Detecção de fraude em aplicativos de E-commerce

Mariana A. Guimarães, Fabio S. Lopes

FCI – Universidade Presbiteriana Mackenzie (UPM)
Rua da Consolação, 930 – 01302-907 – São Paulo –SP – Brazil
mariana.araujoguimaraes@gmail.com.br,flopes@mackenzie.br

Abstract. *Due to technological growth, online shopping has become essential in people's lives because what they want is convenience and convenience when shopping. With this great growth, fraudsters also take advantage of the situation through fraud. Fraud in applications and e-commerce can be detected from studies and machine learning mechanisms. For this reason, fighting fraud is so necessary as the trend is growing and fraudsters, with each passing day, find methods to practice and improve their actions in order to obtain financial benefits. Companies need to adopt machine learning methods to obtain more accurate and reliable predictions to combat fraudulent attacks. This project aims to understand the different types of fraud, how they happen, their risks and how to detect a possible fraud through machine learning technologies and methods.*

Resumo. *Devido ao crescimento tecnológico, as compras on-line se tornaram essenciais na vida da população pois o que elas desejam é a praticidade e comodidade na hora da compra. Com esse grande crescimento, os fraudadores também se aproveitam da situação por meio das fraudes. A fraude em aplicativos e e-commerce, pode ser detectada a partir de estudos e mecanismos de aprendizado de máquina. Por esse motivo, o combate às fraudes é tão necessária pois a tendência é de crescimento e os fraudadores, a cada dia que passa encontram métodos de praticar e aprimorar suas ações a fim obter benefícios financeiros. As empresas precisam adotar métodos de machine learning para obterem previsões mais precisas e confiáveis para combaterem ao ataques fraudulentos. Esse projeto possui como objetivo, entender os diferentes tipos de fraude, como acontecem, seus riscos e como detectar uma possível fraude através de tecnologias e métodos de machine learning.*

1. Introdução

Com o avanço constante da tecnologia e a transformação digital o dia a dia das pessoas e empresas têm se tornado mais prático, eficaz e ágil. Contudo, os criminosos também enxergam muitas oportunidades para se aproveitarem da inocência e das vulnerabilidades dos sistemas para praticarem seus atos criminosos.

Os golpes no mundo online tornaram-se recorrentes em diversos segmentos, principalmente pela criatividade dos fraudadores. Uma das explicações para isso acontecer, é devido a vulnerabilidades no sistema associados à compra em ambientes e-commerce que prejudicam a confiabilidade prejudicando a empresa.

A fraude é qualquer ato ardiloso, enganoso e de má-fé, com o intuito de lesar ou ludibriar outrem para trazer algum tipo de vantagem, na maioria dos casos é financeira,

ao fraudador sobre a vítima. A fraude abrange um universo enorme e complexo, de diferentes origens de crimes. Seus dados podem ser irreparáveis à vítima, sejam eles financeiros, psicológicos ou até mesmo de imagem.

Apesar do constante surgimento de novos meios de pagamento, o cartão de crédito é o meio de pagamento mais utilizado no comércio eletrônico e que não exige, necessariamente, a presença do titular para realizar a transação, e é nesse ponto que os fraudadores enxergam suas oportunidades de ataque em prol de um único objetivo: ganhar dinheiro.

Esse cenário faz com que grandes quadrilhas de fraudadores vivam em busca de meios para conseguirem os dados desses cartões com o intuito de realizar o que é um dos maiores pesadelos do varejo atualmente: a Fraude de Cartão de Crédito.

No mundo digital, ataques em cartões de crédito não são os únicos objetivos dos fraudadores. Eles podem roubar seus dados pessoais e financeiros como RG, CPF, endereço, dados de cartão e entre outros para, por exemplo, solicitar um empréstimo no banco, comprar um imóvel, realizar compras em qualquer ambiente digital e muitas outras práticas criminosas, mas como podem também acessar dados de empresas e vender para a concorrência e ganhar muito dinheiro.

Para se manter longe de transtornos e prejuízos com os tipos de fraude, é preciso saber como elas acontecem, quais são os principais tipos e como detectá-las.

O objetivo desse artigo é apresentar o que é fraude, seus diferentes tipos e detalhar os riscos de não ter um monitoramento antifraude. Sendo assim, o artigo pretende fornecer uma visão mais abrangente das variações da fraude e métodos pelos quais a tecnologia pode ser implementada para melhorar a prevenção e a detecção de fraudes.

1.1. Contextualização e Relevância do Tema

O e-commerce está se tornando cada vez mais relevante para o faturamento das empresas. Com o avanço da tecnologia e o surgimento da pandemia do Coronavírus (COVID-19), os aplicativos de marketplace se tornaram mais populares e alavancaram a tendência de utilização dessas plataformas de compras eletrônicas. De acordo com Eugênio (2016) pôde-se identificar que em poucos anos os consumidores passaram a confiar em mecanismos de segurança e no mesmo contexto a tecnologia de banda larga e a popularização dos smartphones e tablets.

Para Sherly e Nedunchezhian (2010, p.1-7) em meio a esse avanço tecnológico, as fraudes em comércio eletrônico crescem com o aumento das transações online necessitando que as empresas busquem por soluções mais avançadas para se protegerem de serviços financeiros, e os titulares de cartões de crédito contra ataques de fraude online que estão em demasiado crescimento.

A fraude é um risco de negócio que as empresas enfrentam, podendo ocorrer em vários nichos das organizações. Diversos escândalos envolvendo violação de dados ou também conhecida como vazamento de dados, perda de dados e entre outros, que segundo Freitas (2014, p.12) é um incidente de segurança em que dados com informações confidenciais são roubados e utilizados por terceiros não autorizados. Tendo esse contexto em evidência, torna-se cada vez mais necessário que as empresas adotem tecnologias de controle e prevenção a fraude.

Ter um departamento de risco, plataforma de pagamentos, estudos, sistemas de segurança e implantação de tecnologias são iniciativas que ajudarão sua empresa a controlar as fraudes.

