
Keras	Pacote para Python, baseado em TensorFlow para uso em análises de DL	2.4.0	https://github.com/keras-team/keras
Imbalanced learn	Pacote para Python que possibilita a utilização de *Undersampling* e *Oversampling*	0.9.1	https://imbalanced-learn.org/stable/

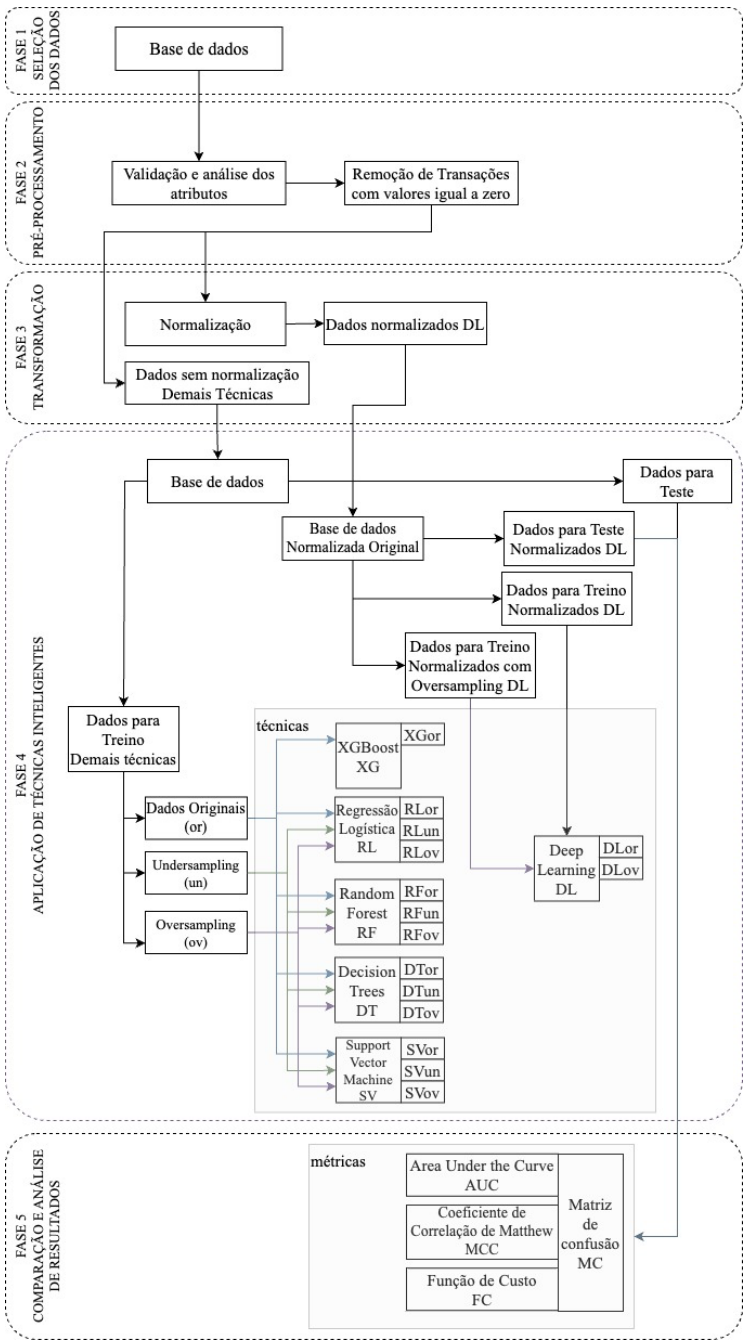
Fonte: o Autor.

O *hardware* utilizado para rodar os programas desenvolvidos foi um PC plataforma Intel core-i7, sexta geração, memória de 16GB, HD 1TB e placa de vídeo independente com 2GB.

3.3 FASES DE DESENVOLVIMENTO DOS EXPERIMENTOS

Apresenta-se na Figura 9, as cinco fases de desenvolvimento dos experimentos computacionais.

Figura 9: Fases de desenvolvimento dos experimentos computacionais



Fonte: o Autor.

Descreve-se a seguir as etapas de desenvolvimento dos experimentos computacionais.

Fase 1: Seleção dos dados

A seleção de dados é a fase em que se define as fontes de informação a serem utilizadas. Os dados podem se encontrar em forma bruta, não estruturada ou

estruturada, com valores alocados a colunas que descrevem a informação coletada. Os dados de interesse devem estar disponíveis para utilização na próxima etapa.

Buscou-se uma base de dados do mundo real com transações de cartões de crédito, que apresentasse variedade de atributos e proporcionasse uma quantidade suficiente de transações para separar em dois subconjuntos de dados, um de treinamento e o outro de teste.

Pela quantidade de transações e pela característica de desbalanceamento com relação a fraudes, a base de dados deve apresentar quantidade suficiente de amostras para exemplificar fraudes.

Assim, a base de dados utilizada na realização dos experimentos computacionais é uma base do mundo real, contendo transações com cartões de crédito europeus, coletadas entre os anos de 2013, com 31 atributos e 282.982 registros (DAL POZZOLO *et al.*, 2014).

A base foi coletada e disponibilizada pelo *Machine Learn Group da Universitè Libre de Bruxelles* no seguinte endereço eletrônico: (https://www.kaggle.com/mlg-ulb/creditcardfraud).

Os atributos identificáveis são: hora da transação, representados como valores numéricos sequencial em segundos, relativo à primeira transação, totalizando uma amostra de 2 dias contínuos; valor da transação em euros; e o atributo classe indicando se a transação é fraude ou normal.

Os demais atributos são resultantes da redução de dimensionalidade, após a aplicação da técnica, denominada PCA do inglês *Principal Component Analysis* (MADHAV; KUMARI, 2020), os atributos foram reduzidos para 28, mantendo as informações dos clientes protegidas, impossibilitando qualquer identificação, mas mantendo a importância e relevância dos atributos. Não foi mencionada a quantidade total de atributos que passaram pela redução de dimensionalidade.

Fase 2: Pré-processamento

Nesta fase os dados contidos na base selecionada passaram pela análise exploratória, com o intuito do entendimento das informações e preparação para as demais fases.

Nesta fase é verificada a existência de valor nulo nas instâncias. Esta validação é importante para que a técnica não considere dados inválidos na determinação de

fraude ou não-fraude. Também se executa a análise exploratória dos dados, a fim de se certificar que os dados totais da base sejam consistentes ao longo dos experimentos.

Fase 3: Transformação

A transformação inclui as tarefas de extração, transformação e carregamento em base de dados. Também podem ser realizadas tarefas de redução e agrupamento de dimensões. Tais tarefas devem ser realizadas de acordo com a técnica que será utilizada, já que cada uma tem sua especificidade. Os dados transformados devem estar em formato utilizável e de fácil acesso para uso das técnicas na próxima fase.

Nesta etapa os dados podem ser normalizados, ou seja, alteram-se os valores de absolutos para relativos, já que algumas técnicas necessitam deste tipo de transformação para utilização correta de seu algoritmo.

Tipicamente pode-se aplicar normalização dos dados, transformação de valores simbólicos para numéricos, ou redução de dimensionalidade da base de dados.

Foi aplicada a normalização nos 28 atributos anonimizados para aplicar a DL, para adequar à necessidade de implementação da técnica, de acordo com a biblioteca de programação utilizada.

Fase 4: Aplicação de técnicas inteligentes

Tanto a base normalizada utilizada para a aplicação de DL quanto a base de dados originais utilizada para a aplicação das demais técnicas foram divididas em dois subconjuntos de dados para treinamento e para teste.

Nesta fase as seguintes técnicas foram aplicadas: Deep Learning (DL), XGboost (XG), Regressão Logística (RL), Decision Trees (DT), Random Forest (RF) e Support Vector Machine (SVM).

A base de dados foi separada de forma aleatória em 2 grupos, mantendo a proporcionalidade entre as ocorrências da classe alvo:

- Dados para treinamento: este subconjunto de dados foi utilizado para que a técnica reconheça padrões dentro da base e gere um modelo, que seja posteriormente utilizado para classificação de novas instâncias de dados.

- Dados para teste: este subconjunto de dados foi utilizado para aferir os resultados do modelo construído a partir dos dados de treinamento

Na sequência foi realizado o ajuste das amostras de treinamento, executado nos casos em que a base de dados utilizada apresente desproporcionalidade significativa entre classes da variável alvo. Foram aplicados os métodos de *Oversampling* e *Undersampling* para as técnicas de RL, DT, RF e SVM.

Estes métodos não foram aplicados para a XG porque o algoritmo que a suporta faz o tratamento intrínseco para bases que apresentam desbalanceamento. No caso da DL apenas o *Oversampling* foi aplicado, já que o *Undersampling* não faria sentido porque a DL necessita de um grande número de instâncias de treinamento.

Na sequência, os dados de treinamento foram aplicados nas técnicas selecionadas. De forma geral, um modelo é gerado para cada combinação de base de treinamento para cada técnica inteligente aplicada, segundo foi apresentado na Figura 9, Fase 4: amostragem original (or), amostragem por *Undersampling* (un) e amostragem por *Oversampling* (ov).

Fase 5: Comparação e análise de resultados

É nesta fase que se validou o desempenho das técnicas utilizadas, pela análise dos resultados obtidos após a aplicação da base de testes para cada modelo gerado no passo anterior, e comparando as métricas de desempenho das técnicas inteligentes para identificarem uma fraude.

Para a comparação das técnicas foram geradas Matrizes de Confusão (MC) e, a partir dos resultados obtidos, as seguintes métricas foram calculadas: AUC, MCC e FC.

A AUC é calculada sobre a curva da característica de operação do receptor, *Receiver Operating Characteristic* (ROC) que basicamente cruza a taxa de verdadeiros positivos contra a taxa de falsos positivos (FANG; ZHANG; HUANG, 2019).

A área sob a curva ROC, *Area Under the Curve* (AUC) é amplamente utilizada como uma métrica de desempenho global do modelo, sendo valores próximos de 1 indicativos de um bom desempenho (FAYZRAKHMANOV; KULIKOV; REPP, 2018).

A base de cálculo da AUC é a MC, que permite avaliar o desempenho de um modelo de classificação. Ela apresenta a quantidade de exemplos de treinamento que

o modelo classificou corretamente, ou seja, verdadeiros positivos e verdadeiros negativos versus a quantidade de exemplos classificados incorretamente, falsos positivos e falsos negativos (FAYZRAKHMANOV; KULIKOV; REPP, 2018)

O Coeficiente de Correlação de Matthews (MCC) é uma métrica de desempenho usada para avaliar técnicas inteligentes na tarefa de classificação. A MCC mede a correlação entre as previsões do modelo e as classes verdadeiras, variando de -1 a 1 (TRISANTO et al., 2020).

