REVISTA TÓPICOS

TÉCNICAS DE MINERAÇÃO DE DADOS PARA IDENTIFICAR PADRÕES SUSPEITOS EM TRANSAÇÕES FINANCEIRAS

DOI: 10.5281/zenodo.12539998

João Ricardo Socca Junior[1]

RESUMO

Com o rápido crescimento tecnológico, as compras online se tornaram indispensáveis, oferecendo praticidade à população. No entanto, esse aumento também resultou no crescimento significativo de fraudes. O combate de atividades fraudulentas é uma realidade na qual os fundadores de plataformas têm aprimorado cada vez mais suas táticas, e as empresas, por sua vez, buscam adotar abordagens proativas e avançadas para manter a integridade das transações online. Este projeto tem como objetivo não apenas compreender os diferentes tipos de fraudes, mas também analisar seus riscos inerentes. A ideia desse projeto visa compreender os diferentes tipos de fraudes, analisar seus riscos e desenvolver métodos de detecção eficazes usando técnicas de Machine Learning. Isso é crucial, pois as empresas precisam adotar abordagens avançadas para prever e combater ataques fraudulentos, garantindo transações online mais seguras e confiáveis.

Palavras-chave:Machine Learning; Cartão de crédito; Fraudes.

ABSTRACT

With the rapid technological growth, online shopping has become indispensable, offering convenience to the population. However, this increase has also led to a significant rise in fraud. The combat against fraudulent activities is a reality in which platform founders continuously refine their tactics, and companies, in turn, strive to adopt proactive and advanced approaches to maintain the integrity of online transactions. This project aims not only to comprehend the different types of fraud but also to analyze their inherent risks. The concept of this project is to understand the various forms of fraud, assess their risks, and develop effective detection methods using Machine Learning techniques. This is crucial as companies need to embrace advanced approaches to predict and combat fraudulent attacks, ensuring safer and more reliable online transactions.

Keywords: Machine learning; Credit card; Fraud.

1 Introdução

Com a constante evolução tecnológica, a transformação digital tem proporcionado praticidade e eficácia no cotidiano de pessoas e empresas. No entanto, a criatividade dos criminosos também tem aumentado, se aproveitando da vulnerabilidade de sistemas para aplicar golpes online. A segurança em ambientes comerciais se torna crucial para preservar a confiabilidade das empresas e mitigar os riscos associados (GUIMARÃES, 2022).

No contexto do comércio eletrônico, os atos fraudulentos podem envolver uma variedade de práticas, como compras não autorizadas por usuários

legítimos, clonagem de cartões de crédito, formação de cartéis para manipulação de preços por parte dos comerciantes, roubo de contas de usuários, uso indevido de sites, entre outros. Essas atividades prejudicam a confiança dos consumidores, afetam a integridade das transações e demandam medidas robustas de segurança, incluindo a utilização de tecnologias avançadas de detecção de fraudes e a implementação de políticas rigorosas para prevenção e combate a essas práticas ilícitas (MATTOS, 2022).

As técnicas de Machine Learning (ML) têm se destacado como uma abordagem crucial na detecção de padrões em dados, possibilitando a automação de tarefas complexas e a realização de previsões. No contexto de segurança, incluindo a detecção de fraudes no comércio eletrônico, o uso de algoritmos de ML permite a análise de grandes volumes de dados para identificar comportamentos suspeitos ou padrões não usuais. Essa capacidade de adaptação e aprendizado contínuo torna o ML um diferencial significativo em diversas áreas, incluindo a segurança cibernética, contribuindo para a eficácia na detecção e prevenção de atividades fraudulentas (FREITAS; JUNIOR, 2019).

O trabalho menciona a aplicação da técnica de Mineração de Dados, com ênfase na detecção de fraudes em pagamentos online no Brasil, citando trabalhos anteriores como (JUNIOR, 2018) e (JÚNIOR et al., 2012). No contexto específico deste trabalho, se busca utilizar técnicas de ML no processo de Knowledge Discovery in Databases (KDD) para identificar de maneira eficaz e rápida possíveis atividades fraudulentas em pedidos de

pagamentos online. A condução do experimento se dará em um ambiente de teste construído a partir da compilação de dados anônimos, empregando um conjunto de dados públicos como principal fonte de informação.

1.1 Tema

Esse trabalho tem como objetivo principal desenvolver métodos de detecção eficazes, usando técnicas de Machine Learning para prevenir fraudes bancárias.

A Seção 1 aborda conceitos relacionados a fraudes, apresentando o tema, o problema, os objetivos (geral e específicos) e a justificativa do problema. A Seção 2 tem o referencial teórico, explorando trabalhos similares que utilizam modelos de ML na detecção de fraudes. Na Seção 3, se detalha o procedimento metodológico adotado. Por fim, a Seção 4 apresenta o cronograma do estudo desenvolvido.

1.2 Problema

Um dos maiores desafios ao identificar padrões suspeitos em transações financeiras por meio de técnicas de Machine Learning é a constante evolução das táticas de fraude. Os fraudadores são ágeis em ajustar e modificar suas abordagens para evitar detecção. Além disso, a presença de dados desbalanceados pode ser um problema. Muitas vezes, transações fraudulentas representam uma pequena parcela do conjunto de dados total. Isso pode levar o modelo a ser viésado em direção às transações normais,

dificultando a identificação de padrões relacionados a atividades fraudulentas.

1.3 Objetivos

Tem como objetivo realizar o uso de técnicas de machine learning na identificação de padrões suspeitos em transações financeiras, visando a minimização de falsos positivos, e estabelecer um ciclo de melhoria contínua para enfrentar os desafios em constante evolução do cenário de segurança financeira. Deste modo, os modelos de máquina serão postos em prática sobre um conjunto de dados para observar o grau de aprendizado sob seu respectivo treinamento, para então obter uma validação adequada que possibilite ajudar a aplicação destes métodos no mercado financeiro com mais eficiência.

1.3.1 Objetivo geral

O objetivo geral deste estudo é aplicar e avaliar técnicas de mineração de dados para a identificação de padrões suspeitos em transações financeiras. A pesquisa visa aprimorar a detecção de atividades fraudulentas por meio da análise de dados transacionais, contribuindo para o aprimoramento dos sistemas de segurança e prevenção de fraudes no setor financeiro.

1.3.2 Objetivos específicos

- Escolher técnicas de mineração de dados, incluindo algoritmos e pré-processamento, para analisar transações financeiras;

- Coletar e preparar dados de transações financeiras garantindo qualidade e relevância para análises;
- Comparar a confiabilidade entre modelos;
- Demonstrar a eficiência de modelos para tipos de fraudes distintas;

1.4 Justificativa

A detecção de fraudes em transações financeiras é uma preocupação crucial para instituições e usuários. Devido ao crescente volume de dados, a aplicação de técnicas de mineração de dados se torna essencial. A justificativa desse trabalho visa desenvolver e aprimorar métodos que possam identificar padrões suspeitos, contribuindo para a segurança e integridade das operações financeiras, buscando fornecer insights valiosos e ferramentas práticas para combater atividades fraudulentas.

O desafio contínuo é que essas ameaças se tornam cada dia mais complexas, devido à constante evolução de ataques. A utilização de modelos eficientes de aprendizado de máquina é um passo importante para se identificar transações fraudulentas. Além de reduzir prejuízos financeiros, esses modelos fortalecem a recuperação de valores e minimizam o risco de danos à reputação da instituição. Esse enfoque não apenas protege os interesses financeiros, mas contribui para a construção e manutenção de relações sólidas com os clientes.