Portanto, é importante analisar possíveis falhas e vulnerabilidades no sistema que colaboram com os ataques e entender que as transações fraudulentas para Behera e Panigrahi (2015) podem ser detectadas observando as suspeitas mudanças no comportamento do consumidor, sendo a técnica de mineração de dados utilizada para extrair padrões dos dados e propor técnicas de classificação podendo ser aplicadas para detectar e prevenir fraudes.

1.2. Objeto de Pesquisa

1.2.1. Contextualização do Problema de Pesquisa

Atividades fraudulentas podem ocorrer em diversas áreas, como redes sociais, banking on-line e em comércio eletrônico. As fraudes estão crescendo juntamente com a expansão da tecnologia resultando em grandes perdas para os negócios das empresas.

Uma pesquisa realizada pela Associação Brasileira de Comércio Eletrônico (ABComm) em parceria com a Neotrust aponta que o varejo digital concentrou cerca de 43 milhões de consumidores únicos, tendo um aumento de 36,7% em relação ao ano de 2020 (BM&C NEWS, 2021). A receita teve um aumento de 68,5% em comparação com ano anterior (2020), obtendo um valor equivalente a R$ 301 milhões em compras pela internet, esse número poderia ser ainda maior se grande parte das transações não fossem bloqueadas pelos varejistas por suspeita de fraude.

De acordo com uma pesquisa realizada no Brasil pela Vesta, 42% dos entrevistados informaram que já passaram por um constrangimento de terem alguma de suas compras online bloqueadas, recusadas ou algum atraso por suspeita de fraude (BM&C NEWS, 2021). A pesquisa também indicou que 43% das pessoas entrevistadas apontaram que se passassem por essa situação reclamariam em redes sociais ou em sites como o Reclame Aqui, 31% disseram que avisariam seus parentes e amigos sobre a situação que passaram e 20% responderam que não comprariam na mesma loja (BM&C NEWS, 2021).

Quando se fala de fraude, não pode deixar passar um termo muito conhecido e muita das vezes pode ser assustador para o negócio: chargeback. O termo traduzido do inglês significa “reversão de pagamentos” e consiste na devolução dos valores de uma transação realizada com cartão de crédito e os motivos para que isso ocorra podem ser: contestação de uma compra não reconhecida ou alegação de fraude online por parte do cliente ou do banco, e até mesmo o não reconhecimento do produto comprado (Adyen, 2021).

No mundo do e-commerce, 91% dos casos de chargeback são de fato uma fraude, ou seja, quando uma pessoa utiliza o cartão de crédito que ele não seja o titular e que não obteve seu consentimento para realização da compra (Adyen, 2021). O chargeback não é apenas constrangedor para o cliente mas também para empresa, que implica uma série de problemas, como multas das operadoras de cartão de crédito, diminuição da receita, penalização pelos bancos e a falta de confiança do cliente.

Segundo a Adyen (2021), as operadoras de cartão de crédito Visa e Mastercard possuem programas que monitoram as companhias que possuam mais de 100 contestações por mês e em que os pedidos representam 1% do total de transações. As empresas que possuem um alto nível de chargeback recebem uma notificação e um tempo para corrigirem os erros e caso persistam, as lojas começam a receber multas por cada chargeback recebido.

De acordo com as pesquisas apontadas nos parágrafos anteriores, um fator muito importante na realização de compras online é sem dúvidas ter confiança no site/aplicativo e ter uma boa recomendação. Quando ocorre um problema como a fraude, a imagem da marca está sendo prejudicada levando o cliente a ter uma memória ruim da loja e quando se fala de e-commerce, confiança é a chave do negócio.

Neste contexto, o presente artigo objetiva responder a seguinte pergunta: Como as tecnologias de machine learning podem ajudar o e-commerce a detectar ataques fraudulentos?

1.3. Objetivos do Estudo

1.3.1. Objetivo Geral

O presente trabalho tem por objetivo final ou geral identificar transações fraudulentas de cartões de crédito a partir de algoritmos de machine learning em aplicativos de e-commerce.

1.4. Justificativa

Em decorrência do avanço tecnológico e o grande crescimento das lojas virtuais, todas as pessoas estão vulneráveis a caírem em algum tipo de fraude. É muito comum como os fraudadores agem e quando menos se espera, o ato já foi praticado. A proposta desse artigo é apresentar o conceito sobre fraude, seus diferentes tipos e mostrar como é possível identificar transações fraudulentas de cartões de crédito com algoritmos de machine learning. Será apresentando também alguns exemplos de algoritmos que podem ajudar na detecção.

Sendo assim, o interesse pelo tema proposto neste projeto parte da consideração de toda a problemática em torno dos ataques de fraude que o e-commerce passa durante suas vendas, que cresce assustadoramente no Brasil e no mundo, é válido compreender estudos que mostrem que o monitoramento e acompanhamento do controle interno podem evitar grandes perdas financeiras. Para Pereira, Santos e Rocha (2014), o controle interno tem como objetivo a medição de padrões, a avaliação de desempenho, a comparação de metas, com o intuito de corrigir vulnerabilidades, detectar anormalidades através dos resultados obtidos em análises exploratórias no intuito de simplificar as rotinas passiveis de erros ou fraudes. O controle interno tem três objetivos: salvaguarda dos interesses da empresa, precisão relatórios financeiros e estímulo à eficiência operacional.

O trabalho é importante também a partir do momento que pretende evidenciar dados que mostrem o crescimento dos ataques de fraude no e-commerce, além de estudos que apresentem evidências que existem diferentes tipos de fraudes e como o avanço tecnológico pode ajudar os departamentos de risco a identificarem um ataque de fraude a partir de comportamentos para concluírem suas ações.

A escolha deste tema está associado ao fato de a autora ter trabalhado na área de risco de uma pequena de empresa que utilizava serviços do governo para fornecer créditos de bilhete único para a população que baixasse o aplicativo. A empresa sofreu ataques fraudulentos em seu aplicativo em que os fraudadores utilizavam diversos cartões de crédito no mesmo cadastro para abastecerem bilhete único. O projeto irá contribuir para o enriquecimento do seu desempenho profissional e para outras pequenas empresas que não possuem muitos recursos mas que se interessem pelo assunto e compreendam que um ataque desses pode ocorrer em seu varejo virtual.