Valores próximos de 1 indicam correlação positiva forte entre as previsões e as classes verdadeiras, o que significa que o modelo está fazendo previsões precisas. Valores próximos de -1 indicam correlação negativa forte, o que significa que o modelo está fazendo previsões erradas, e valores próximos de 0 indicam falta de correlação, o que significa que o modelo não está fazendo previsões confiáveis.

A MCC tem a capacidade de equilibrar a precisão e o *recall*, tornando-a uma métrica robusta aplicada em problemas de classificação com bases desbalanceadas. O MCC também é inferido a partir dos resultados da MC.

A Função de Custo (FC), refere-se ao custo de erro de classificação, Equação 4. A FC é calculada pela taxa de falsos positivos da MC multiplicada pelo custo da transação que foi considerada como não fraude, mas na realidade é uma fraude.

Esta é uma métrica que se conecta com as regras de negócio das empresas, e traduz o desempenho da técnica inteligente para uma linguagem comum aos tomadores de decisão, o custo de uma predição errônea (WHITROW *et al.*, 2009).

Para comparar os desempenhos da aplicação das técnicas inteligentes selecionadas com base nos resultados da AUC, MCC e FC, gerou-se um *ranking* baseado nos resultados obtidos individualmente.

A estratégia de decisão para selecionar a técnica mais adequada para a tarefa de identificação de fraudes tomou como base o critério de desempenho FC com a MCC e AUC, servindo de parâmetro para comparação final.

Os resultados dos experimentos computacionais e a discussão são apresentados no próximo capítulo.

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Neste capítulo, os resultados dos experimentos computacionais são apresentados e discutidos.

4.1 FASES DE DESENVOLVIMENTO DOS EXPERIMENTOS COMPUTACIONAIS

O desenvolvimento dos experimentos computacionais segue as fases apresentadas na Figura 9, que são:

a) Fase 1: Seleção dos dados;

b) Fase 2: Pré-processamento;

c) Fase 3: Transformação;

d) Fase 4: Aplicação de técnicas inteligentes;

e) Fase 5: Comparação e análise de resultados.

a) Fase 1: Seleção dos dados

O descritivo da base de dados com os valores máximos e mínimos e a contagem de valores não nulos para cada atributo existente, obtidos por meio da análise exploratória de dados é apresentado no Quadro 3.

Quadro 3: Descritivo da base de dados

atributo	descrição	qtd instâncias	min	max
Time	hora da transação	284807	0	172792
Amount	valor da transação	284807	0	25,691.16
Class	Classe Fraude(1)	284807	0	1
V1	valores anonimizados e normalizados	284807	-56.41	2.45
V2		284807	-72.72	22.06
V3		284807	-48.33	9.38
V4		284807	-5.68	16.88
V5		284807	-113.74	34.80
V6		284807	-26.16	73.30
V7		284807	-43.56	120.59
V8		284807	-73.22	20.01
V9		284807	-13.43	15.59
V10		284807	-24.59	23.75
V11		284807	-4.80	12.02
V12		284807	-18.68	7.85
V13		284807	-5.79	7.13
V14		284807	-19.21	10.53
V15		284807	-4.50	8.88
V16		284807	-14.13	17.32
V17		284807	-25.16	9.25
V18		284807	-9.50	5.04
V19		284807	-7.21	5.59
V20		284807	-54.50	39.42
V21		284807	-34.83	27.20
V22		284807	-10.93	10.50
V23		284807	-44.81	22.53
V24		284807	-2.84	4.58
V25		284807	-10.30	7.52
V26		284807	-2.60	3.52
V27		284807	-22.57	31.61
V28		284807	-15.43	33.85

Fonte: o Autor.

A técnica PCA foi aplicada nos atributos V1 a V28 para serem disponibilizados publicamente e apresentaram valores não nulos em todas as instâncias. O atributo *Time* contém a hora da transação em segundos, a partir da primeira transação existente na base, ou seja, cada transação real foi apresentada na ordem de sua execução.

Os valores das transações (*Amount*) variaram de 0 a € 25.691,16. O atributo *Class* contém informação binária da transação, na qual a transação de não fraude apresenta valor igual a zero, e no caso de fraude valor igual a um.

Apresenta-se no Quadro 4 uma amostra com cinco instâncias, consideradas como exemplo da base de dados utilizada.

Quadro 4: Amostra de instâncias da base de dados

Instância	Time	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10
620	471	1.377497	-0.662565	-0.130149	-0.56268	-0.832895	-0.910754	-0.327043	-0.201709	-0.523053	0.606911
621	472	-1.10092	1.029588	1.348333	-1.362082	-0.343465	-0.671659	0.291222	0.379994	0.338839	-0.438421
622	472	1.017055	-0.185049	1.181666	1.07349	-0.550586	0.971827	-0.806452	0.484792	0.517268	-0.060124
623	472	-3.043541	-3.157307	1.088463	2.288644	1.359805	-1.064823	0.325574	-0.067794	-0.270953	-0.838587
624	472	1.040781	0.109569	0.357987	1.118998	-0.105373	-0.056837	0.055026	0.045165	-0.350573	0.151602
Instância	**Time**	**V11**	**V12**	**V13**	**V14**	**V15**	**V16**	**V17**	**V18**	**V19**	**V20**
620	471	-1.054682	-1.360771	-1.342496	0.068812	-0.045774	0.700457	0.573051	-1.365161	0.94765	0.04262
621	472	-0.51177	-0.547061	-1.245946	0.263624	0.901413	0.382383	-0.267488	-0.649734	-1.067109	0.002147
622	472	1.44699	1.198013	-0.070891	0.006577	0.432215	-0.149873	-0.090841	-0.195277	-0.870041	-0.164293
623	472	-0.414575	-0.503141	0.676502	-1.692029	2.000635	0.66678	0.599717	1.725321	0.283345	2.102339
624	472	1.576598	1.181847	0.390602	0.476672	0.445941	0.039947	-0.469182	-0.066496	-0.564016	-0.020911
Instância	**Time**	**V21**	**V22**	**V23**	**V24**	**V25**	**V26**	**V27**	**V28**	**Amount**	**Class**
620	471	0.133023	0.287921	-0.224325	0.052896	0.775265	-0.042445	-0.026107	0.003801	48	0
621	472	-0.110388	-0.180427	-0.007197	0.068877	-0.41054	0.731643	0.084051	-0.057236	0.92	0
622	472	0.239287	0.875848	-0.053458	-0.269918	0.328907	-0.217332	0.096208	0.020796	17.57	0
623	472	0.661696	0.435477	1.375966	-0.293803	0.279798	-0.145362	-0.252773	0.035764	529	1
624	472	0.188378	0.487631	-0.147081	0.036691	0.565457	-0.275489	0.023386	0.019021	59.88	0

Fonte: O Autor.

Para facilitar a visualização, as colunas Instância e *Time* foram reproduzidas à esquerda no empilhamento de cada rótulo.

b) Fase 2: Pré-processamento

Os dados da base selecionada passaram por análise exploratória para o entendimento das informações e preparação para as demais fases.

Os atributos da base de dados foram divididos em 2 grupos para melhor entendimento de sua estrutura:

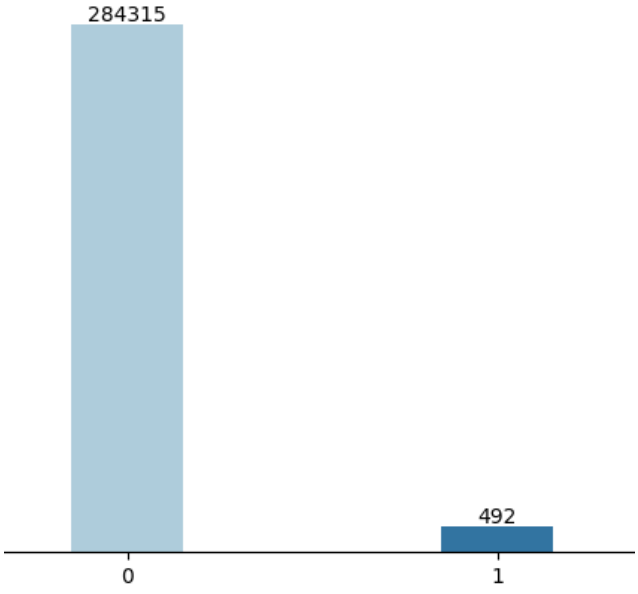
a. Atributos conhecidos: *Time* (hora relativa com relação à primeira transação da base), *Amount* (valor de cada transação) e *Class* (informação se a transação é ou não fraude).

b. Atributos V1 a V28 anonimizados: Os valores destes atributos foram anonimizados para evitar a exposição das informações dos usuários detentores do cartão de crédito, podendo conter dados de natureza sensível como o saldo bancário.

Todos os atributos continham valores para todas as instâncias. Assim, segundo este critério, todas as instâncias estão aptas para serem utilizadas.

Foi realizada a análise da distribuição de classes ou da ou variável alvo (*Class*), que identifica fraudes para os atributos conhecidos. Encontrou-se desproporcionalidade de 0,17% na ocorrência de fraudes em comparação com as transações de não fraude. Como pode ser visualizado no gráfico da Figura 10 esta desproporcionalidade caracteriza o desbalanceamento da base de dados para a classe alvo.

Figura 10: Distribuição de classes



Fonte: o Autor.

Pode-se verificar na Figura 10 o desbalanceamento representado em números. A classe que representa as fraudes contém 492 instâncias e a classe que representa não fraudes contém 284.315 instâncias. Estes números refletem a dificuldade de uma técnica inteligente em identificar as fraudes, o que justifica a utilização de *Oversampling* e *Undersampling*.

Outro atributo analisado foi o valor da operação, cujo valor médio é de €88,39, e a distribuição por faixa de valores apresentada na Tabela 1. As ocorrências mais frequentes, com 79,518% dos casos, estão na faixa entre €0,01 até €100,00.

Tabela 1: Distribuição de valores de transações por faixa de valor

Valor da transação	**Quantidade de instâncias**	**% das instâncias**
€0	1.825	0,641%
De €0,01 a €100,00	226.474	79,518%
De €100,01 a €200,00	27.671	9,716%
De €200,01 a €1.000,00	25.897	9,083%
De €1.001,01 a €5.000,00	2.885	1,013%
De €5.000,01 a €10.000,00	48	0,017%
De €10.001,01 a €25.692,00	7	0.002%
Total de instâncias	**284.807**	**100%**

Fonte: o Autor.