2 Fundamentação Teórica

Nesta seção, é apresentado o embasamento teórico fundamental usado com base no princípio do contexto das fraudes, conduzindo um estudo comparativo entre os modelos de aprendizado. A Seção 2.1 contextualiza as fraudes bancárias, enquanto a Seção 2.2 aborda os modelos eficientes de machine learning no cenário financeiro. Na Seção 2.3, destaca os tipos de algoritmos que são detalhados em subseções, seguindo a seguinte ordem: Árvores de Decisão, Support Vector Machine e Naive Bayes.

2.1 Fraudes Bancárias

A fraude possui impactos tanto sociais quanto financeiros. Para as instituições, implica em custos que incluem as perdas financeiras decorrentes da transação fraudulenta e também os investimentos em análises. Desde o desenvolvimento e implementação de modelos eficazes até verificações manuais, quando necessárias. Além disso, há consequências intangíveis, como danos à reputação e insatisfação do cliente, os quais são difíceis de serem mensurados (PICCIN, 2022).

No Brasil, estima-se a ocorrência de 7 fraudes por minuto, gerando um impacto anual estimado em 3,6 bilhões de reais. No geral, estima-se que 1,34% das transações realizadas englobam algum tipo de tentativa de fraude. Esse percentual é maior em algumas regiões do país, como no Norte, chegando a 3,5% das transações. Além disso, existe também uma concentração de fraude através de aparelhos de smartphones, sendo 4,24% das principais tentativas de fraudes, devido a sua alta procura no mercado e a facilidade de revenda (CRISTOVÃO; BUSCAGLIA, 2022).

2.2 Utilização de modelos de maquinas para detecção

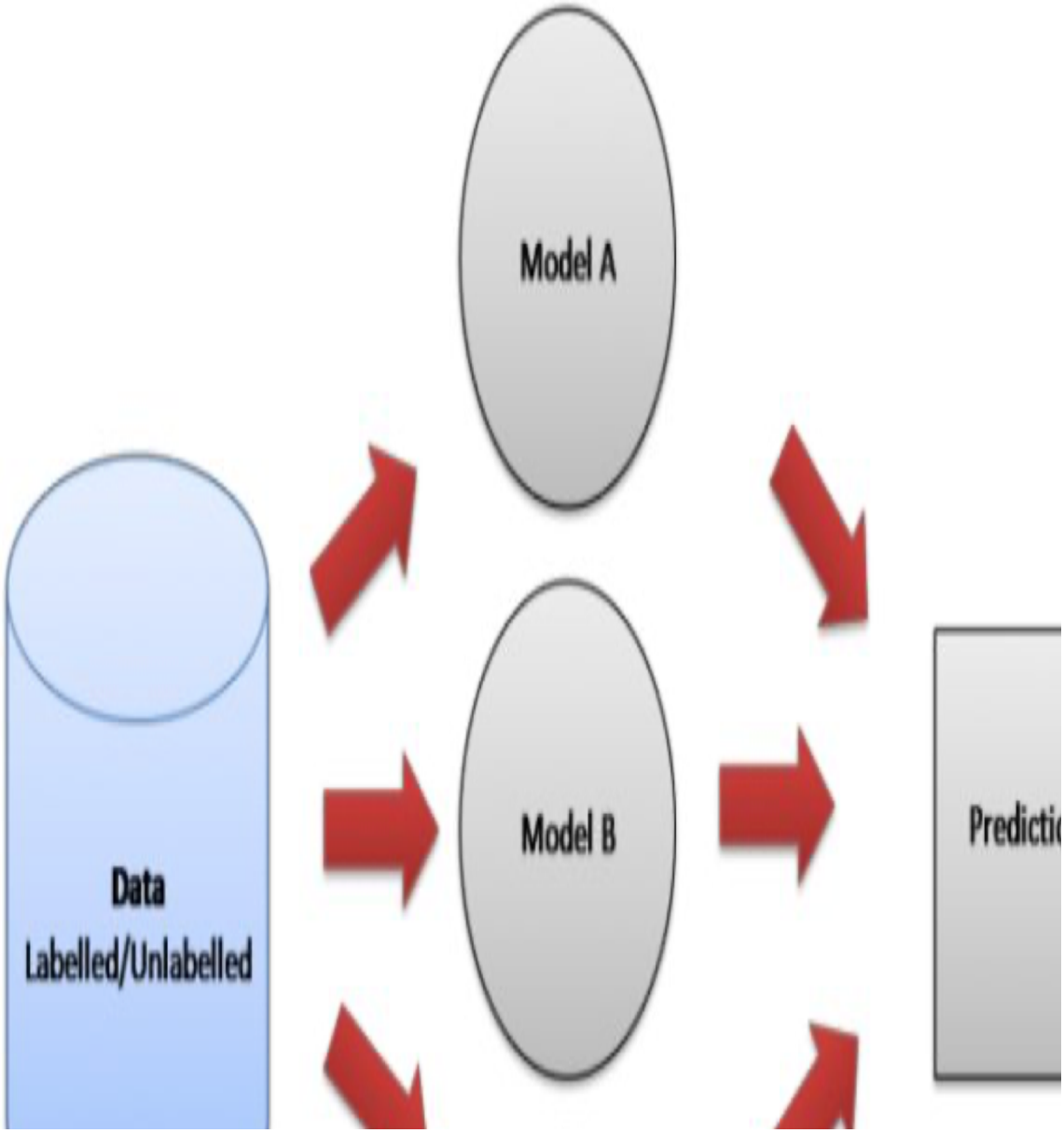
O treinamento de modelos de aprendizado de máquina para a detecção de fraudes em um conjunto de dados, denominado de Dataset, representa a capacidade de aprender padrões em transações bancárias. O modelo de aprendizado M1, é treinado inicialmente, e o modelo de aprendizado M2, é introduzido e treinado no mesmo conjunto de dados. A comparação de seus desempenhos ao serem aplicados ao conjunto de dados permite avaliar suas habilidades na detecção de fraudes. Os resultados podem indicar se M2 superou M1, ou se ambos possuem mesmo desempenho ou se M1 permanece superior. Essa comparação reflete a dinâmica de treinamento e avaliação de modelos de aprendizado de máquina em busca do melhor desempenho na detecção de fraudes (PICCIN, 2022).