Outro fato a ser considerado é que os problemas com fraude no mundo virtual no qual todas as pessoas estão envolvidas exigem uma análise muito profunda de todas as variáveis envolvidas. Dentro desse contexto, esse trabalho se justifica, pois abrange os principais pontos, servindo de base para outros trabalhos, e contribuindo como fonte de informações para estudantes e demais interesses que atuem na área de Risco.

2. Referencial Teórico

O referencial teórico da presente pesquisa foi estruturado em dois tópicos: Conceitos Envolvidos e Trabalhos Correlatos.

2.1. Conceitos Envolvidos

Como mencionado anteriormente, segundo o dicionário, a fraude é um ato ardiloso, enganoso e de má-fé que tem como objetivo lesar ou ludibriar outrem para trazer alguma vantagem financeira ao fraudador sobre a vítima. A fraude abrange um universo muito complexo com diferentes origens e devido a evolução das transações comerciais na internet e ao aumento das compras realizadas no e-commerce, os criminosos encontram grandes oportunidades nesse negócio.

A fraude tem origem nos mais diversos métodos e variadas formas, por ser um crime dinâmico e suas variações se desenvolvem dia após dia com diversas tentativas diferentes até que um método seja descoberto. Sobretudo, por se tratar de um assunto muito complexo, a fraude possui muitos tipos, alguns mais comuns e outros que servem de base para outras variações, de acordo com a ClearSale (2021). Segundo a ClearSale (2021), a seguir, será explicado 12 tipos diferentes de fraude, sendo:

- Roubo de identidade: o criminoso se passa por outra pessoa utilizando seus dados de identidade de terceiros com o objetivo de realizar comprar em nome da vítima, sendo um dos crimes mais praticados há anos.

- Pedido de estorno: consiste no criminoso realizar uma compra no site/aplicativo utilizando o cartão de crédito da vítima, logo após o recebimento do produto, ele entra em contato com a instituição financeira e relata que foi vítima de um golpe solicitando o estorno do valor e dessa forma, a loja virtual faz a devolução “indevida” do dinheiro para o fraudador.

- Interceptação de mercadorias: pode ser dividida em duas formas: a primeira ocorre quando o responsável pela ação criminosa altera o endereço de entrega cadastrado pelo usuário legítimo, a segunda forma ocorre quando o criminoso se informa a respeito da data e horário em que a entrega será concluída se passando pelo morador ou informa que ele não se encontra e assina o recebimento do produto.

- Controle da conta do usuário: os fraudadores agem tendo acesso total à conta do usuário podendo fazer alterações de endereço de entrega e acesso aos dados de cartão de crédito ou dados bancários da vítima.

- Phishing: também chamado de “pesca de dados”, é uma das variações da fraude que mais ocorrem e em constante crescimento. Por se tratar de um golpe que tem o intuito de oferecer ofertas exclusivas e recompensas que atraem e induzem os usuários a clicarem em links falsos enviados por e-mail, sms, sites falsos ou até mesmo aparecer na tela de sua rede social. Ao clicar no link, é redirecionado para páginas adulteradas contendo malwares que se instalam na máquina da vítima, a partir desse momento, a vítima está vulnerável correndo risco de exposição de seus dados pessoais gerando transações bancárias indevidas e não autorizadas.

- Páginas clonadas: em que os hackers invadem o site da loja e alteram o link de compra, direcionando o usuário à uma página falsa sem que ele perceba pois o layout é idêntico ao original, quando o usuário preenche suas informações e seus dados, o pagamento é desviado após a finalização da transação.

- Botnets: é um conjunto de dispositivos conectados à internet infectados por malwares possibilitando o controle dos ladrões. No momento em que ocorre a fraude, os criminosos utilizam os botnets para vazamento de credenciais, acessos não permitidos, roubo de dados e ataques por negação de serviço distribuído que causam inatividade não planejada da aplicação.

- Triangulação: os criminosos criam lojas falsas e com produtos de alta procura no mercado e com preços mais baixos que o comum. O objetivo é obter os dados das vítimas para outras finalidades e com isso, os produtos são revendidos em nome de terceiros.

- Fraude amiga: ocorre quando um parente, amigo ou familiar realiza uma compra com os meios de pagamento do titular sem seu consentimento e quando ele recebe a fatura e não reconhece a compra, entra em contato com a instituição financeira do cartão informando que não realizou aquela compra gerando então um chargeback.

- Autofraude: é uma ação diferente das anteriores pois é um tipo de fraude em que o próprio titular do cartão realiza e contesta, dentro do prazo de 180 dias, a compra mesmo já tendo recebido.

- Fraude de afiliada: é gerada por uma afiliada na tentativa de gerar receita ilegítima, ou seja, cenários fictícios são criados a fim de induzir estabelecimentos comerciais a pagarem comissões indevidas a falsos afiliados que teriam direito a comissões sobre as vendas.

- Teste de cartão: ocorre quando os criminosos utilizam lojas virtuais ou aplicativos de e-commerce para testar a base de cartões de crédito que possuem em suas mãos. O objetivo dessa fraude é realmente realizar diversas tentativas de compra para descobrirem se os cartões estão bloqueados, cancelados ou se o limite do cartão de crédito foi atingido

Tendo em vista os eventos citados anteriormente, é possível identificar diversos momentos em que a fraude está presente em situações dos dias atuais. Com o avanço e expansão da tecnologia, existe o desenvolvimento de trabalhos utilizando metodologias de aprendizado de máquina, visando mitigar a ocorrência de fraudes e que será mais bem detalhado na seção a seguir.

Para Mehta e Patel (2011), Machine Learning é a capacidade de fazer computadores executarem ações de modo autônomo, ou seja, sem a necessidade de instruções pré-programadas. O aprendizado de máquina é um método de análise de dados que automatiza a construção de modelos analíticos a partir da construção de algoritmos para ensinar máquinas a desempenharem determinadas tarefas.