Aplicando a mesma segmentação de distribuições da Tabela 1 e selecionando apenas as transações marcadas como fraude, chega-se à distribuição de transações da Tabela 2. Para este caso, os valores percentuais da faixa de €0,01 até €100,00 também é o mais frequente com ocorrência de 68,089% dos casos. Portanto, as fraudes seguem a tendência encontrada no total das transações.

Tabela 2: Distribuição de transações fraudulentas por faixa de valor

Valor da transação	**Quantidade de instâncias**	**% das instâncias**
€0,00	27	5,488%
De €0,01 a €100,00	362	68,089%
De €100,01 a €200,00	76	15,477%
De €200,01 a €1.000,00	45	9,146%
De €1.000,01 a €5.000,00	9	1,829%
De €5.000,01 a €10.000,00	0	0%
De €10.000,01 a €25.692,00	0	0%
Total de instâncias	**492**	**100%**

Fonte: o Autor.

Para este atributo também foi calculado o valor total de todas as transações, que resulta em € 25.162.590,01, sendo os valores relativos a fraudes no montante de € 60.127,97 ou 0.24% do total.

Pela análise das Tabelas 1 e 2, foi verificada a existência de valores iguais a zero nas transações. Do ponto de vista prático, como regra de negócio, não faz sentido a existência de tais transações. Desta forma, para evitar um viés que possa interferir na aplicação das técnicas inteligentes em encontrar uma fraude, estas instâncias foram eliminadas da base.

Após a remoção das 1.825 instâncias com valores de transação igual a zero, a nova distribuição da variável alvo que caracteriza fraudes contém 465 instâncias, o que representa 0,164% do total da base de 282.982 instâncias.

Nesta base não foram identificados valores nulos ou faltantes para os atributos conhecidos ou anonimizados. Não houve a necessidade de tratamento com relação a estes pontos. A análise exploratória confirmou o desbalanceamento das classes e, que não houve nenhum impedimento no uso da base para a aplicação das técnicas inteligentes selecionadas.

c) Fase 3: Transformação

Das técnicas inteligentes selecionadas e aplicadas, somente a base de dados processada pela DL foi normalizada, devido à sua natureza computacional, requerida pela implementação do modelo em ambiente de produção.

Foi aplicada a padronização da base de treinamento utilizando a biblioteca *Standard Scaler* disponibilizada no *scikit learn* (https://scikit-learn.org). Com esta biblioteca, aplicou-se o método da distância de cada ponto para a média divididas pelo desvio-padrão.

Não houve a necessidade de conversão de valores textuais para numéricos porque as instâncias estão no formato numérico. A redução de dimensionalidade não foi aplicada neste trabalho, a fim de manter todas as características nativas dos atributos anonimizados, já que base de dados original coletada do site sofreu redução com a técnica PCA. Uma vez que não se sabe o que eles contêm, uma nova redução de dimensionalidade poderia remover informações importantes para a detecção de fraudes.

d) Fase 4: Aplicação das técnicas inteligentes

Nesta fase, a base de dados foi dividida em 2 subconjuntos: um para teste e outro para treinamento da técnica inteligente. Para obter uma divisão otimizada foram feitos testes para determinar esta proporção.

Foi utilizada a DT para definir esta divisão dos subconjuntos baseada em dois motivos: por ser o algoritmo base para duas técnicas que serão comparadas: a RF e a XG, e por figurar entre as três técnicas mais utilizadas para detecção de fraudes em cartões de crédito, segundo Al-Hashedi e Magalingam (2021).

Para dividir os dados foi utilizada a função da biblioteca *scikit learn* denominada train_test_split, que gera os subconjuntos de teste e treinamento, preservando a proporcionalidade das classes da base original.

O teste consistiu em se variar o percentual da base de treinamento de 30% a 90%, com incrementos de 10% a cada nova aplicação. Os resultados foram obtidos e os valores de AUC e MCC calculados para comparação.

Apresenta-se no Quadro 5 os resultados obtidos nos testes, prev 0 e prev 1 são resultantes da previsão de não fraude e fraude, respectivamente, sendo os valores real 0 e real 1 os valores de não fraude e fraude existentes na base de dados utilizada.

Quadro 5: Resultados da determinação de tamanho de base de treinamento

% da base treinamento	MC			AUC	MCC
		prev 0	prev 1		
30%	real 0	197641	121	0.88773	0.724079
	real 1	73	253		
40%	real 0	169414	97	0.897563	0.743694
	real 1	57	222		
50%	real 0	141192	66	0.858135	0.71627
	real 1	66	167		
60%	real 0	112968	39	0.835848	0.715263
	real 1	61	125		
70%	real 0	84714	41	0.860472	0.715858
	real 1	39	101		
80%	real 0	56471	33	0.897557	0.741367
	real 1	19	74		
90%	real 0	28238	14	0.893369	0.7553
	real 1	10	37		

Fonte: o Autor.

Por esta avaliação os melhores casos foram a base de treinamento com 40% (AUC de 0,897563 a MCC 0,743694) e com 80% (AUC de 0,897557 e MCC de 0,741367) do total de instâncias. Foi selecionada a proporção de 40% para a base de

treinamento para manter um maior número de transações de fraude na base de teste para avaliar o desempenho das técnicas.

Desta forma, 40% do número de instâncias foi separado para treinamento e 60% reservado para uso nos testes. A base de treinamento resultante possui 113.006 instâncias de transações não fraudulentas e 186 instâncias de fraude. A base de testes ficou com 169.511 instancias de não fraude e 279 de fraude.

Uma vez definida a base de treinamento, mais dois subconjuntos de dados foram gerados: um sendo oriundo da aplicação de *Undersampling*, removendo instâncias da classe majoritária e o outro proveniente da aplicação de *Oversampling*, adicionando instâncias à classe minoritária. Para esta tarefa foi utilizada a biblioteca *imbalanced learn*.

Com a finalidade de se definir qual a proporção ideal da correção de desproporcionalidade entre as classes, a mesma estratégia de variar os percentuais e calcular o AUC e MCC para comparação foi aplicada à técnica de DT.

Tanto para o *Undersampling* como para o *Oversampling* iniciou-se a proporcionalidade entre as classes em 20% até 90%, em incrementos de 10% a cada teste.

Para o *Undersampling* pelo ajuste nas proporções citadas acima, temos como resultado o Quadro 6.

Quadro 6: Resultados da determinação de proporcionalidade para *Undersampling*

% undersampling	MC			AUC	MCC
		prev 0	prev 1		
20%	real 0	163886	5625	0.9206841	0.1865468
	real 1	35	244		
30%	real 0	164607	4904	0.9192266	0.1980943
	real 1	37	242		
40%	real 0	161372	8139	0.9204371	0.1571712
	real 1	31	248		
50%	real 0	161625	7886	0.9122228	0.1564018
	real 1	36	243		
60%	real 0	159592	9919	0.9187709	0.1429629
	real 1	29	250		
70%	real 0	155870	1364	0.9131686	0.1221032
	real 1	2	25		
80%	real 0	153017	1649	0.901169	0.1089949
	real 1	2	25		
90%	real 0	152067	1744	0.900159	0.1060889
	real 1	2	25		

Fonte: o Autor.

Como proporção de melhor desempenho termos de AUC e MCC, foi observado para a proporcionalidade em 20% (AUC de 0,9206841 e MCC de 0,1865468). Desta forma, a base de treinamento final com *Undersampling* ficou com a seguinte distribuição: 906 instâncias não-fraude e 186 instâncias de fraude.

Para *Oversampling*, apresenta-se no Quadro 7 os resultados que mostram que tanto os percentuais de 30% quanto de 50% tiveram os melhores resultados para AUC (0,8672035 e 0,8689897) e MCC (0,7521103 e 0,7515493) respectivamente.

Foi adotado o percentual de 30% pela questão de efetividade na rapidez de processamento, já que ficamos com uma base de treinamento menor que a de 50%. Desta forma, a base de treinamento com *Oversampling* ficou com uma distribuição de 113.006 instâncias com transações não-fraude e 33.901 instâncias de fraude.

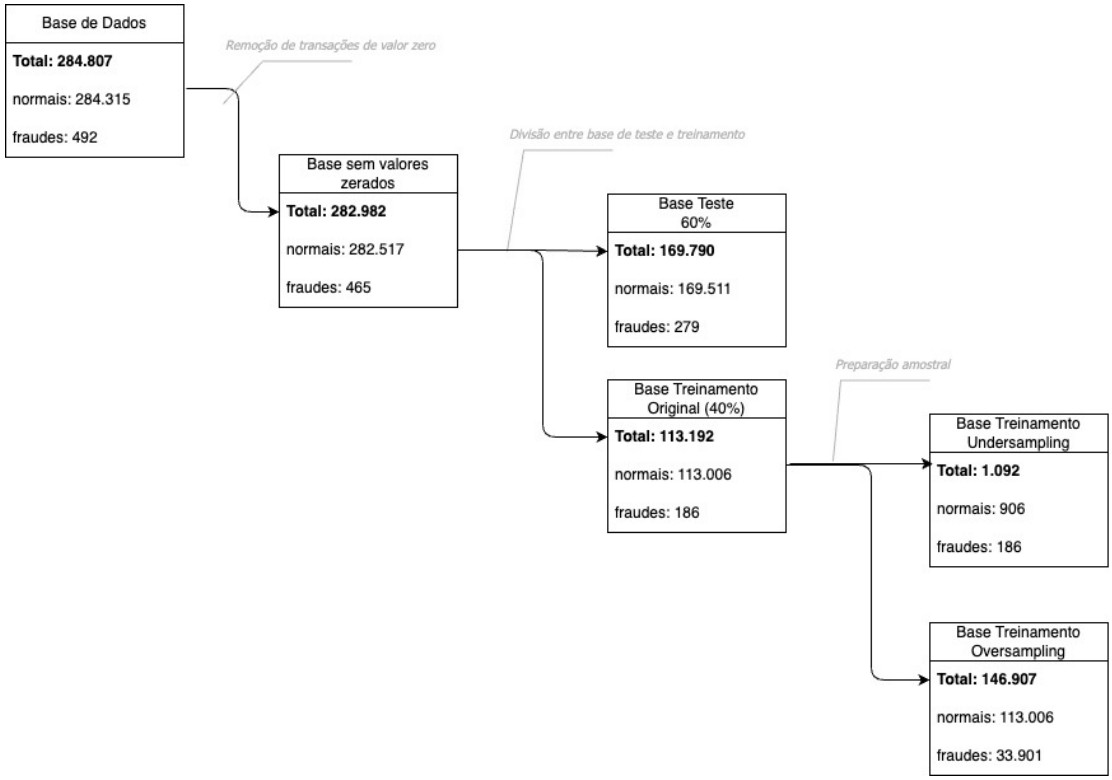
Quadro 7: Resultados da determinação de proporcionalidade para *Oversampling*

% oversampling	MC			AUC	MCC
		prev 0	prev 1		
20%	real 0	169444	67	0.8582253	0.7323477
	real 1	79	200		
30%	real 0	169450	61	0.8672035	0.7521103
	real 1	74	205		
40%	real 0	169437	74	0.8653731	0.7320571
	real 1	75	204		
50%	real 0	169448	63	0.8689897	0.7515493
	real 1	73	206		
60%	real 0	169445	66	0.854644	0.7291276
	real 1	81	198		
70%	real 0	169445	66	0.854644	0.7291276
	real 1	81	198		
80%	real 0	169443	68	0.8564302	0.7286779
	real 1	80	199		
90%	real 0	169446	65	0.8600233	0.7374036
	real 1	78	201		

Fonte: o Autor.