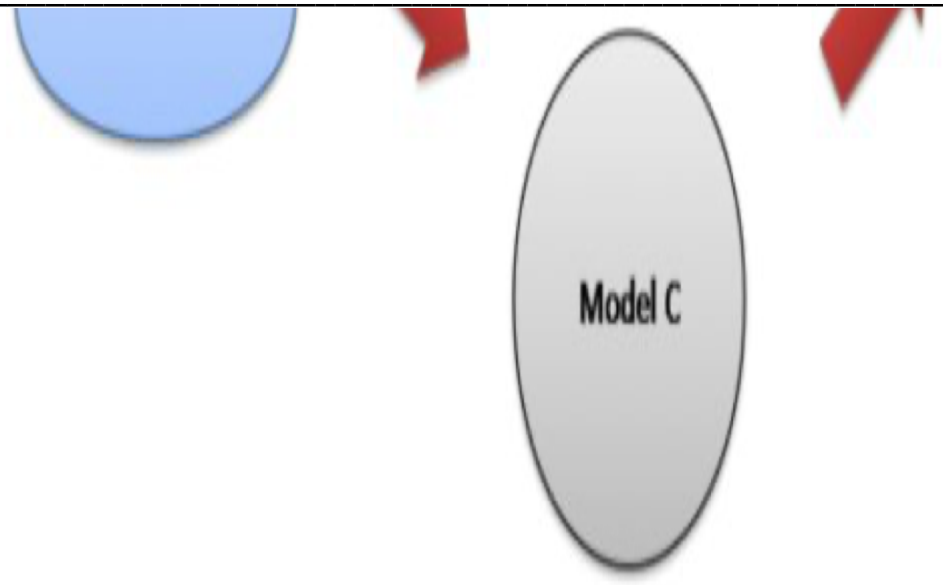
Para enriquecer a análise e aprimorar a eficácia do processo, a comparação de resultados e a extração de conhecimento são essenciais, uma vez que, conforme destacado por (HAYKIN, 2001), o conhecimento pode e deve ser adquirido a partir do ambiente através de um processo de aprendizagem. Embora os modelos estejam em operação constante, desafios como a detecção de fraudes persistem ativamente. A complexidade desse cenário demanda uma abordagem adaptativa, pois não há uma técnica de aprendizado de máquina infalível, pois cada técnica se destaca conforme as características específicas da base de dados (PÁSCOA, 2018).

Segundo (ZHANG; MA, 2012), para otimizar a confiabilidade dos resultados e avaliar sua precisão por meio da métrica accuracy denominada de precisão para identificar eventos. A busca por eficiência e alta precisão

em algoritmos é crucial na resolução de problemas, onde cada método de aprendizado individual desempenha um papel essencial, conforme a Figura 1.

Figura 1 – Agrupamento de métodos de alta predição.





Fonte: Experimentos de laboratórios.

2.3 Classificação supervisionada

O processo de aprendizagem supervisionada se desenrola em duas fases distintas, na fase inicial ocorre a aprendizagem propriamente dita, na qual a máquina aprende, e na segunda fase, essa máquina age sobre um conjunto de dados, realizando a classificação com base nos princípios dos modelos de Machine Learning. Durante o aprendizado, a máquina utiliza um conjunto de dados como referência, em seguida os classifica em categorias específicas. Os métodos de classificação, então, se materializam como ações, conhecidas como regras classificatórias, com o objetivo de separar os dados em categorias que melhor se alinham no intuito de prever resultados por meio de saídas discretas. Esse ciclo de aprendizado e classificação é fundamental para a eficácia do modelo em antecipar resultados (SOUSA, 2021).

2.3.1 Modelos de Aprendizado de Máquina

O Aprendizado de Máquina (AM) representa um conjunto de métodos computacionais que utilizam conhecimento disponível para otimizar o desempenho em tarefas específicas e aprimorar previsões em problemas diversos (MOHRI; ROSTAMIZADEH; TALWALKAR, 2012).

Enquadrado como uma subcategoria da inteligência artificial, o ML tem como objetivo principal observar dados para identificar padrões e, com base nessas observações, gerar métodos eficazes na resolução de problemas (AMARAL, 2016). No contexto dos algoritmos de AM, termos essenciais incluem objetos, que são instâncias de dados e atributos que são características que definem cada objeto. E os rótulos, que representam categorias atribuídas aos objetos, sendo relevantes em problemas de classificação (CRISTOVÃO; BUSCAGLIA, 2022).

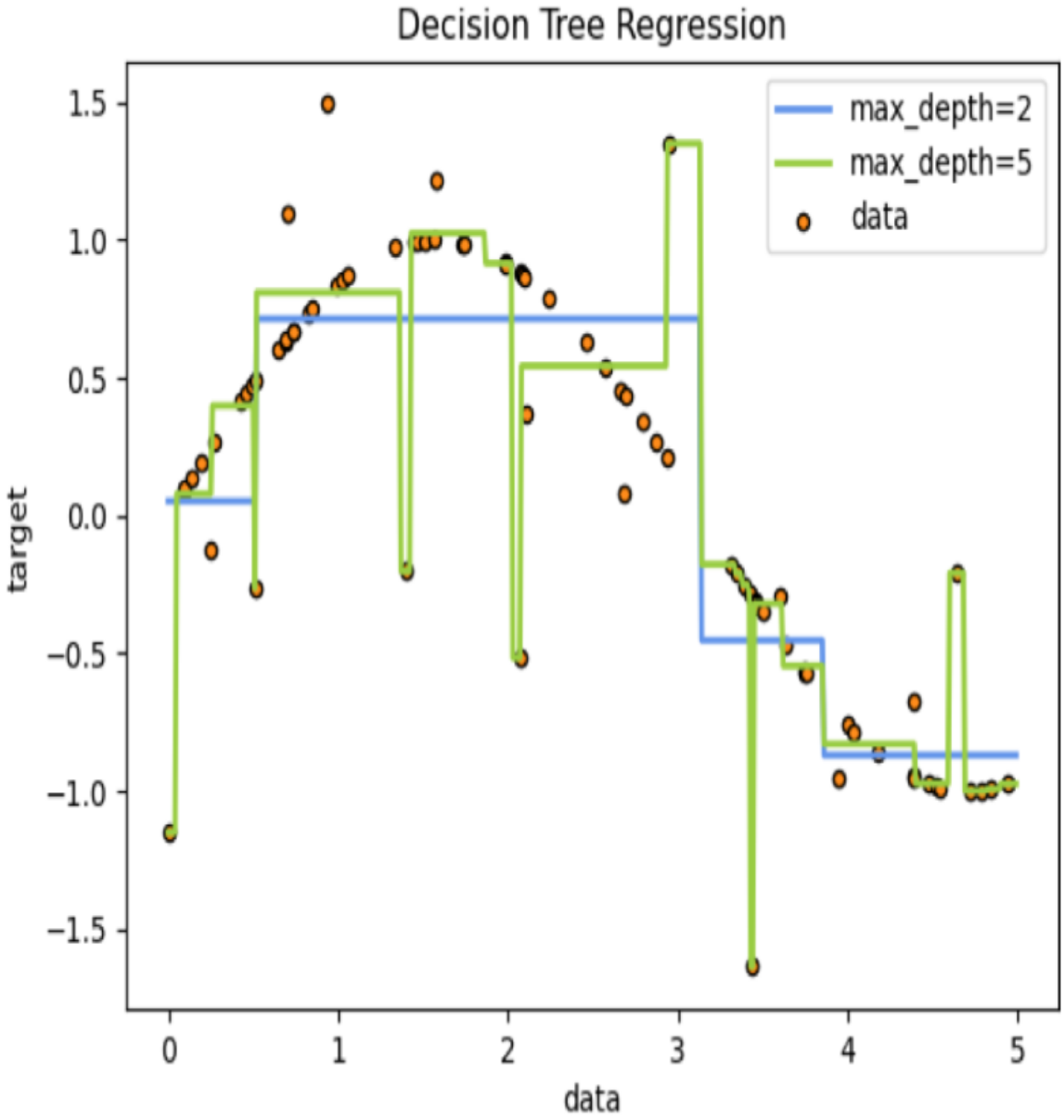
2.3.2 Árvores de Decisão

O algoritmo de Árvores de Decisão, destacado neste estudo, é estruturado em um conjunto de nós diferenciados pela raiz, estabelecendo uma relação hierárquica denominada "paternidade", o que confere eficiência ao processo de aprendizado. Amplamente utilizado na análise de descrições com níveis de complexidade, sua aplicação é se estabelece entre custo e benefício, bem como pela probabilidade durante e após o treinamento (PICCIN, 2022).