Como apresentado por Bishop (2006), Trevor, Robert e JH (2009), Murphy (2012) e Barber (2012) o aprendizado de máquina desempenha papel fundamental em áreas como estatística, mineração de dados e inteligência artificial, além de ser cada vez mais utilizadas em outras disciplinas como áreas de engenharia.

É um ramo importante da Inteligência Artificial em que um algoritmo de ML possibilita sistemas a aprenderem com dados, identificar padrões e tomar decisões de forma autônoma. Com o aprendizado de máquina é possível reconhecer e extrair padrões de um grande volume de dados sendo então, construído um modelo de aprendizado. A construção do modelo de aprendizado de dados é composta na observação dados como: exemplos, experiência direta ou instrução, após o aprendizado, o algoritmo é capaz de executar tarefas complexas, prever com um nível de precisão ainda maior e se comportar de forma inteligente. De forma resumida, o ML é uma forma de trazer benefícios futuros com base em experiências do passado.

Técnicas de machine learning são aplicadas para detecção de fraudes, em que há uma grande quantidade de transações não fraudulentas do que fraudulentas dificultando a identificação. Para Amarasinghe, Aponso e Krishnarajah (2018) esses métodos são necessários para buscar soluções mais precisas.

De acordo com Omar, Fred e Swaib (2018), a utilização de algoritmos de machine learning para identificar perfis fraudulentos reduz processos manuais e automatiza análises e verificação das transações para classificação como fraude e não fraude.

Pacheco (2019) apresenta que o aprendizado de máquina possui dois principais subcampos de aprendizado, sendo eles o aprendizado supervisionado e o não supervisionado. O método supervisionado exige dados rotulados com foco na previsão precisa, sendo que já existem dados prévios do padrão que se busca identificar, por outro lado o não supervisionado agrupa as informações por semelhança sem a utilização de rótulos sendo o objetivo a identificação de padrões nos dados. Um aprendizado que não foi apresentado mas será descrito é o semi-supervisionado que utiliza as duas técnicas anteriormente citadas para obter o resultado esperado, segundo Zhou (2018).

Após uma breve explicação sobre os possíveis tipos de aprendizado no meio do machine learning, serão apresentados na seção a seguir, os classificadores empregados neste artigo.

2.2. Trabalhos Correlatos

Com o avanço e expansão da tecnologia, existe o desenvolvimento de trabalhos utilizando metodologias de aprendizado de máquina, visando mitigar a ocorrência de fraudes.

Pracidelli (2018) realizou um estudo para identificação de fraudes utilizando data mining e machine learning em empresa de transporte privado que opera por aplicativos. O objetivo do artigo foi detalhar uma detecção de fraude na arquitetura baseada na identificação de padrões de comportamento em bases de corrida de uma empresa de transporte de aplicativos, considerando a construção de um artefato capaz de minimizar

o problema com o uso de algoritmos supervisionados e não supervisionados com base em técnicas de machine learning e com isso a arquitetura foi implementada e permitiu validar o modelo, com melhor performance e acurácia, capaz de identificar suspeitas de fraude de forma mais precisa.

A autora fez uma revisão da literatura explicando o que é o machine learning e como pode utiliza-lo na detecção de fraude. Detalhou os métodos de agrupamento e classificação, técnicas de machine learning como, Rede Neural Artificial - ANN e Suport Vector Machine – SVM para poder definir a arquitetura desenvolvida para detecção de fraude com base em estudos obtidos em seu artigo. Essas revisões foram importantes para que a autora pudesse realizar experimentos baseando-se nos principais passos na metodologia DRS - Design Science Research.

A proposta deste artigo foi identificar as corridas suspeitas de fraude a partir do agrupamento de características em comum para poder rotulá-las. Após o início da execução de classificação utilizando os algoritmos SVM e ANN com o intuito de verificar qual dos dois obteve melhores resultados. Com a execução dos agrupamentos, foi possível classificar se as corridas eram fraudulentas ou legítimas.

O estudo chegou à conclusão de que é possível detectar fraude com a arquitetura aplicada demonstrando adequada para a implementação em empresas de transporte por aplicativo, sendo o K-means e Redes Neurais que apresentaram melhores resultados.

Oliveira (2016) apresentou um estudo para detecção de fraudes em cartões utilizando um classificador baseado m regra de associação de regressão logística. O objetivo do artigo é apresentar uma arquitetura baseada em regras de associação e regressão logística para minerar regras nos dados e produzir, como resultado, conjuntos de regras de detecção de transações fraudulentas disponibilizando para os especialistas. Sendo assim, os especialistas terão auxílio de computadores para descobrir e gerar regras que embasam o classificador com o intuito de diminuir a chance de ocorrer novos padrões fraudulentos que anteriormente não foram reconhecidos e gerar e manter as regras mais eficientes.

O autor chegou à seguinte conclusão: a aplicação combinada das técnicas estatísticas de análise sensível ao custo, regras de associação e regressão logística mostraram-se conceituais e teoricamente coerentes. Os resultados do experimento demonstraram a viabilidade técnica e prática da proposta.

3. Metodologia da Pesquisa

O propósito da pesquisa aplicada deste artigo é de exploração. Inicialmente, será analisada uma base de dados aberta com dados de transações em cartão de crédito sendo o objetivo identificar se as transações podem ser classificadas como fraude ou como uma transação confiável.

Os dados coletados para a pesquisa serão processados de forma quantitativa em que técnicas e algoritmos de machine learning serão aplicados para chegar em um resultado satisfatório. Para que o andamento da pesquisa seja precisa, alguns passos serão tomados:

1. Análise exploratória da base de dados
2. Preparação dos dados

3. Separar a base de treino e teste
4. Balanceamento dos dados
5. Escolha do melhor método de balanceamento de dados
6. Escolha do melhor algoritmo
7. Execução do algoritmo
8. Resultados

A finalidade da pesquisa explicativa busca identificar os perfis fraudulentos, assim como os perfis confiáveis para compreender se os fraudadores mantém um padrão quando praticam o ataque. Também será identificado os comportamentos de um modo geral das transações a fim de detectar uma fraude.