A Figura 11 traz o resumo das alterações na base de dados até a formação das bases de treinamento e testes utilizadas nas próximas etapas.

Figura 11: Transformações aplicadas à base de dados



Fonte: o Autor.

Apresenta-se na Tabela 3 as Informações consolidadas da base de dados, resultantes do pré-processamento e da aplicação dos métodos de *Undersampling* e *Oversampling*.

Tabela 3: Identificação das bases de treinamento para as técnicas inteligentes

	Base de dados original	Base de dados original sem valores zerados	Base de treinamento original pré-processada	Base de dados de treinamento com *Undersampling*	Base de treinamento com O*versampling*
Número de atributos	31	31	31	31	31
Número de instâncias	284.807	282.982	113.192	906	146.907
Número de fraudes	492	465	186	186	33.901
Percentual de fraudes	0,17%	0,16%	0.16%	20,5%	23,1%
Técnica**s** aplicadas	-	-	DL, XG, RL, DT, RF, SVM	RL, DT, RF, SVM	RL, DL, DT, RF, SVM

Fonte: o Autor.

Apresenta-se na Tabela 4 as configurações utilizadas em cada técnica inteligente selecionada.

Tabela 4: Identificação das técnicas inteligentes utilizadas

Técnica inteligente	Descrição
Deep Learning	DL foi configurada para uma camada de entrada com 30 neurônios, um para cada atributo da base, seguida por 3 camadas invisíveis e uma de saída. As camadas invisíveis possuem 512, 256 e 32 neurônios cada e a camada de saída contém apenas um neurônio (KEWEI *et al.*, 2021). A técnica foi implantada na biblioteca keras que possibilita uma escolha aleatória de um percentual de neurônios para ser ignorado em cada iteração do modelo, este valor foi ajustado para 30%. Este parâmetro auxilia para que a técnica não crie um viés relativo aos dados de treinamento. Foram realizadas 7 iterações ou épocas, otimizador Adam, taxa de aprendizado 0,0001 e tamanho de lote 2048. Os dados de treinamento separados para a aplicação da técnica de DL passaram pela normalização
XGboost	XG foi aplicada utilizando 1000 estimadores, sem árvores paralelas e com *booster* do tipo *gbtree*, que utiliza uma composição de árvores de decisão no modelo. O objetivo escolhido foi regressão linear, para o caso de variável alvo ser binária. Como métrica de avaliação intrínseca do modelo foi escolhida a taxa de erro de classificação binária. É informado à técnica a escala de desbalanceamento da base de 0.16%. Para a tarefa de treinamento, o subconjunto de dados apresentado à técnica não passou pela normalização por não haver uma necessidade explícita para utilização dos dados neste formato.
Regressão Logística	A RL escolhida foi a do tipo linear, máximo de 100 iterações, tolerância de 0,0001.
Árvores de Decisão	Para classificação utilizando DT foi utilizado o critério de variância *gini.*
Random Forest	RF foi configurada com 20 estimadores, também utilizando critério de variância *gini.*
Máquina de Vetores de Suporte	SV foi configurada para utilizar kernel tipo Linear.

Fonte: o Autor.

Apresenta-se, na Tabela 5 as abreviaturas dos modelos gerados com base nas técnicas inteligentes selecionadas, bem como as bases de dados utilizadas para realizar o treinamento.

Tabela 5: Identificação das técnicas inteligentes aplicadas

Identificação	Técnica	Base de dados
DLor	*Deep Learning*	Base de teste original
XGor	*XGboost*	
RLor	*Regressão Logística*	
DTor	*Decision Trees*	
RFor	*Random Forest*	
SVor	*Support Vector Machine*	
RLun	*Regressão Logística*	Base de teste com *Undersampling*
DTun	*Decision Trees*	
RFun	*Random Forest*	
SVun	*Support Vector Machine*	
RLov	*Regressão Logística*	Base de teste com O*versampling*
DTov	*Decision Trees*	
RFov	*Random Forest*	
SVov	*Support Vector Machine*	
DLov	*Deep Learning*	

Fonte: o Autor.

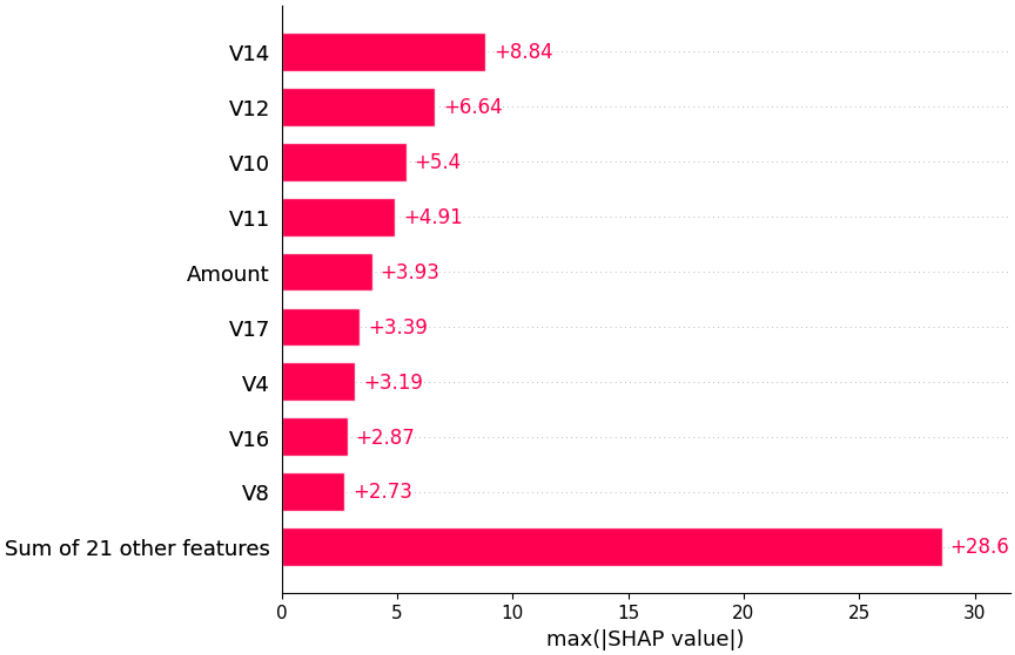
Pode-se observar na Tabela 5 que foram gerados 15 modelos com base nas técnicas inteligentes aplicadas, considerando a base de dados original, com a aplicação de *Oversampling* e de *Undersampling*.

Fase 5: Comparação e análise de resultados

No processo de detecção de fraude na base de dados, cada técnica durante o processo de treinamento elenca os atributos que são determinantes na decisão de ser ou não uma fraude.

Todas as técnicas consideraram os mesmos atributos como sendo mais importantes para a definição dos modelos. A Figura 12 mostra a influência do impacto de cada atributo no resultado final, neste exemplo para a Regressão Logística.

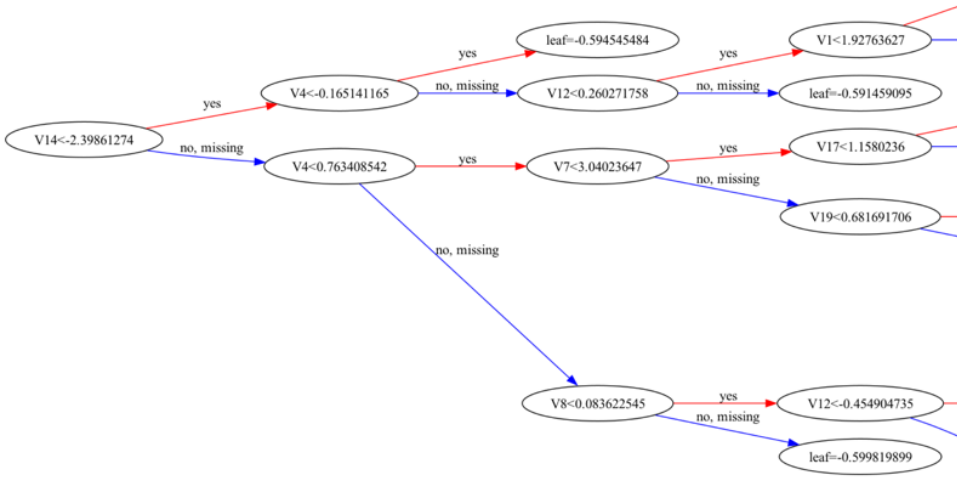
Figura 12: importância de cada atributo na formação do modelo RL



Fonte: o Autor.

Para o modelo da RL o atributo mais importante foi V14. A Figura 13 mostra os primeiros galhos da árvore de decisão formada pela XGboost, também utilizada como exemplo em que V14 é o mais importante para a definição do primeiro galho.