Reconhecido como um modelo de inferência intuitiva devido a sua simplicidade, as arvores de decisão durante o treinamento atua com base

em um conjunto de dados predefinidos, que se ramifica caso necessário, e que ao se expandir, o conjunto passa por sucessivas divisões até atingir uma condição de parada satisfatória, aplicando a estratégia "dividir para conquistar". Essa abordagem resulta na criação de subclasses que aprimoram tanto o treinamento quanto o processo de decisão, visando minimizar o erro, interferindo o mínimo possível em suas predições (GAMA et al., 2004), conforme ilustrado na Figura 2 abaixo.

Figura 2 – Visualização usando Árvores de Decisão.



Fonte: Scikit-learn: machine learning in python, 2024.

Os algoritmos de árvores de decisão são empregados em técnicas de machine learning para a detecção de transações bancárias suspeitas. Esses

algoritmos formam uma estrutura de árvore com base nos dados de treinamento, representando o conhecimento adquirido. A estrutura da árvore é então utilizada para classificar transações, distinguindo entre aquelas consideradas normais e as que levantam suspeitas (LIMA, 2023). Nesse contexto, Bhattacharyya et al. (2011) afirma que os nós de decisão na árvore podem representar testes relacionados a diferentes atributos das transações, como valores, padrões de gastos, localização geográfica, entre outros. As arestas conectadas a esses nós refletem os resultados desses testes, enquanto os nós folha indicam a classificação final da transação, se é suspeita ou não.

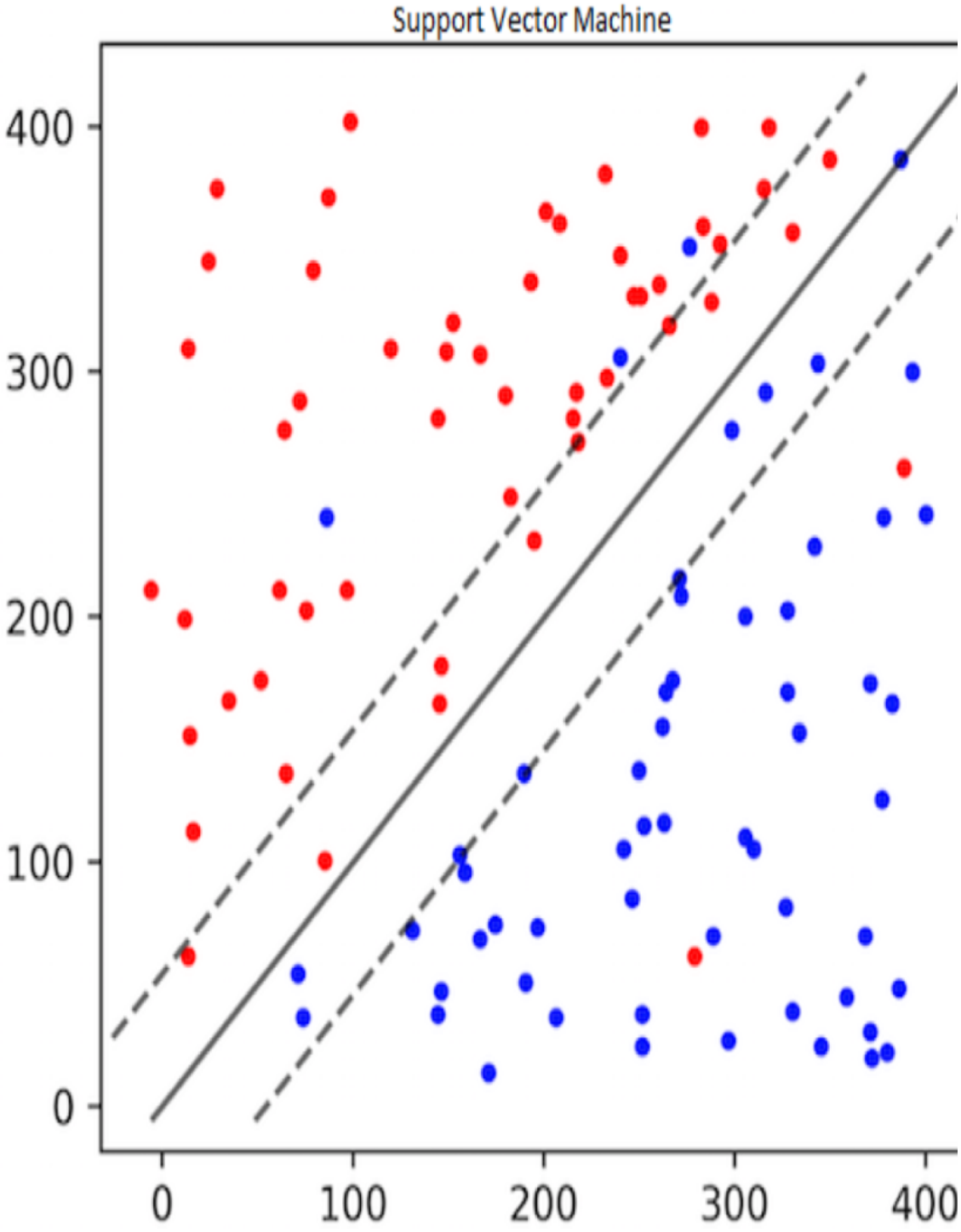
2.3.3 Support Vector Machine (SVM)

O SVM (Support Vector Machine), incialmente proposto por (CORTES; VAPNIK, 1995), se destaca como uma abordagem versátil para desafios de classificação ou regressão, visando mitigar incertezas associadas a erros no conjunto de testes durante o aprendizado. Diferenciando de modelos mais generalistas, como Redes Neurais, o SVM foi concebido como um modelo robusto, fundamentado no estudo da probabilidade e na busca de minimizar erros durante a separação. Este algoritmo de classificação aproxima as margens de uma instância a ser classificada com as instâncias mais próximas, proporcionando uma visualização dos pontos em um plano através de retas de vetores de suporte, conforme exposto por (AMARAL, 2016).

O Support Vector Machine (SVM) é um método de classificação adequado para problemas linearmente separáveis, onde as classes podem ser

delimitadas por uma fronteira linear. No entanto, mesmo em conjuntos de dados não linearmente separáveis, o SVM pode ser aplicado utilizando a técnica conhecida como kernel trick de acordo com (KOWALCZYK, 2017), e conforme pode ser visualizada através da Figura 3.

Figura 3 – Visualização usando Vetores de Suporte


Support Vector Machine
400
300
200
100
0
0
100
200
300
400

Fonte: Scikit-learn: machine learning in python, 2024.

O SVM (Support Vector Machine), apresentam sensibilidade a ruídos e outliers, podendo ocorrer sobreajuste aos dados de treinamento. Para lidar com essa limitação, o SVM oferece a calibração de parâmetros de "folga", permitindo a desconsideração de observações discrepantes. Isso significa que o SVM pode tolerar a classificação incorreta de algumas amostras indesejáveis, proporcionando maior robustez ao modelo (LIMA, 2023).

2.3.4 Classificação Naive Bayes

O modelo de Naive Bayes (NB), concebido pelo matemático Thomas Bayes, representa uma abordagem de aprendizado supervisionado baseada em algoritmos que se destacam na classificação por probabilidade, superando sua designação de "ingênuo". Demonstrando eficácia em aplicações do mundo real, com base na aproximação da probabilidade (SOUSA, 2021).