4. Desenvolvimento e Resultados

Nesta seção, será apresentada o desenvolvimento da lógica para detecção de fraude em um dataset aberto do Kaggle (Credit Card Fraud Detection, 2018) e os resultados obtidos.

Conforme citado anteriormente, para desenvolvimento do artigo foi utilizado um conjunto de dados aberto do Kaggle (Credit Card Fraud Detection, 2018). Este conjunto de dados contém transações feitas por cartões de crédito de titulares europeus realizadas em 2013 por um período de dois dias, em que possui 284.807 transações sendo 492 transações consideradas fraudulentas. Pode ser observado que o conjunto de dados é altamente desbalanceado pois a classe positiva para fraudes, corresponde por apenas 0,172% de todas as transações.

O conjunto de dados contém apenas variáveis de entrada numéricas que são resultado de uma transformação PCA. Por questões de confidencialidade, não foi possível que a fonte fornecesse os recursos originais e mais informações básicas sobre os dados. As colunas V1, V2, V3, ...V28 são os principais componentes obtidos com o PCA com exceção das colunas “Time”, “Value” e “Class” que representam respectivamente os segundos decorridos entre cada transação e a primeira transação, valor da transação e variável de resposta para 1 em caso de fraude e 0 caso negativo de fraude.

Com o objetivo de conhecer o conjunto de dados, será iniciado o passo de análise exploratória. Conforme a figura 1, é possível verificar as 5 linhas iniciais do conjunto de dados e como os dados (V1, V2, V3, ... V28) ficaram após a transformação com o PCA.

	Time	V1	V2	V3	V4	V5	V6	V7	V8	V9	...	V28	Amount	Class
0	0.0	-1.359807	-0.072781	2.536347	1.378155	-0.338321	0.462388	0.239599	0.098698	0.363787	...	-0.021053	149.62	0
1	0.0	1.191857	0.266151	0.166480	0.448154	0.060018	-0.082361	-0.078803	0.085102	-0.255425	...	0.014724	2.69	0
2	1.0	-1.358354	-1.340163	1.773209	0.379780	-0.503198	1.800499	0.791461	0.247676	-1.514654	...	-0.059752	378.66	0
3	1.0	-0.966272	-0.185226	1.792993	-0.863291	-0.010309	1.247203	0.237609	0.377436	-1.387024	...	0.061458	123.50	0
4	2.0	-1.158233	0.877737	1.548718	0.403034	-0.407193	0.095921	0.592941	-0.270533	0.817739	...	0.215153	69.99	0

Figura 1. Conhecendo o conjunto de dados

Ainda na análise exploratória, para que não haja futuros problemas é necessário verificar se o conjunto de dados possui valores ausentes para que sejam tratados, e nesse processo não foi localizado nenhum dado faltante sendo assim, não necessitando de um trabalho de limpeza.

Conforme descrito anteriormente, a base de dados contém um desbalanceamento notório pois as classes classificatórias para fraude (Class = 1) contém 492 casos positivos para fraude, representando apenas 0,17% e 284315 para casos negativos de fraude. Para que o modelo não sofra problemas em seu treinamento e acurácia é necessário balancear os dados.

O último passo dentro da análise exploratória foi analisar através do boxplot, se contém diferença no padrão das transações em relação a variável Amount. E de acordo com a figura 2, é possível enxergar que existe uma distribuição diferente para ambas as classes, beneficiando o treinamento do algoritmo.

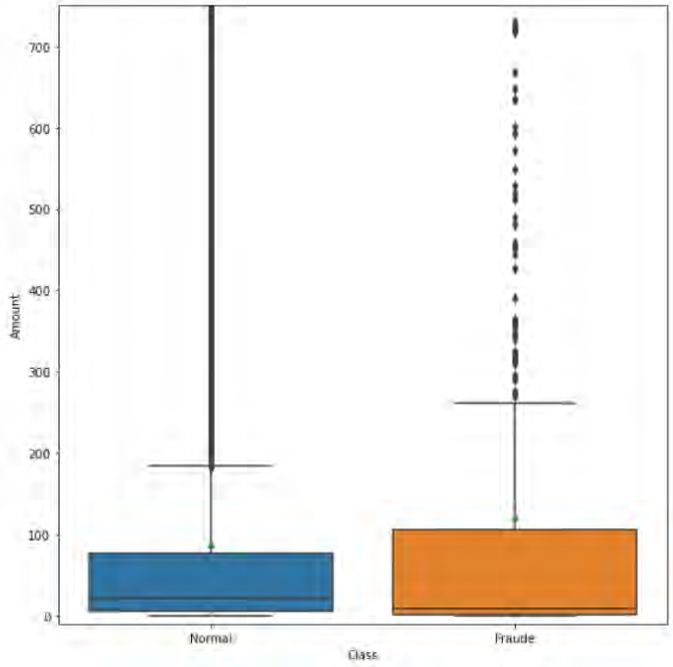

Figura 2. Análise da diferença no padrão das transações em relação a variável Amount

O próximo passo para dar andamento no artigo será realizar a preparação dos dados das colunas Time e Amount que não estão padronizadas no conjunto. A padronização será realizada utilizando a classe StandardScaler da biblioteca slkearn.preprocessing, que de acordo com a sua documentação (Preprocessing data, c2007-2022), implementa a TransformAPI para calcular a média e o desvio padrão em um conjunto de treinamento para poder reaplicar posteriormente a mesma transformação no conjunto de teste.