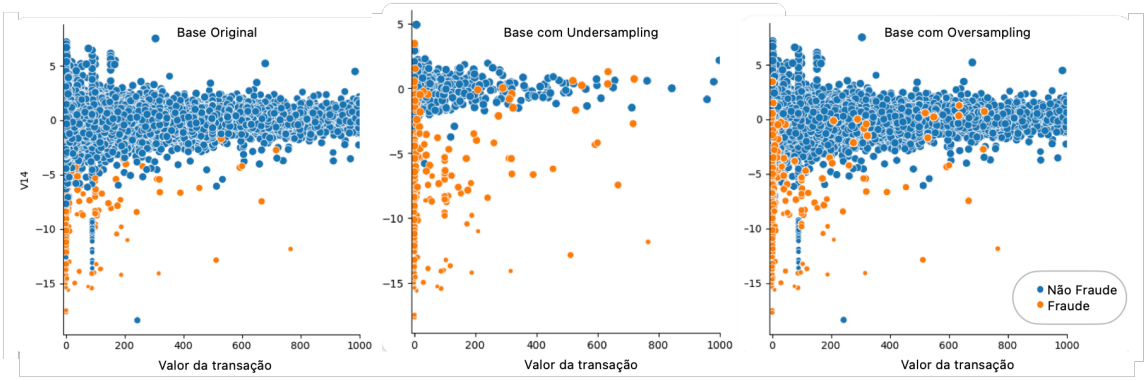
Figura 13: Início da árvore de decisão pela XGboost



Fonte: o Autor.

Tomando V14 como atributo de importância podemos traçar a distribuição de fraudes deste atributo em função do valor para a base de treinamento original, a Figura 14 mostra o gráfico resultante.

Figura 14: Gráfico Fraudes por V14 por valor de transação para cada base



Fonte: o Autor.

Os pontos azuis são as ocorrências de não fraude, os pontos laranjas representam as ocorrências de fraudes. Apesar da baixa incidência frente ao total, para os valores menores a identificação de fraude é mais clara frente às de valores maiores.

Para as amostragens de *Undersampling* e *Oversampling*, os valores de fraude ficam mais evidentes, possibilitando um melhor desempenho na classificação do que na base original de treinamento. O efeito das técnicas de amostragem *Undersampling* e *Oversampling* têm por objetivo deixar mais evidente as ocorrências das fraudes.

Para aferir os resultados das classificações foram geradas MC para cada modelo apresentado na Tabela 5. A MC é base para a análise de resultados, apresentando o desempenho de cada técnica na detecção de fraudes.

4.2 ANÁLISE DE RESULTADOS DAS MÉTRICAS AUC E MCC

O Quadro 8 mostra os resultados obtidos para a MC, AUC e, MCC, após a aplicação das técnicas na base teste.

Quadro 8: Resultados obtidos para a MC, MCC e AUC

Técnica	MC			AUC	MCC
		prev 0	prev 1		
DLor	real 0	169508	3	0.741927	0.687695
	real 1	144	135		
XGor	real 0	169470	41	0.899521	0.821391
	real 1	56	223		
RLor	real 0	169483	28	0.775903	0.683013
	real 1	125	154		
DTor	real 0	169422	89	0.833071	0.670961
	real 1	93	186		
RFor	real 0	169498	13	0.874514	0.839557
	real 1	70	209		
SVor	real 0	169477	34	0.654022	0.469483
	real 1	193	86		
RLun	real 0	168256	1255	0.935366	0.376887
	real 1	34	245		
DTun	real 0	164425	5086	0.904353	0.188015
	real 1	45	234		
RFun	real 0	169013	498	0.928639	0.527818
	real 1	39	240		
SVun	real 0	168643	868	0.818228	0.329294
	real 1	100	179		
RLov	real 0	168118	1393	0.938543	0.363223
	real 1	32	247		
DTov	real 0	169421	90	0.815147	0.645487
	real 1	103	176		
RFov	real 0	169496	15	0.872716	0.833653
	real 1	71	208		
SVov	real 0	169126	385	0.884169	0.524434
	real 1	64	215		
DLov	real 0	165488	4023	0.920033	0.217457
	real 1	38	241		

Fonte: o Autor.

A análise dos resultados foi dividida em:

a) Técnicas inteligentes aplicadas à base de dados original;
b) Técnicas inteligentes aplicadas à base de dados com *Undersampling* e;
c) Técnicas inteligentes aplicadas à base de dados com *Oversampling*.

a) Análise dos resultados das técnicas inteligentes aplicadas à base de dados original

A análise do Quadro 7, considerando AUC, mostra que XGor teve o melhor desempenho com valor de 0,899521. Esta técnica apresenta um tratamento nativo

para o desbalanceamento de classes, o que trouxe vantagem em seu desempenho. RFor ficou em segunda lugar com 0,872716, seguida pela DTor com 0,833071.

Vale ressaltar, que DLor é altamente dependente de uma grande quantidade de exemplos de treinamento. Para a classe de transações não fraude, o desempenho foi bom, apresentando apenas 3 FN, porém, para a classe minoritária, que apresenta pequeno número de exemplos, o desempenho foi abaixo, identificando apenas 48% dos casos.

O desempenho em MCC leva em consideração não apenas a proporção de acertos e erros, mas também como os resultados são distribuídos em todas as categorias.

Desta forma, pode ser utilizado em situações de bases desbalanceadas. Os melhores desempenhos para esta métrica foram: em primeiro lugar a RFor com 0,839557, seguida da RFov com 0,833653; XGor com 0,821391 e DLor com 0,687695.

As duas técnicas que se destacaram nestas duas métricas aplicadas na base de dados original foram a XGor e a RFor, ambas, utilizando árvores de decisão como base para seus algoritmos. XGor apresentou o melhor desempenho para AUC e o terceiro lugar para MCC. Já, RFor apresentou o melhor desempenho para MCC e o segundo melhor desempenho para AUC.

b) Análise dos resultados das técnicas inteligentes aplicadas à base de dados com *Undersampling*

Para AUC os melhores desempenhos foram da RLun com 0,935366, seguida pela RFun com 0,928639 e pela DTun com 0,904353. O uso de balanceamento nas bases de treinamento pode prejudicar o resultado da MCC, já que a generalização é extrema, apesar de auxiliar na detecção de fraudes, porém traz um aumento, principalmente nos FN, o que prejudica o cálculo do MCC.

Desta forma, os melhores desempenhos para MCC ficaram exatamente para as aplicações das técnicas nas bases originais (item a, desta subseção), porém considerando os resultados com *Undersampling*, os melhores desempenhos foram: a RFun com 0,527818, a RLun com 0,376887 e a SVun com 0,329294.

Assim, o melhor desempenho, considerando AUC ficou para a RLun, sendo a segunda melhor em MCC e o melhor desempenho para MCC ficou com RFun, sendo a segunda para AUC.

c) Análise dos resultados das técnicas inteligentes aplicadas à base de dados com *Oversampling*

De forma geral, as técnicas aplicadas na base de dados com *Oversampling* apresentaram desempenhos próximos ou superiores quando comparadas com os desempenhos da base de dados original, mas com desempenho inferior quando aplicadas à base de dados com *Undersampling*, com exceção da técnica RLov.

No caso da DL, o uso da base de treinamento com *Oversampling* melhorou a capacidade de detecção de fraudes. Como já discutido, esta técnica é dependente do aumento dos exemplos apresentados como fraude, contribuindo para a melhora da métrica AUC. Notou-se, porém, que houve o aparecimento de FNs e consequente diminuição do MCC.

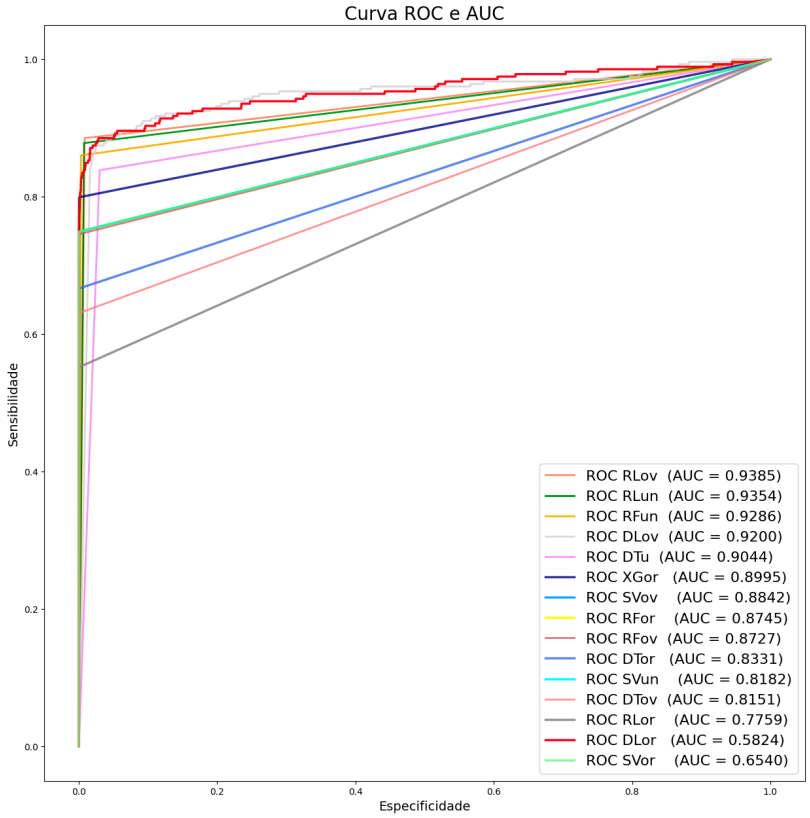
Dentre as técnicas aplicadas na base de dados com *Oversampling*, as que apresentaram os melhores desempenhos para AUC foram: a RLov com 0,938543, seguia pela DLov com 0,920033 e pela SVov com 0,884169. Com relação ao desempenho para MCC, tem-se seguinte classificação: em primeiro a RFov com 0,833653, seguida pela DTov com 0,645487 e pela Vov 0,524434.

Considera-se, então, com base na análise dos resultados dos experimentos computacionais, que a RLov teve o melhor desempenho para AUC e foi a quarta em MCC, a RFov teve o melhor desempenho para MCC, ficando em quarto lugar para a AUC.

Apresenta-se na Figura 15 os resultados da curva ROC e da AUC para cada técnica inteligente aplicada.

A Regressão Logística (RL), de forma geral, ao ser aplicada à base de dados original e às bases de dados desbalanceadas, respondeu bem quando o desbalanceamento das classes foi reduzido com *Undersampling* e *Oversampling*, como pode-se verificar as curvas ROC e os valores de AUC, que colocaram a RL, ocupando as duas primeiras posições.

Figura 15: Resultados da curva ROC/AUC para cada técnica



Fonte: o Autor.

A RLov consegue identificar as fraudes reais, ainda que, apresentando uma quantidade expressiva de FN frente às demais, mas que é relativamente baixa percentualmente no total de transações (0,8%).