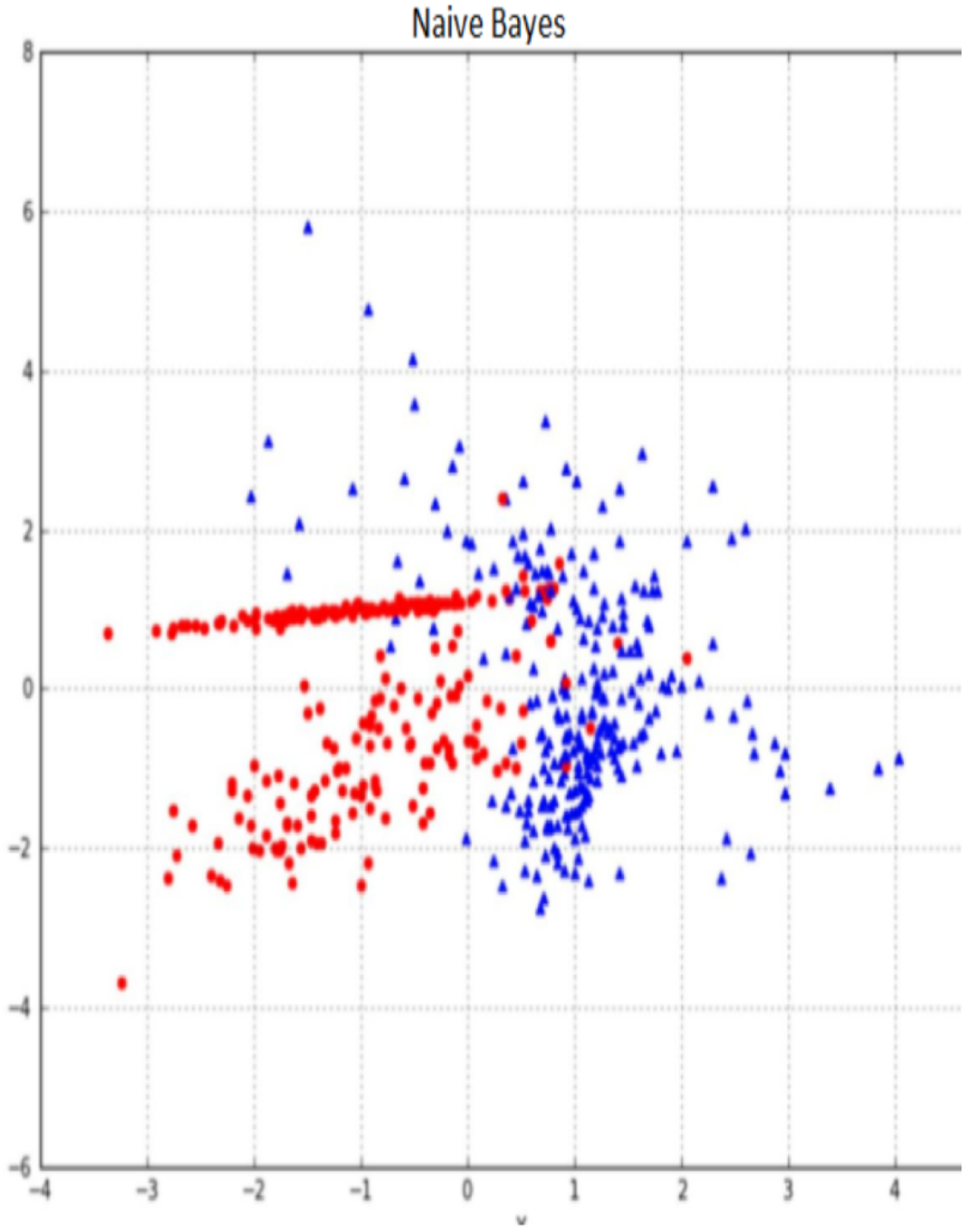
Sousa (2021) ainda afirma que o método opera com base em probabilidades condicionais e na regra de Bayes, permitindo a manipulação de probabilidades para tomar decisões ótimas com base nos dados observados. Considerando um cenário prático, como a detecção de fraudes em uma instituição bancária, o modelo Naive Bayes se destaca ao induzir, de forma probabilística, a classificação de novas características.

De acordo com Benz (2017), durante a fase de teste, o modelo recebe uma nova transação e calcula a probabilidade. A transação é então atribuída à

classe com a maior probabilidade, e dessa forma consegue detectar transações suspeitas, e assim, identificar as probabilidades mais altas de serem consideradas suspeitas.

O processo de classificação envolve treinar o modelo com um conjunto de dados rotulados, onde transações são marcadas como normais ou suspeitas. O modelo utiliza as características dessas transações para calcular as probabilidades condicionais e estima a probabilidade de uma transação ser suspeita ou normal (BENZ, 2017), conforme ilustrado na Figura 4.

Figura 4 – Visualização usando Naive Bayes


Naive Bayes
8
6
4
2
0
−2
−4
−6
−4
−3
−2
−1
0
1
2
3
4

Fonte: Scikit-learn: machine learning in python, 2024.

Nesse contexto, considerando um conjunto de atributos X e uma variável de classe Y, caso haja uma relação não determinística entre eles, indicando independência dos atributos em X, é possível tratar X e Y como variáveis aleatórias. Assim, pode-se modelar probabilisticamente o relacionamento entre eles usando a probabilidade condicional P(Y|X). Essa probabilidade condicional é também chamada de probabilidade posterior de Y, em contraste com sua probabilidade anterior P(Y) (BENZ, 2017).

De acordo com Júnior et al. (2012), na fase de treinamento do modelo, as probabi- lidades posteriores P(Y|X) são determinadas para cada combinação de X e Y, utilizando informações coletadas a partir dos dados de treinamento. Com base nessas probabilidades, durante a classificação de um registro de teste X, a classe Y é identificada escolhendo aquela que maximiza a probabilidade posterior, ou seja, P(Y|X).

Conforme destacado por Roza e Pegoraro (2020), o Naive Bayes, apesar de sua simplicidade e eficiência, realiza suposições robustas acerca da independência condicional das características, o que pode nem sempre refletir a realidade. No entanto, em muitos cenários, este método tem demonstrado capacidade de fornecer resultados satisfatórios na detecção de padrões e anomalias em transações bancárias.

3 Resultados Obtidos

A análise desse trabalho culminou na identificação de padrões suspeitos em tran- sações financeiras por meio da aplicação de técnicas de mineração de dados, utilizando Árvores de Decisão, Naive Bayes e Máquinas de Vetores de Suporte (SVM), visando identificar padrões suspeitos em transações financeiras. Utilizando um conjunto de dados representativo, se concentrou na detecção de comportamentos anômalos que poderiam indicar atividades fraudulentas. Os resultados obtidos revelam insights sobre a presença de transações normais e fraudulentas, fornecendo uma base sólida para aprimorar os mecanismos de segurança no setor financeiro.

Para construir os classificadores, foi usado dados transacionais obtidos da plataforma Kaggle, uma comunidade global de cientistas de dados. Esses dados foram aprimorados com abordagens de Machine Learning. O projeto foi realizado por meio da ferramenta do Google Colaboratory, um serviço de nuvem gratuito da Google muito usado por desenvolvedores para efetuar projetos de aprendizado de máquina. A escolha dessa ferramenta se deu devido a sua capacidade de proporcionar um ambiente colaborativo e eficiente. Para abordar a detecção de operações fraudulentas, foram explorados os métodos de Árvores de Decisão, Support Vector Machine (SVM) e Naive Bayes. Essa análise comparativa proporcionou avaliar a eficácia de cada método na identificação de fraudes bancárias, contribuindo para a seleção do modelo mais adequado ao contexto específico do problema.