Scaler_amount	Scaler_time
0.244964	-1.996583
-0.342475	-1.996583
1.160686	-1.996562
0.140534	-1.996562
-0.073403	-1.996541

Figura 3. Scaler das colunas Amount e Time

Dando andamento, a base será dividida em base de treino e base de teste para então iniciarmos o balanceamento dos dados com o objetivo de o modelo apresentar um desempenho melhor para conseguir realizar a identificação das transações fraudulentas. Neste artigo, serão usados dois modelos para balanceamento dos dados: ADASYN e SMOTE, segundo sua documentação o ADASYN concentra-se em gerar amostras próximas as amostras originais que são classificadas erroneamente usando o classificador k-Nearest Neighbors, enquanto a implementação do SMOTE não fará nenhuma distinção entre amostras fáceis e difíceis a serem classificadas usando a regra dos vizinhos mais próximos. A seguir, na tabela 1, é possível observar o resultado do balanceamento dos dados com o ADASYN e SMOTE.

Tabela 1. Resultado do balanceamento dos dados utilizando ADASYN e SMOTE

Balanceamento	Classificação	Resultado (quantidade de casos)
ADASYN	**Fraude**	**213.284**
	Não fraude	**213.236**
SMOTE	**Fraude**	**213.236**
	Não fraude	**213.236**

O balanceamento da base já foi concluído mas ainda não é possível identificar qual modelo performou um melhor balanceamento. Para dar prosseguimento, o estudo vai contar com a utilização de dois modelos de machine learning, sendo Regressão Logística e Árvore de Decisão e verificar qual dos dois teve a melhor acurácia e então escolher o modelo de balanceamento.

Segundo o TIBCO, a regressão logística é um algoritmo de machine learning utilizado para ajudar a criar previsões precisas para os problemas de classificação e de acordo com Ayush Pant (2019) transforma sua saída usando a função sigmoide logística para retornar um valor de probabilidade.

De acordo com Gabriel Sacramento (2021), árvore de decisão é um algoritmo de machine learning utilizado para classificação e regressão, ou seja, pode ser utilizado para prever categorias discretas (sim ou não/ 1 ou 0) e prever valores numéricos. Ela estabelece nos que se relacionam entre si por uma hierarquia em que existe o nó-raiz, sendo o mais importante, e os nós-folha que são os resultados. Ainda, segundo Gabriel Sacramento (2021), no contexto de machine learning, o nó-raiz é um dos atributos da base de dados e o nó-folha é a classe ou valor que será gerado como resposta.

Com base nas explicações citadas nos parágrafos anteriores, os modelos serão construídos e com base na acurácia e na matriz de decisão, decidir qual o melhor modelo. Primeiro, será observado a construção do modelo de Regressão Logística utilizando ADASYN.

Na figura 4, pode-se observar que o modelo previu 114 fraudes, porém um ponto negativo no modelo foi que a quantidade de falsos positivos (FP) indicam que durante as transações, os cartões de crédito seriam bloqueados mais vezes elevando a taxa de recusa pelo cliente, mas com isso, os prejuízos seriam menores.

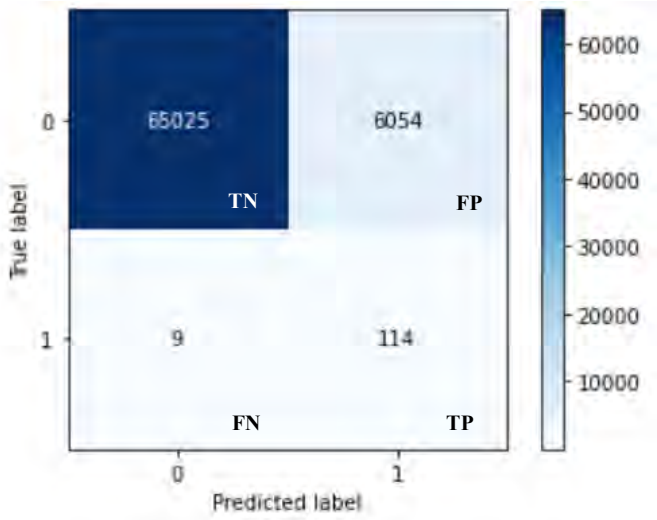

Figura 4. Matriz de Confusão – Regressão Logística com ADASYN

Na figura 5, é possível observar a acurácia, precisão, recall e outras métricas.

	precision	recall	f1-score	support
0	0.9999	0.9148	0.9555	71079
1	0.0185	0.9268	0.0362	123
accuracy			0.9148	71202
macro avg	0.5092	0.9208	0.4958	71202
weighted avg	0.9982	0.9148	0.9539	71202

AUC = 0.9208

Figura 5. Resumo da classificação

Na figura 6, será apresentada a construção do modelo de Regressão Logística utilizando SMOTE. Pode-se observar que fazendo a comparação entre o ADASYN e o SMOTE, a quantidade de falsos negativos (FN) teve crescimento de 6 casos, a quantidade de verdadeiros positivos (TP) caiu 6 casos, porém quando analisada a quantidade de falsos positivos (FP) nota-se uma diminuição de mais de 4000 casos. E com isso, os cartões de crédito utilizados durante as transações seriam bloqueados menos vezes. Os valores referentes a área sob a curva Roc estão bem próximas.

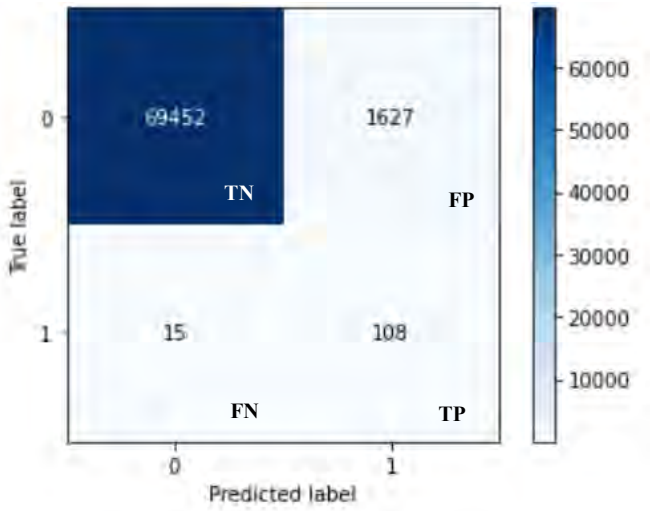

Figura 6. Matriz de Confusão – Regressão Logística com SMOTE

Comparando a acurácia, houve uma pequena diferença de 6,21%

	precision	recall	f1-score	support
0	0.9998	0.9771	0.9883	71079
1	0.0622	0.8780	0.1163	123
accuracy			0.9769	71202
macro avg	0.5310	0.9276	0.5523	71202
weighted avg	0.9982	0.9769	0.9868	71202