Os resultados mostram que para a AUC o melhor desempenho ficou para a RLov, sendo a décima segunda para MCC. Já, a melhor para MCC foi a RFor, sendo a oitava para AUC.

4.3 ANÁLISE DE RESULTADOS DA MÉTRICA FC

Compara-se e analisa-se, a seguir os resultados obtidos com as métricas AUC e MCC com o resultado obtido com a aplicação da FC. FC considera para cada FP o valor da transação como penalizador da pontuação. Portanto, quanto maior o valor, pior o desempenho. Os valores variam de 0 a 100, sendo o valor percentual da soma dos valores de todas as transações FP dividido pelo valor total possível das transações de fraude.

Apresenta-se, no Quadro 9 os valores da MC de cada técnica aplicada e a comparação dos resultados da AUC, do MCC com os resultados obtidos no cálculo da FC.

Quadro 9: Resultados obtidos para a MC, AUC, MCC e FC

Técnica	MC			AUC	MCC	FC
		prev 0	prev 1			
DLor	real 0	169508	3	0.741927	0.687695	66.76
	real 1	144	135			
XGor	real 0	169470	41	0.899521	0.821391	22.05
	real 1	56	223			
RLor	real 0	169483	28	0.775903	0.683013	54.97
	real 1	125	154			
DTor	real 0	169422	89	0.833071	0.670961	38.20
	real 1	93	186			
RFor	real 0	169498	13	0.874514	0.839557	27.99
	real 1	70	209			
SVor	real 0	169477	34	0.654022	0.469483	76.94
	real 1	193	86			
RLun	real 0	168256	1255	0.935366	0.376887	11.41
	real 1	34	245			
DTun	real 0	164425	5086	0.904353	0.188015	17.80
	real 1	45	234			
RFun	real 0	169013	498	0.928639	0.527818	17.98
	real 1	39	240			
SVun	real 0	168643	868	0.818228	0.329294	37.42
	real 1	100	179			
RLov	real 0	168118	1393	0.938543	0.363223	9.97
	real 1	32	247			
DTov	real 0	169421	90	0.815147	0.645487	53.90
	real 1	103	176			
RFov	real 0	169496	15	0.872716	0.833653	34.49
	real 1	71	208			
SVov	real 0	169126	385	0.884169	0.524434	22.13
	real 1	64	215			
DLov	real 0	165488	4023	0.920033	0.217457	13.71
	real 1	38	241			

Fonte: o Autor.

FC é uma métrica que deriva da MC, porém agrega outras informações não disponíveis nela, já que, deve-se calcular o peso para cada FP. Para a FC, a técnica que apresentou o melhor desempenho foi a RLov com FC=9,97, seguida pela RLun com FC=11,41, DLov com FC=13,71, DTun com 17,80, RFun com 17,98 e XGor com FC=22,05.

Com base na Figura 14, RL conseguiu não apenas identificar uma maior quantidade de casos de fraude, como também encontrar mais casos de maiores valores de transação.

Apresenta-se, no Quadro 10 a diferença entre a FC e a taxa de FP para cada técnica inteligente aplicada. O intuito desta análise é mostrar a taxa de erros percentual comparado com a relação FC para o total possível de fraudes, apresentando a diferença percentual entre os dois valores.

Quadro 10: Comparativo de desempenho da FC e Taxa de FP

Técnica	FC	TX FP	DIFERENÇA
RLov	9.973	11.470	1.497
RLun	11.413	12.186	0.774
DLov	13.710	13.620	-0.090
DTun	17.797	16.129	-1.667
RFun	17.983	13.978	-4.005
XGor	22.050	20.072	-1.979
SVov	22.130	22.939	0.809
RFor	27.985	25.090	-2.896
RFov	34.493	25.448	-9.045
SVun	37.421	35.842	-1.578
DTor	38.200	33.333	-4.867
DTov	53.902	36.918	-16.985
RLor	54.968	44.803	-10.165
DLor	66.757	51.613	-15.144
SVor	76.939	69.176	-7.763

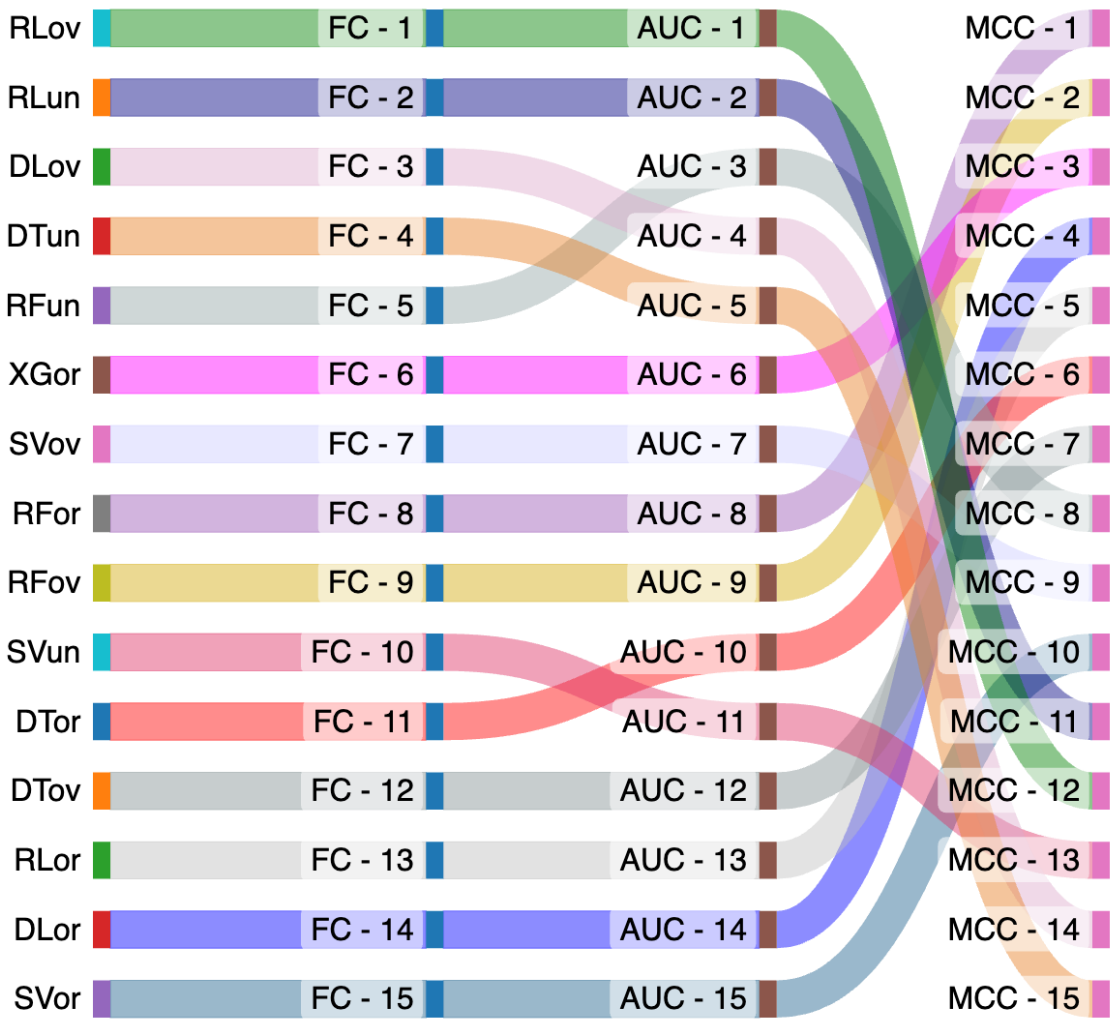
Fonte: o Autor.

Comparando as técnicas DLov foi a que resultou em menor diferença absoluta entre FC e TX FP abaixo de 1%, e DTov com a maior diferença absoluta entre estes parâmetros, na faixa dos 17%.

A Figura 16 mostra o comparativo entre os desempenhos das técnicas em cada métrica, tomando-se como base a métrica FC. De maneira geral, não há uma ligação

direta entre as métricas, FC apresenta alguma semelhança com os resultados da AUC mas nada que seja conclusivo.

Figura 16: Desempenho de cada métrica



Fonte: o Autor.

Não há garantias de que AUC ou MCC sejam totalmente alinhadas com FC, pois a diferença primordial entre elas não reside apenas nos resultados da CM, mas sim na análise qualitativa dos erros das técnicas, como explorado no Quadro 10.

Lembrando que a análise de FC considera que o custo de um FN não é significativo, mas a ocorrência de FN prejudica muito o cálculo de MCC, evidenciado pela diferença entre estas duas métricas.

Pode-se considerar como um dos motivos que levaram a RLov a ter o melhor desempenho para a FC, dentre todas as técnicas aplicadas neste trabalho foi porque

os erros de detecção ocorreram em uma faixa, onde os valores não prejudicaram a sua efetividade.

Deve-se considerar também, que a RL é tradicionalmente aplicada em problemas de detecção de fraudes e, que o modelo apresentou aderência à base de dados utilizada, haja visto que a mesma RL, também teve o melhor desempenho para AUC.

Apesar de técnicas inteligentes robustas e com alta capacidade de processamento, como a DLor que não apresentou bom desempenho, pode-se concluir que necessitam de maior número de exemplos para realizar o treinamento. Esta conclusão é confirmada quando se utiliza DLov, com o aumento do número de casos de fraudes na base de treinamento a efetividade do modelo é evidenciada tanto por AUC quanto por FC.

Numa situação real de ambiente de produção de uma operadora de crédito, certamente o uso da técnica RLov traria benefícios para o negócio, pela capacidade de identificação das fraudes, por ser uma técnica que não demanda um grande esforço computacional, tanto na operação quanto frente a uma necessidade de retreinamento da técnica. A FC para este caso, mostra que, aproximadamente 90% dos valores monetários resultantes de fraudes seriam barrados pela técnica.

Mesmo ainda, olhando para a questão do fraco desempenho em MCC, causado pelo número de FN, a taxa é baixa, inferior a 1%, o que não traria impactos significativos às empresas, como por exemplo as reclamações de cartões não sendo autorizados por suspeita de fraude.

5 CONCLUSÃO

Os desafios para detectar fraudes em meio ao excessivo volume de transações que ocorrem requer bom desempenho por parte de uma técnica inteligente. Para isto, aplicar métricas de comparação é uma atividade relevante e com resultados práticos.