Para a seleção de recursos, foi descartada a coluna categórica IsFlaggedFraud por representar menos de 0,00% do conjunto total, sendo

assim irrelevante. Uma observação interessante é que as colunas oldbalanceDest e newbalanceOrig, apresentaram saída 0,00 quando há fraude. Pode-se observar também que os dados de fraudes parecem indicar que os fraudadores agem sistematicamente e seguem um padrão com pouca variação ao longo do mês, o que facilita na execução do algoritmo de machine learning e dessa forma ajuda melhorar a taxa de assertividade do modelo.

3.1 Distribuição de Transações

A análise dos dados mostra um DataFrame com 6362620 linhas e 11 colunas usado na realização prática desse trabalho, apresentando normalidade na maioria das transações financeiras (99.87%), indicando que a maior parte das operações é legítima. Por outro lado, apenas 0.13% são identificadas como fraudulentas, mostrando que esse tipo de atividade é pouco usual. Além disso, as tentativas marcadas como transações fraudulentas representam uma parcela quase insignificante, apenas 0.00%. Isso implica que, mesmo sendo poucas, as transações fraudulentas são identificadas com alta precisão por métodos de detecção de padrões e aprendizado de máquina, conseguindo discernir padrões incomuns ou suspeitos nas transações, possibilitando a identificação eficaz de atividades fraudulentas.

Na Tabela 1, exibe os tipos de transações identificadas, e como essa identificação de atividades fraudulentas desempenha um papel na preservação da segurança e confiança nos sistemas financeiros. A implementação de métodos usados para esse trabalho, foram essenciais

para a detecção e obtenção do propósito de reconhecer uma tentativa de fraude. Apesar de a maioria das transações seguir um curso lícito, a manutenção desses dados deve ser constante e indispensável para garantir a integridade do sistema financeiro global.

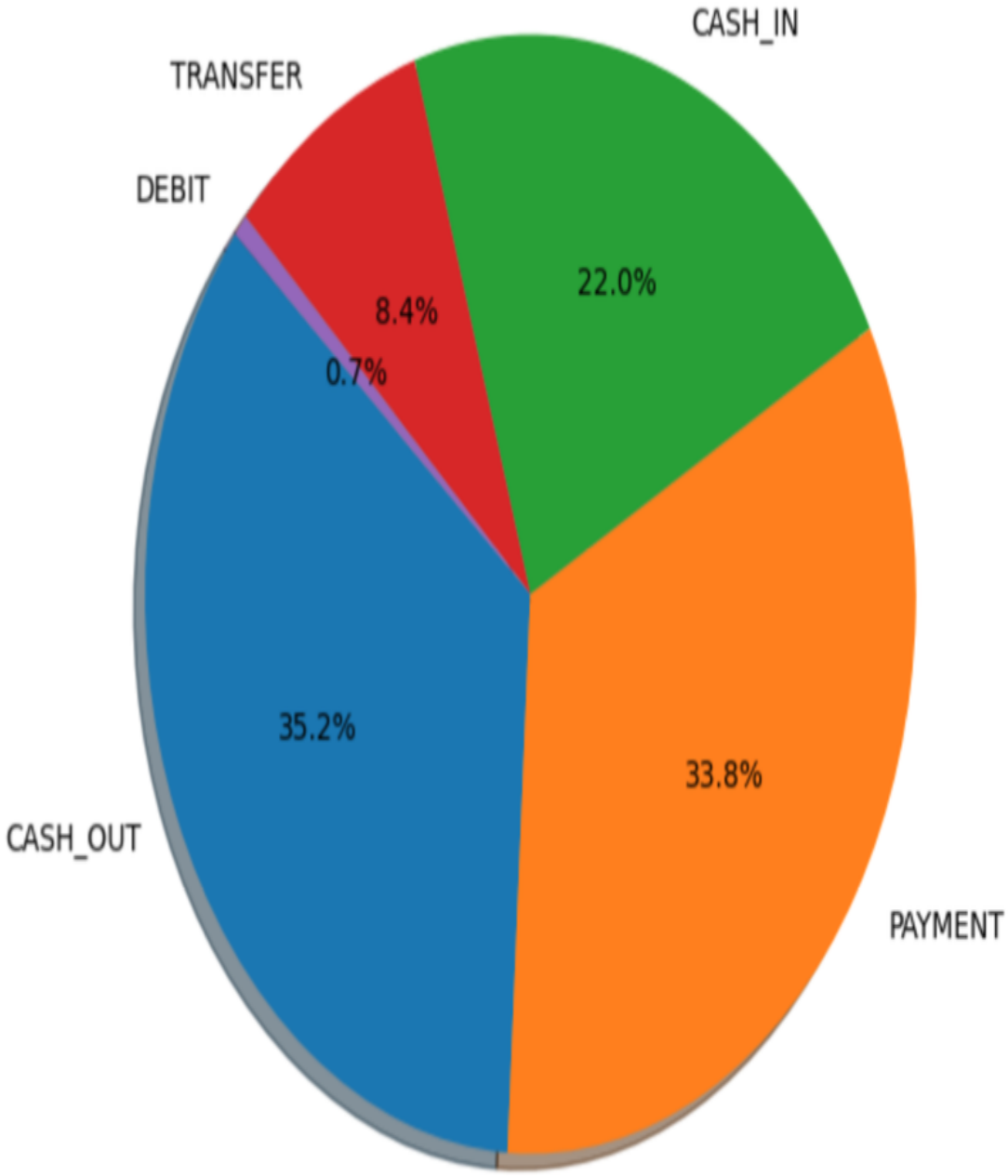
Tabela 1 – Tipos de Transações

Transações	Quantidade	Percentual
Normais	6354407	99.87%
Fraudulentas	8213	0.13%
Tentativas de Fraudes	16	0.00%

Fonte: https://www.kaggle.com/code/anuhskaa/fraud-data-analysis

Na Figura 5 abaixo, exibe os cinco tipos de transações que foram realizadas para o proposito desse trabalho, demonstrando que existe um uso muito maior de 33,2% de saque, seguido de 33,8% de transações de cartão de créditos pelo usuário, 22% em dinheiro, 8,4% por transferência e 0,7% via debito.