AUC = 0.9276

Figura 7. Resumo da classificação

Dando continuidade, será apresentada a construção do modelo de Árvores de Decisão utilizando o ADASYN. Na figura 8, observa-se que a quantidade de falsos negativos (FN) não está perto de ser nem a maior e nem a menor em comparação aos modelos anteriores, a quantidade de fraudes ficou equilibrada e assim como o modelo de Regressão Logística - ADASYN, o modelo atual possui um ponto negativo referente a quantidade de falsos positivos (FP).

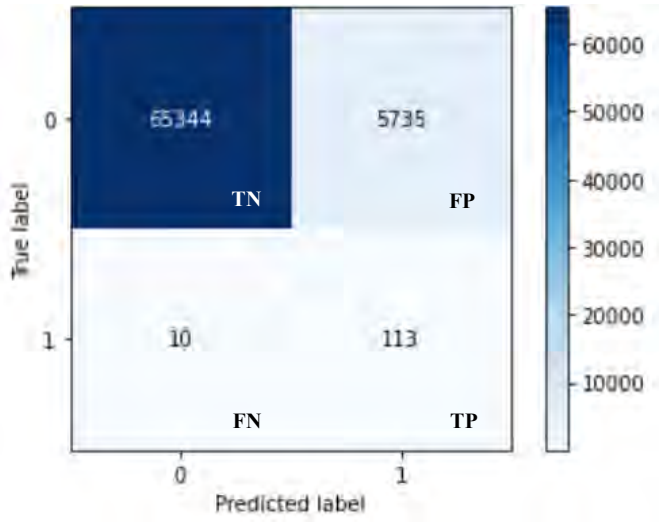

Figura 8. Matriz de Confusão – Árvores de Decisão com ADASYN

De acordo com o a figura 9, o modelo obteve uma acurácia de 0,9193.

	precision	recall	f1-score	support
0	0.9998	0.9193	0.9579	71079
1	0.0193	0.9187	0.0378	123
accuracy			0.9193	71202
macro avg	0.5096	0.9190	0.4979	71202
weighted avg	0.9982	0.9193	0.9563	71202

AUC = 0.9190

Figura 9. Resumo da classificação

A seguir, será apresentada a construção do modelo de Árvores de Decisão utilizando o SMOTE. Na figura 10, observa-se que a quantidade de falsos negativos (FN) teve um aumento em comparação com os modelos anteriores, a quantidade de fraudes previstas teve uma pequena queda.

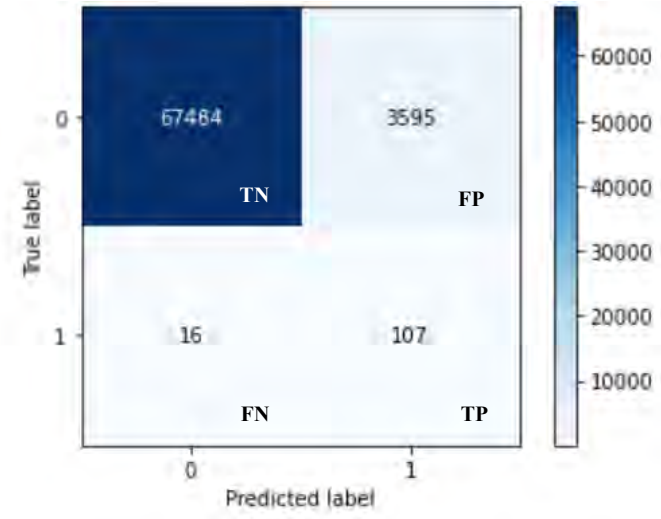

Figura 10. Matriz de Confusão – Árvores de Decisão com SMOTE

O modelo atual obteve um considerável AUC de 0,9097 porém não um dos melhores.

	precision	recall	f1-score	support
0	0.9998	0.9494	0.9739	71079
1	0.0289	0.8699	0.0559	123
accuracy			0.9493	71202
macro avg	0.5143	0.9097	0.5149	71202
weighted avg	0.9981	0.9493	0.9724	71202

AUC = 0.9097

Figura 11. Resumo da classificação

Durante o desenvolvimento deste artigo, foi possível notar que este conjunto de dados é um pouco diferente dos outros. Ele possui muitas variáveis não identificáveis que podem dificultar o desenvolvimento, não possui valores nulos e não teve a necessidade de uma limpeza de dados. Por outro lado, a base possuía um desbalanceamento muito notável em que foi necessário o tratamento.

5. Conclusões e recomendações

O desenvolvimento do presente estudo possibilitou uma análise de como é possível identificar fraudes a partir de uma base de transações de cartão de crédito e como isso pode ajudar uma empresa que deseja controlar suas transações e evitar prejuízos.

Com base no desenvolvimento do modelo de machine learning foi possível identificar que o algoritmo obteve a melhor quantidade de fraudes foi a Regressão Logística utilizando dados balanceados com o método ADASYN obtendo 91% de acurácia, mas com um dos melhores resultados na quantidade de casos positivos de fraude identificados de 114.

A escolha do conjunto de dados utilizada no presente trabalho impactou em certas limitações, que de acordo com a descrição do conjunto de dados (Credit Card Fraud Detection, 2018) devido a questões de confidencialidade, não foi possível fornecer os recursos originais e mais informações básicas sobre os dados.

Em pesquisas futuras, propõe-se um novo conjunto de dados que possua mais variáveis que possam ser utilizadas para identificação de fraude e outros métodos para enriquecimento do estudo. Tais exercícios demonstrariam a real eficácia da implantação de modelos de machine learning para identificação de fraude em conjunto de dados de transações de cartões de crédito.