Cada tipo de métrica aplicada pode levar à escolha de uma determinada técnica inteligente. Todas têm sua validade, mas a base correta para tomada de decisão deve levar em conta a finalidade principal da utilização desta técnica. Em outras palavras, o impacto nas métricas é o que vai indicar a melhor técnica a ser utilizada.

Levando-se em consideração o componente de aplicação prática, as empresas se interessam pela viabilidade da implantação de ferramentas de tecnologia. Além de apurar os custos de implantação, manutenção e operação da tecnologia, um fator preponderante é o custo evitado.

O uso da FC se mostra um caminho para a tomada de decisão nas empresas sobre as técnicas que serão utilizadas. Ela apresenta um comparativo entre a capacidade de identificação da fraude e o impacto financeiro provável de sua utilização.

O melhor desempenho da RLov reflete os parágrafos acima, ao ser selecionada uma técnica utilizada com frequência na literatura, que tem uma praticidade de implementação tanto na operação quanto frente a uma necessidade de retreinamento de modelo.

No estudo do Aprendizado de Máquina, o princípio da Navalha de Occam recomenda que, diante de vários modelos, o mais simples deve ser escolhido, como ocorreu com a RL com *Oversampling.*

Destaca-se que, ao considerar o custo de uma predição incorreta, não basta avaliar somente os resultados obtidos com as métricas AUC e MCC. Deve-se considerar também a aplicação da FC para apoiar a escolha de uma técnica inteligente.

Considera-se como contribuição do trabalho para a pesquisa acadêmica, o desenvolvimento de um roteiro com cinco fases, aplicando diversas técnicas ao problema da detecção de fraudes em cartões de crédito e, principalmente a comparação do desempenho destas técnicas, por meio de métricas tradicionais,

adicionadas à FC, o que caracteriza uma lacuna acadêmica para este tipo de pesquisa.

Considera-se também como contribuição, o fato deste trabalho apresentar para as empresas uma análise de desempenho alternativa à tradicional, aplicando a FC e, mostrando que uma técnica tradicional e considerada mais simples frente às outras que foram aplicadas, pode sim se tornar uma alternativa.

Para o cliente portador de um cartão de crédito, a contribuição reside no bloqueio mais assertivo do uso impróprio de seu cartão de crédito, frente à uma transação com características de fraude. A instituição emissora do cartão pode informar ao cliente o evento e iniciar o processo de troca da numeração do cartão, trazendo tranquilidade ao cliente em situações de risco financeiro.

Considera-se como limitação deste trabalho, a característica da base de dados utilizada permitir apenas a detecção da fraude, e não sua identificação efetiva. Como, por exemplo, a localidade com maiores ocorrências ou a identificação do cartão de crédito sendo utilizado.

A base de dados utilizada contém a maioria dos atributos como não identificados, comprometendo o entendimento dos fatores que afetaram a identificação de fraudes. Por este motivo o foco deste trabalho se limitou à detecção das fraudes. Outra limitação considerada é o fato de que não foram encontrados na literatura estudos que pudessem ser comparados com os resultados obtidos neste trabalho.

Como sugestão de trabalhos futuros, considera-se a utilização do processo utilizado neste trabalho em outras bases de dados com transações de cartões de crédito, para análise e aferição do uso de FC em outras situações reais.

Para os casos em que existirem quantidade suficiente de instâncias para utilização, este trabalho pode também ter um desdobramento em quantificar esforços de custos em produção, custos efetivos de utilização pela análise de FC ao longo do tempo.

REFERÊNCIAS

ABDALLAH, Aisha; MAAROF, Mohd Aizaini; ZAINAL, Anazida. **Fraud detection system: A survey**. Journal of Network and Computer Applications, vol. 68, p. 90–113, 2016. https://doi.org/10.1016/j.jnca.2016.04.007.

ABECS, Associação Brasileira das Empresas de Cartões de Crédito e Serviços. **Balanço do setor de meios eletrônicos de pagamento 1t2021**. [*S. l.*: *s. n.*], 2021. Disponível em: https://api.abecs.org.br/wp-content/uploads/2021/05/COLETIVA-ABECS-1T21-1.pdf.

ALENZI, H. Z.; ALJEHANE, N. O. **Fraud Detection in Credit Cards using Logistic Regression**. International Journal of Advanced Computer Science and Applications, vol. 11, nº 12, p. 540–551, 2020. https://doi.org/10.14569/IJACSA.2020.0111265.

AL-HASHEDI, Khaled Gubran; MAGALINGAM, Pritheega. **Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019**. Computer Science Review, vol. 40, p. 100402, 2021. https://doi.org/10.1016/j.cosrev.2021.100402.

ASHA, RB; SURESH KUMAR, KR. **Credit card fraud detection using artificial neural network**. Global Transitions Proceedings, vol. 2, nº 1, p. 35–41, 2021. DOI 10.1016/j.gltp.2021.01.006. Disponível em: https://doi.org/10.1016/j.gltp.2021.01.006.

AXUR. **Atividade criminosa online no Brasil**. [*S. l.*: *s. n.*], 2021. Disponível em: https://conteudo.axur.com/hubfs/E-books/Relatórios trimestrais/Relatorio_Axur_Q4_2020+year-in-review.pdf.

BAHNSEN, Alejandro Correa; STOJANOVIC, Aleksandar; AOUADA, Djamila; OTTERSTEN, Björn. **Cost sensitive credit card fraud detection using bayes minimum risk**. Proceedings - 2013 12th International Conference on Machine Learning and Applications, ICMLA 2013, vol. 1, p. 333–338, 2013. https://doi.org/10.1109/ICMLA.2013.68.

BASIT, A.; ZAFAR, M.; LIU, X.; JAVED, A. R.; JALIL, Z.; KIFAYAT, K. **A comprehensive survey of AI-enabled phishing attacks detection techniques**. Telecommunication Systems, vol. 76, nº 1, p. 139–154, 2021. https://doi.org/10.1007/s11235-020-00733-2.

BENCHAJI, Ibtissam; DOUZI, Samira; EL OUAHIDI, Bouabid. **Credit card fraud detection model based on LSTM recurrent neural networks**. Journal of Advances in Information Technology, vol. 12, nº 2, p. 113–118, 2021. https://doi.org/10.12720/jait.12.2.113-118.

BOLTON, Richard J.; HAND, David J. **Unsupervised Profiling Methods for Fraud Detection**. Proc. Credit Scoring and Credit Control VII, , p. 5–7, 2001. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.24.5743.

CHEN, Y. R.; LEU, J. S.; HUANG, S. A.; WANG, J. T.; TAKADA, J. I. **Predicting Default Risk on Peer-to-Peer Lending Imbalanced Datasets**. IEEE Access, vol. 9, p. 73103–73109, 2021. https://doi.org/10.1109/ACCESS.2021.3079701.

CHIGADA, Joel M. **A qualitative analysis of the feasibility of deploying biometric authentication systems to augment security protocols of bank card transactions**. SA Journal of Information Management, vol. 22, nº 1, 10 dez. 2020. https://doi.org/10.4102/sajim.v22i1.1194.

DAL POZZOLO, Andrea; CAELEN, Olivier; LE BORGNE, Yann Aël; WATERSCHOOT, Serge; BONTEMPI, Gianluca. **Learned lessons in credit card fraud detection from a practitioner perspective**. Expert Systems with Applications, vol. 41, nº 10, p. 4915–4928, 2014. https://doi.org/10.1016/j.eswa.2014.02.026.

DINERS. **Diners Club International History**. 2021. Disponível em: https://www.dinersclub.com/about-us/history. Acessado em: 20 jun. 2021.

DORNADULA, Vaishnavi Nath; GEETHA, S. **Credit Card Fraud Detection using Machine Learning Algorithms**. Procedia Computer Science, vol. 165, p. 631–641, 2019. DOI 10.1016/j.procs.2020.01.057. Disponível em: https://doi.org/10.1016/j.procs.2020.01.057.

FANG, Yong; ZHANG, Yunyun; HUANG, Cheng. **Credit card fraud detection based on machine learning**. Computers, Materials and Continua, vol. 61, nº 1, p. 185–195, 2019. https://doi.org/10.32604/cmc.2019.06144.

FAYZRAKHMANOV, R.; KULIKOV, A.; REPP, P. **The difference between precision-recall and ROC curves for evaluating the performance of credit card fraud detection models**. 6., 2018. **Proceedings of International Conference on Applied Innovation in IT** [...]. [*S. l.*: *s. n.*], 2018. vol. 6, p. 17–22.

FOROUGH, Javad; MOMTAZI, Saeedeh. **Ensemble of deep sequential models for credit card fraud detection**. Applied Soft Computing, vol. 99, p. 106883, 2021. DOI 10.1016/j.asoc.2020.106883. Disponível em: https://doi.org/10.1016/j.asoc.2020.106883.

GAMA, João. **Functional Trees**. Machine Learning, vol. 55, nº 3, p. 219–250, jun. 2004. https://doi.org/10.1023/B:MACH.0000027782.67192.13.

GUPTA, A.; LOHANI, M. C.; MANCHANDA, M. **Financial fraud detection using naive bayes algorithm in highly imbalance data set**. Journal of Discrete Mathematical Sciences and Cryptography, vol. 24, nº 5, p. 1559–1572, 2021. https://doi.org/10.1080/09720529.2021.1969733.

HAND, D. J.; WHITROW, C.; ADAMS, N. M.; JUSZCZAK, P.; WESTON, D. **Performance criteria for plastic card fraud detection tools**. Journal of the Operational Research Society, vol. 59, nº 7, p. 956–962, 21 jul. 2008. DOI 10.1057/palgrave.jors.2602418. Disponível em: https://www.tandfonline.com/doi/full/10.1057/palgrave.jors.2602418.

ILEBERI, E.; SUN, Y.; WANG, Z. **Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost**. IEEE Access, vol. 9, p. 165286–165294, 2021. https://doi.org/10.1109/ACCESS.2021.3134330.

JAIN, Yashvi; JAIN, Sarika. **A Comparative Analysis of Various Credit Card Fraud Detection Techniques**. nº 5, p. 402–407, 2019. .

JURGOVSKY, Johannes; GRANITZER, Michael; ZIEGLER, Konstantin; CALABRETTO, Sylvie; PORTIER, Pierre Edouard; HE-GUELTON, Liyun; CAELEN, Olivier. **Sequence classification for credit-card fraud detection**. Expert Systems with Applications, vol. 100, p. 234–245, 2018. DOI 10.1016/j.eswa.2018.01.037. Disponível em: https://doi.org/10.1016/j.eswa.2018.01.037.