Figura 5 – Tipos de Transações

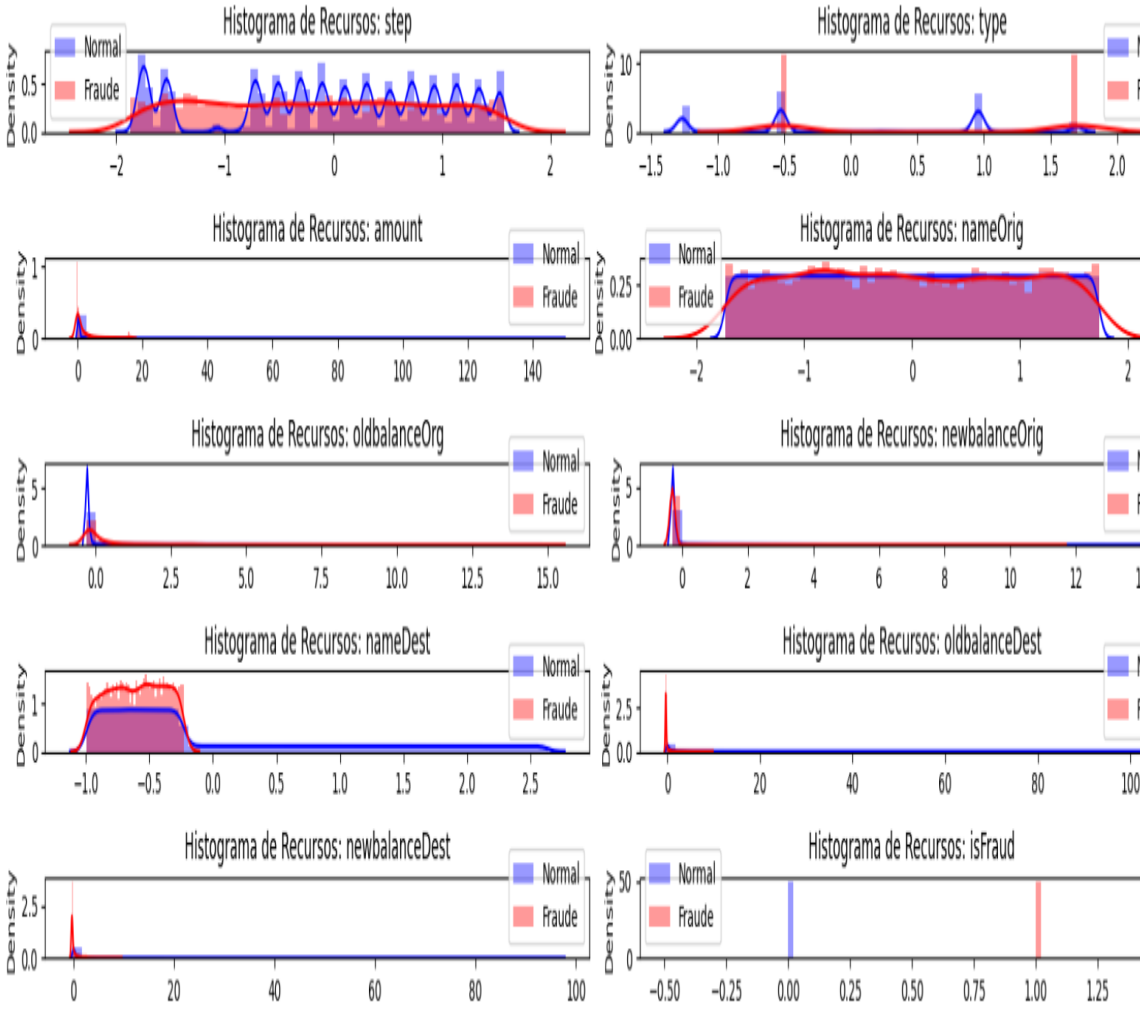


Fonte: Do autor.

A detecção de transações suspeitas é de suma importância para assegurar a integridade financeira, incorporando as técnicas adequadas de Machine Learning (ML) para cada tipo de transação. Para transferências, se analisa históricos para verificar se houve algum tipo de desvio, os débitos foram examinados por meio de detecção de outliers, os saques por sua vez, usa uma abordagem focada na geolocalização, os pagamentos em dinheiro são avaliados agrupamento os dados e as transações com cartão de crédito utilizam modelos preditivos e análise de comportamento do usuário.

Na Figura 6, mostra cada transação suspeita desse trabalho, sendo caracterizada por seus atributos, como o tempo da transação (step), o tipo de transação (type), o valor envolvido na transação (amount), as informações das contas de origem e destino (nameOrig, oldbalanceOrg, newbalanceOrig, nameDest, oldbalanceDest, newbalanceDest). A variável isFraud, assume o valor 1 se a transação é suspeita de fraude e 0 se não é.

Figura 6 – Transações Suspeitas



Fonte: Do autor.

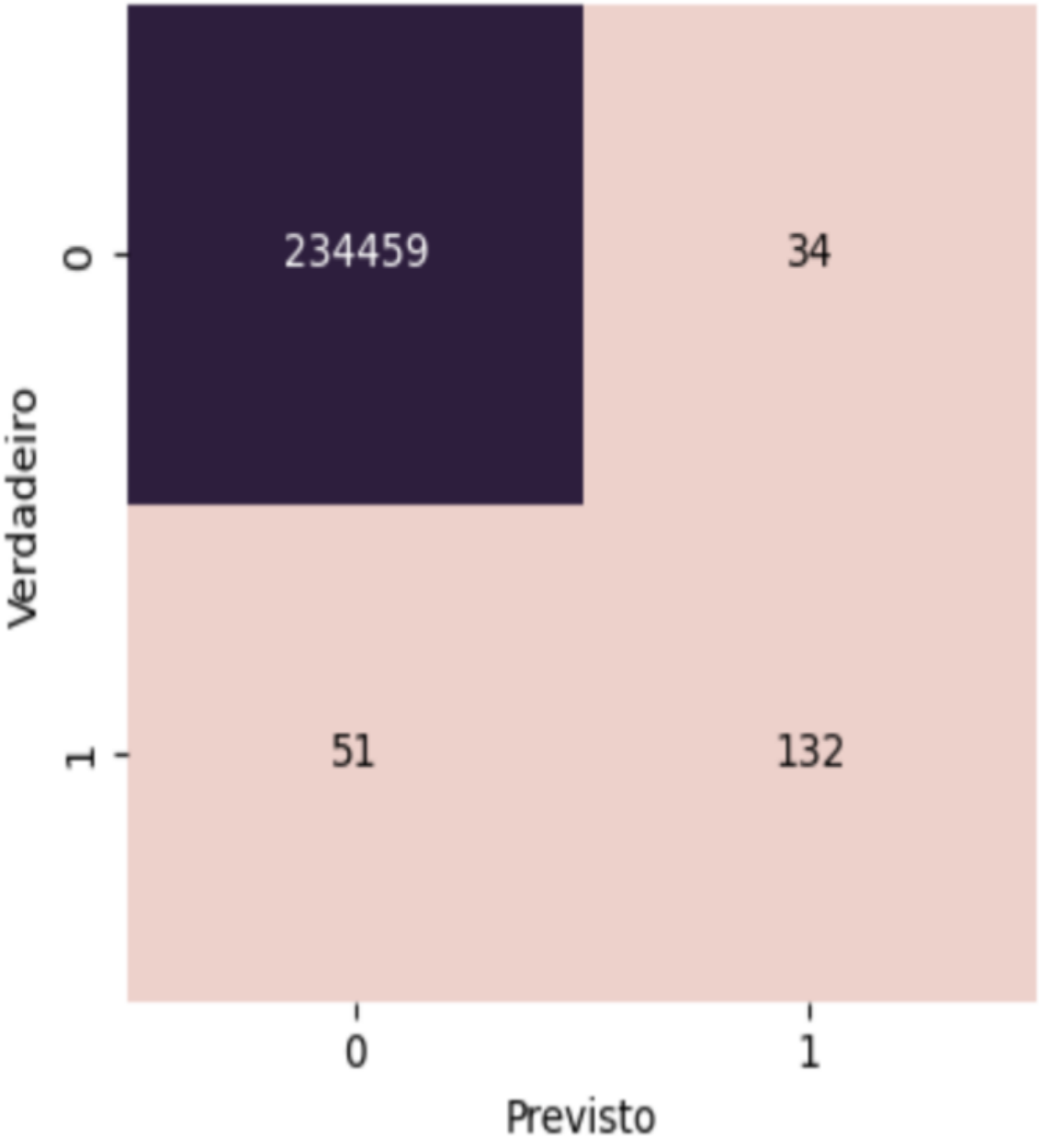
Esses números mostram que a maioria das transações podem ou não serem seguras, e que a detecção de fraudes usando técnicas de machine learning são eficazes, mesmo em casos que não demonstre ser uma ameaça visível, é muito importante usar métodos de aprendizado de maquina com o objetivo de garantir a segurança financeira.