Referências

ADYEN; Chargeback: o pesadelo de qualquer empresa, nov. 2021. Disponível em: <https://www.adyen.com/pt_BR/blog/chargeback-pesadelo-qualquer-empresa>. Acesso em: 02 de novembro de 2021.

AMARASINGHE, Thushara; APONSO, Achala; KRISHNARAJAH, Naomi. Critical Analysis of Machine Learning Based Approaches for Fraud Detection in Financial Transactions. Proceedings Of The 2018 International Conference On Machine Learning Technologies – Icmlt'18, [s.l.], p.12-17, 2018. ACM Press. http://dx.doi.org/10.1145/3231884.3231894. Disponível em: <http://doi.acm.org/10.1145/3231884.3231894>. Acesso em: 15 de maio de 2021.

BEHERA, Tanmay Kumar; PANIGRAHI, Suvasini. Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering & Neural Network. 2015 Second International Conference On Advances In Computing And Communication Engineering, [s.l.], p.494-499, maio 2015. IEEE. http://dx.doi.org/10.1109/icacce.2015.33.

BMC NEWS; E-commerce pode perder R$ 7 bilhões por falhas no combate à fraude, revela pesquisa, jul. 2021. Disponível em: <https://www.bmcnews.com.br/2021/07/27/e-commerce-pode-perder-r-7-bilhoes-por-falhas-no-combate-a-fraude-revela-pesquisa/>. Acesso em: 30 de novembro de 2021.

CLEARSALE; Fraude: entenda que é e saiba quais são os principais tipos, maio. 2021. Disponível em: <https://blogbr.clear.sale/fraude-no-e-commerce-entenda-este-fenmeno-e-saiba-quais-s-o-os-principais-tipos>. Acesso em: 25 de novembro de 2021.

EUGÊNIO, Marcio. E-commerce no Brasil perfil do mercado e do e-consumidor. 2016. Disponível em: <https://www.e-commerce.org.br/e-commerce-no-brasil-perfil-do-mercado-e-do-e-consumidor-2/>. Acesso em: 16 maio 2021.

FREITAS, Vitor Hugo. Violação de dados pessoais e o princípio da eficiência: Um diálogo entre o público e o privado. 2014. Disponível em: < http://publicadireito.com.br/artigos/?cod=ffb5597397de30f2>. Acesso em: 16 de maio de 2021.

JUNIOR, J. C. P.; Modelos para detecção de fraudes utilizando técnicas de aprendizado de máquina, 2019. Disponível em: <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/27166/Dissertacao_Joao_Carlos_Pacheco_VFinal_2.pdf>. Acesso em: 04 de dezembro de 2021.

KAGGLE; Credit Card Fraud Detection, 2018. Disponível em: < https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud?datasetId=310&searchQuery=detec%C3%A7%C3%A3>. Acesso em: 13 de março de 2022.

OLIVEIRA, P. H. M. A.; Detecção de fraudes em cartões: um classificador baseado em regras de associação regressão logística, 2016. Disponível em: <https://www.teses.usp.br/teses/disponiveis/45/45134/tde-01022016-204144/publico/Paulo_Oliveira_Mestrado_PPGCC.pdf>. Acesso em 04 de dezembro de 2021.

OMAR, Sinayobye Janvier; FRED, Kiwanuka; SWAIB, Kaawaase Kyanda. A state-of-the-art review of machine learning techniques for fraud detection research. Proceedings Of The 2018 International Conference On Software Engineering In Africa - Seia '18, [s.l.], p.11-19, 2018. ACM Press. http://dx.doi.org/10.1145/3195528.3195534.

PANT, Ayush. Introduction to Logistic Regression. 2019. Disponível em: < https://towardsdatascience.com/introduction-to-logistic-regression-66248243c148>. Acesso em: 10 de maio 2022.

PATEL, Vaishali Rajeev; MEHTA, Rupa G.. Performance analysis of MK-means clustering algorithm with normalization approach. 2011 World Congress On Information And Communication Technologies, Mumbai, p.974-979, dez. 2011. IEEE. http://dx.doi.org/10.1109/wict.2011.6141380. Disponível em: <https://ieeexplore.ieee.org/abstract/document/6141380/>. Acesso em: 15 de maio 2021.

PEREIRA, V. F.; SANTOS A. das N.; ROCHA L. F. Da. Procedimentos de prevenção de fraude contábil numa empresa de comércio exterior. UFSC, 2014.

SACRAMENTO, Gabriel; Árvore de Decisão: Entenda esse algoritmo de machine learing, jul. 2021. Disponível em: < https://blog.somostera.com/data-science/arvores-de-decisao#:~:text=Uma%20%C3%A1rvore%20de%20decis%C3%A3o%20%C3%A9,valor%20do%20lucro%20em%20reais).>. Acesso em: 14 de maio de 2022.

SCKIT-LEARN; Preprocessing data, c2007-2022. Disponível em: < https://scikit-learn.org/stable/modules/preprocessing.html#standardization-or-mean-removal-and-variance-scaling>. Acesso em: 06 de junho de 2022.

SHERLY, K. K.; NEDUNCHEZHIAN, R. BOAT adaptive credit card fraud detection system. 2010 Ieee International Conference On Computational Intelligence And Computing Research, [s.l.], p.1-7, dez. 2010. IEEE. http://dx.doi.org/10.1109/iccic.2010.5705824.

TIBCO; Whats is logistic regression. Disponível em: < https://www.tibco.com/pt-br/reference-center/what-is-logistic-regression#:~:text=A%20regress%C3%A3o%20log%C3%ADstica%20%C3%A9%20um,ajudar%20a%20criar%20previs%C3%B5es%20precisas.>. Acesso em: 10 de maio de 2022.

TREVOR, H.; ROBERT, T.; JH, F. The elements of statistical learning: data mining, inference, and prediction. [S.l.]: New York, NY: Springer, 2009.