KEWEI, X.; PENG, B.; JIANG, Y.; LU, T. **A Hybrid Deep Learning Model for Online Fraud Detection**. 2021. **2021 IEEE International Conference on Consumer Electronics and Computer Engineering, ICCECE 2021** [...]. [*S. l.*: *s. n.*], 2021. p. 431–434. https://doi.org/10.1109/ICCECE51280.2021.9342110.

KIM, E.; LEE, J.; SHIN, H.; YANG, H.; CHO, S.; NAM, S. K.; SONG, Y.; YOON, J. A.; KIM, J. I. **Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning**. Expert Systems with Applications, vol. 128, p. 214–224, 2019. https://doi.org/10.1016/j.eswa.2019.03.042.

LI, W. **Imbalanced data optimization combining K-means and SMOTE**. International Journal of Performability Engineering, vol. 15, nº 8, p. 2173–2181, 2019. https://doi.org/10.23940/ijpe.19.08.p17.21732181.

LI, Zhenchuan; HUANG, Mian; LIU, Guanjun; JIANG, Changjun. **A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection**. Expert Systems with Applications, vol. 175, nº January, p. 114750, 2021. DOI 10.1016/j.eswa.2021.114750. Disponível em: https://doi.org/10.1016/j.eswa.2021.114750.

LIU, Jian; GU, Xin; SHANG, Chao. **Quantitative Detection of Financial Fraud Based on Deep Learning with Combination of E-Commerce Big Data**. Complexity, vol. 2020, 2020. https://doi.org/10.1155/2020/6685888.

LOREY, Vilma Ataíde. **Aquisições Estratégicas: Um Estudo Sobre o Mercado de Cartões de Crédito**. , p. 103, 2008. .

LUCAS, Yvan; PORTIER, Pierre Edouard; LAPORTE, Léa; HE-GUELTON, Liyun; CAELEN, Olivier; GRANITZER, Michael; CALABRETTO, Sylvie. **Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs**. Future Generation Computer Systems, vol. 102, p. 393–402, 2020. DOI 10.1016/j.future.2019.08.029. Disponível em: https://doi.org/10.1016/j.future.2019.08.029.

MADHAV, V. Venu; KUMARI, K. Aruna. **Analysis of Credit Card Fraud Data using PCA**. [*S. l.*: *s. n.*], 2020.

MITCHELL, Tom. **Machine Learning**. [*S. l.*: *s. n.*], 1997.

MROZEK, P.; PANNEERSELVAM, J.; BAGDASAR, O. **Efficient resampling for fraud detection during anonymised credit card transactions with unbalanced datasets**. 2020. **Proceedings - 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing, UCC 2020** [...]. [*S. l.*: *s. n.*], 2020. p. 426–433. https://doi.org/10.1109/UCC48980.2020.00067.

NAVEEN, P.; DIWAN, B. **Relative Analysis of ML Algorithm QDA, LR and SVM for Credit Card Fraud Detection Dataset**. 7 out. 2020. **2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)** [...]. [*S. l.*]: IEEE, 7 out. 2020. p. 976–981. DOI 10.1109/I-SMAC49090.2020.9243602. Disponível em: https://ieeexplore.ieee.org/document/9243602/.

NEGI, S.; DAS, S. K.; BODH, R. **Credit Card Fraud Detection using Deep and Machine Learning**. 2022. **Proceedings - International Conference on Applied Artificial Intelligence and Computing, ICAAIC 2022** [...]. [*S. l.*: *s. n.*], 2022. p. 455–461. https://doi.org/10.1109/ICAAIC53929.2022.9792941.

OLOWOOKERE, Toluwase Ayobami; ADEWALE, Olumide Sunday. **A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach**. Scientific African, vol. 8, p. e00464, 2020. DOI 10.1016/j.sciaf.2020.e00464. Disponível em: https://doi.org/10.1016/j.sciaf.2020.e00464.

PRISCILLA, C. Victoria; PRABHA, D. Padma. **Influence of Optimizing XGBoost to handle Class Imbalance in Credit Card Fraud Detection**. ago. 2020. **2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)** [...]. [*S. l.*]: IEEE, ago. 2020. p. 1309–1315. https://doi.org/10.1109/ICSSIT48917.2020.9214206.

RAUDHA, F.; SAEEDI, M. **Artificial intelligence and machine learning as a tool in preventing and detecting financial fraud: A systematic literature review**. Journal of Advanced Research in Dynamical and Control Systems, vol. 11, nº 11 Special, p. 904–911, 2019. https://doi.org/10.5373/JARDCS/V11SP11/20193114.

SHRESTHA, Ajay; MAHMOOD, Ausif. **Review of Deep Learning Algorithms and Architectures**. IEEE Access, vol. 7, p. 53040–53065, 2019. https://doi.org/10.1109/ACCESS.2019.2912200.

SINGH, Ajeet; JAIN, Anurag. **Adaptive credit card fraud detection techniques based on feature selection method**. Advances in computer communication and computational sciences. [*S. l.*]: Springer, 2019. p. 167–178.

SLADE, Emma L.; DWIVEDI, Yogesh K.; PIERCY, Niall C.; WILLIAMS, Michael D. **Modeling Consumers' Adoption Intentions of Remote Mobile Payments in the United Kingdom: Extending UTAUT with Innovativeness, Risk, and Trust**. Psychology & Marketing, vol. 32, nº 8, p. 860–873, ago. 2015. https://doi.org/10.1002/mar.20823.

TAE, Chung Min; HUNG, Phan Duy. **Comparing ML Algorithms on Financial Fraud Detection**. 19 jul. 2019. **Proceedings of the 2019 2nd International Conference on Data Science and Information Technology** [...]. New York, NY, USA: ACM, 19 jul. 2019. p. 25–29. https://doi.org/10.1145/3352411.3352416.

TANOUZ, D.; SUBRAMANIAN, R. Raja; ESWAR, D.; REDDY, G. V. Parameswara; KUMAR, A. Ranjith; PRANEETH, C. H. V. N. M. **Credit Card Fraud Detection Using Machine Learning**. 2021. **2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)** [...]. [*S. l.*: *s. n.*], 2021. p. 967–972.

THEJAS, G. S.; DHEESHJITH, Surya; IYENGAR, S. S.; SUNITHA, N. R.; BADRINATH, Prajwal. **A hybrid and effective learning approach for Click Fraud detection**. Machine Learning with Applications, vol. 3, nº November 2020, p. 100016, 2021. DOI 10.1016/j.mlwa.2020.100016. Disponível em: https://doi.org/10.1016/j.mlwa.2020.100016.

THIRUPATHI, M.; VINAYAGAMOORTHI, G.; MATHIRAJ, S. **Effect Of Cashless Payment Methods: A Case Study Perspective Analysis**. International Journal of Scientific & Technology Research, vol. 8, nº 08, ago. 2019.

TRISANTO, D; RISMAWATI, N.; MULYA, M. F.; KURNIADI, F. I. **Effectiveness undersampling method and feature reduction in credit card fraud detection**. International Journal of Intelligent Engineering and Systems, vol. 13, nº 2, p. 173–181, 2020. https://doi.org/10.22266/ijies2020.0430.17.

TRISANTO, D.; RISMAWATI, N.; MULYA, M. F.; KURNIADI, F. I. **Modified Focal Loss in Imbalanced XGBoost for Credit Card Fraud Detection**. International Journal of Intelligent Engineering and Systems, vol. 14, nº 4, p. 350–358, 2021. https://doi.org/10.22266/ijies2021.0831.31.

TRISANTO, Dedy; RISMAWATI, Nofita; MULYA, Muhamad Femy; KURNIADI, Felix Indra. **Effectiveness undersampling method and feature reduction in credit card fraud detection**. International Journal of Intelligent Engineering and Systems, vol. 13, nº 2, p. 173–181, 2020. https://doi.org/10.22266/ijies2020.0430.17.

VADAKARA, J. M.; KUMAR, D. V. **Aggrandized random forest to detect the credit card frauds**. Advances in Science, Technology and Engineering Systems, vol. 4, nº 4, p. 121–127, 2019. https://doi.org/10.25046/aj040414.

VICTORIA PRISCILLA, C.; PADMA PRABHA, D. **Analysis of performance on classification algorithms for credit card fraud detection**. Journal of Advanced Research in Dynamical and Control Systems, vol. 12, nº 3 Special, p. 1403–1409, 2020. https://doi.org/10.5373/JARDCS/V12SP3/20201391.

VISA. **A história da Visa**. [*s. d.*]. Disponível em: https://www.visa.com.br/sobre-a-visa/nosso-negocio/historia-da-visa.html. Acessado em: 20 jun. 2021.

WHITROW, C.; HAND, D. J.; JUSZCZAK, P.; WESTON, D.; ADAMS, N. M. **Transaction aggregation as a strategy for credit card fraud detection**. Data Mining and Knowledge Discovery, vol. 18, nº 1, p. 30–55, 2009. https://doi.org/10.1007/s10618-008-0116-z.

YUAN, M. **A Transformer-based Model Integrated with Feature Selection for Credit Card Fraud Detection**. 2022. **ACM International Conference Proceeding Series** [...]. [*S. l.*: *s. n.*], 2022. p. 185–190. https://doi.org/10.1145/3529399.3529429.

ZHANG, Xinwei; HAN, Yaoci; XU, Wei; WANG, Qili. **HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture**. Information Sciences, vol. 557, p. 302–316, 2021. DOI https://doi.org/10.1016/j.ins.2019.05.023. Disponível em: https://www.sciencedirect.com/science/article/pii/S002002551930427X.

ZHININ-VERA, L.; CHANG, O.; VALENCIA-RAMOS, R.; VELASTEGUI, R.; PILLIZA, G. E.; SOCASI, F. Q. **Q-Credit Card Fraud Detector for Imbalanced Classification using Reinforcement Learning**. 1., 2020. **ICAART 2020 - Proceedings of the 12th International Conference on Agents and Artificial Intelligence** [...]. [*S. l.*: *s. n.*], 2020. vol. 1, p. 279–286.

APÊNDICE A – LISTA DE CÓDIGOS UTILIZADOS NOS EXPERIMENTOS

Os códigos em Python utilizados para a realização dos experimentos computacionais, encontram-se disponíveis no seguinte endereço eletrônico: https://github.com/rogerwjl/ccfraud2023.

Os códigos estão divididos em quatro partes: determinação da proporção entre as bases teste e treinamento; determinação da proporcionalidade entre fraude e não fraude para Undersampling e Oversampling e experimentos gerais.