3.1.1 Árvores de Decisão

A aplicação das Árvores de Decisão nesta análise proporcionou insights importantes na detecção de padrões em transações financeiras. Se observou que ao equilibrar a profundidade, foi possível otimizar a precisão por meio de recursos e rótulos do dataframe, removendo colunas irrelevantes e em seguida normalizando esses dados a fim de garantir que sejam capazes de capturar padrões relevantes, sem se ajustar aos detalhes que não agregam aos dados de treinamento. A ideia se baseia em garantir um desempenho robusto e preciso na detecção de padrões em transações financeiras, e evitando o sobreajuste (overfitting), para que não comprometa a generalização do modelo.

A matriz de confusão, de acordo com a Figura 7, facilita a identificação e correção de erros. Ao fornecer informações sobre verdadeiros positivos, falsos positivos, verdadeiros negativos e falsos negativos, a matriz de confusão guia a análise crítica das decisões do modelo em problemas de classificação. Mas também destaca sua eficácia na identificação de instâncias positivas (verdadeiros positivos) e minimiza equívocos (falsos positivos e falsos negativos).

Figura 7 – Matriz de confusão Arvore de Decisão



Fonte: Do autor.

Dessa forma, se observou que a Árvore de Decisão apresentou um desempenho geral muito bom nos seus resultados. Com alta acurácia e

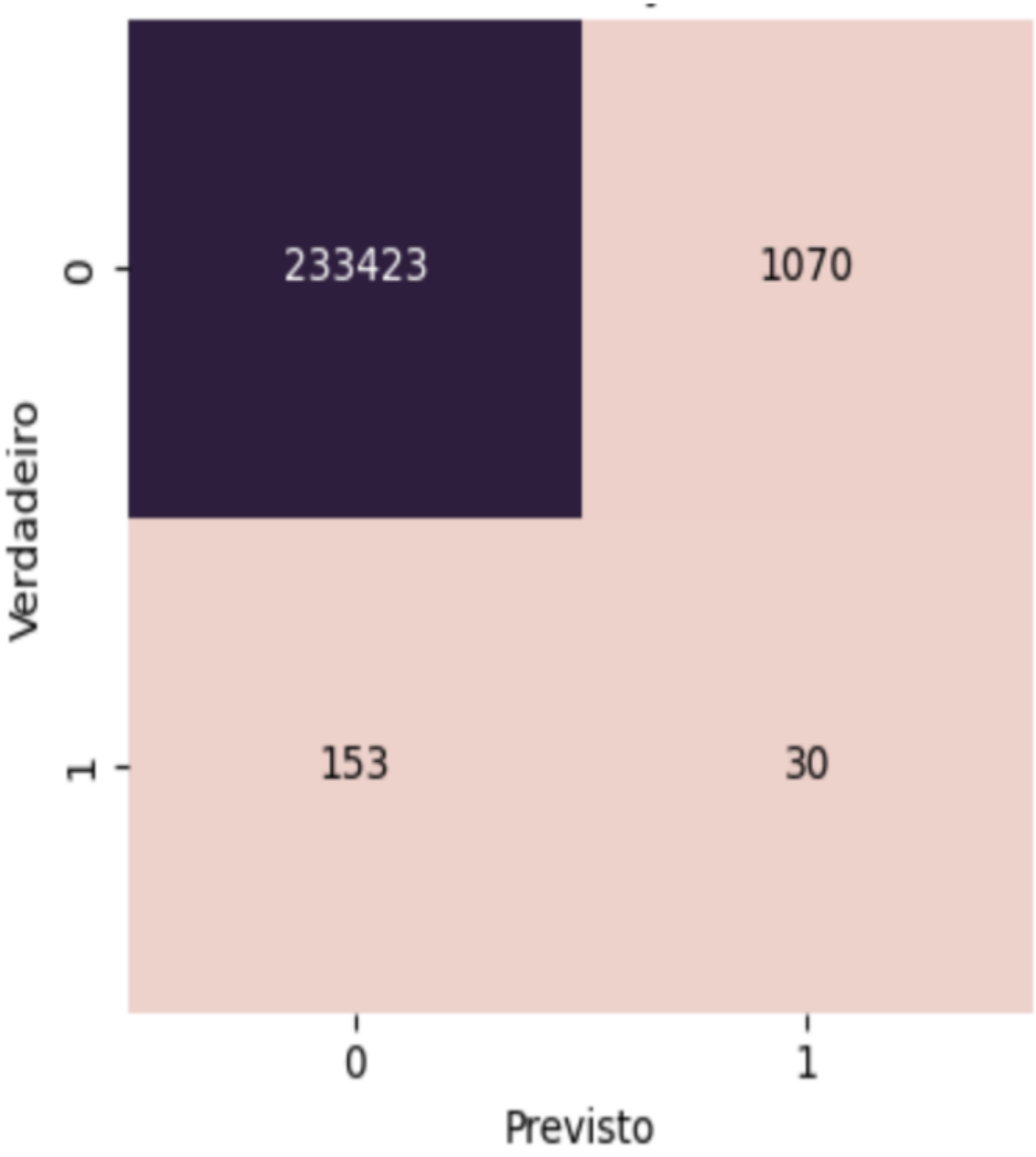
métricas equilibradas de precisão, recall e F1 Score. Isso que dizer que o modelo está realizando bem tanto na identificação de instâncias positivas quanto na prevenção de falsos positivos, contribuindo para a classificação de transações como normais ou fraudulentas. Na interpretação desse cenário financeiro, pode-se compreender o raciocínio por trás das decisões do modelo, gerando confiança no contexto financeiro.

3.1.2 Naive Bayes

O método Naive Bayes utiliza a probabilidade condicional para calcular a probabilidade de uma atividade suspeita ocorrer. Durante a fase de teste, o modelo calculou a probabilidade de uma instância pertencer a cada classe e atribuiu a instância à classe com a maior probabilidade.

Na matriz de confusão, o modelo Naive Bayes, de acordo com a Figura 8, se observa um conjunto detalhado de resultados para avaliar seu desempenho. Esses elementos fornecem uma base para calcular métricas, como precisão, recall, F1 Score e acurácia, oferecendo uma compreensão da capacidade do modelo na tarefa específica de classificação. Essa análise detalhada da matriz de confusão visa aprimorar estratégias, ajustar parâmetros e otimizar o modelo Naive Bayes, contribuindo assim para uma abordagem mais refinada e eficaz na identificação de padrões e na tomada de decisões em problemas de classificação.

Figura 8 – Matriz de confusão Naive Bayes



Fonte: Do autor.

Diante da análise detalhada do desempenho do Naive Bayes, se apresentado inicialmente uma alta acurácia, o modelo enfrenta desafios na detecção de

transações suspeitas, como indicado pelas métricas de precisão, recall e F1 Score. A disparidade entre essas métricas demonstra que o modelo tende a classificar erroneamente um número expressivo de transações como suspeitas, resultando em baixa precisão. Simultaneamente, o baixo recall evidencia a dificuldade do modelo em identificar de forma eficaz as transações fraudulentas, fazendo com que perca dados importantes no processo de detecção.

3.1.3 Support Vector Machine (SVM)

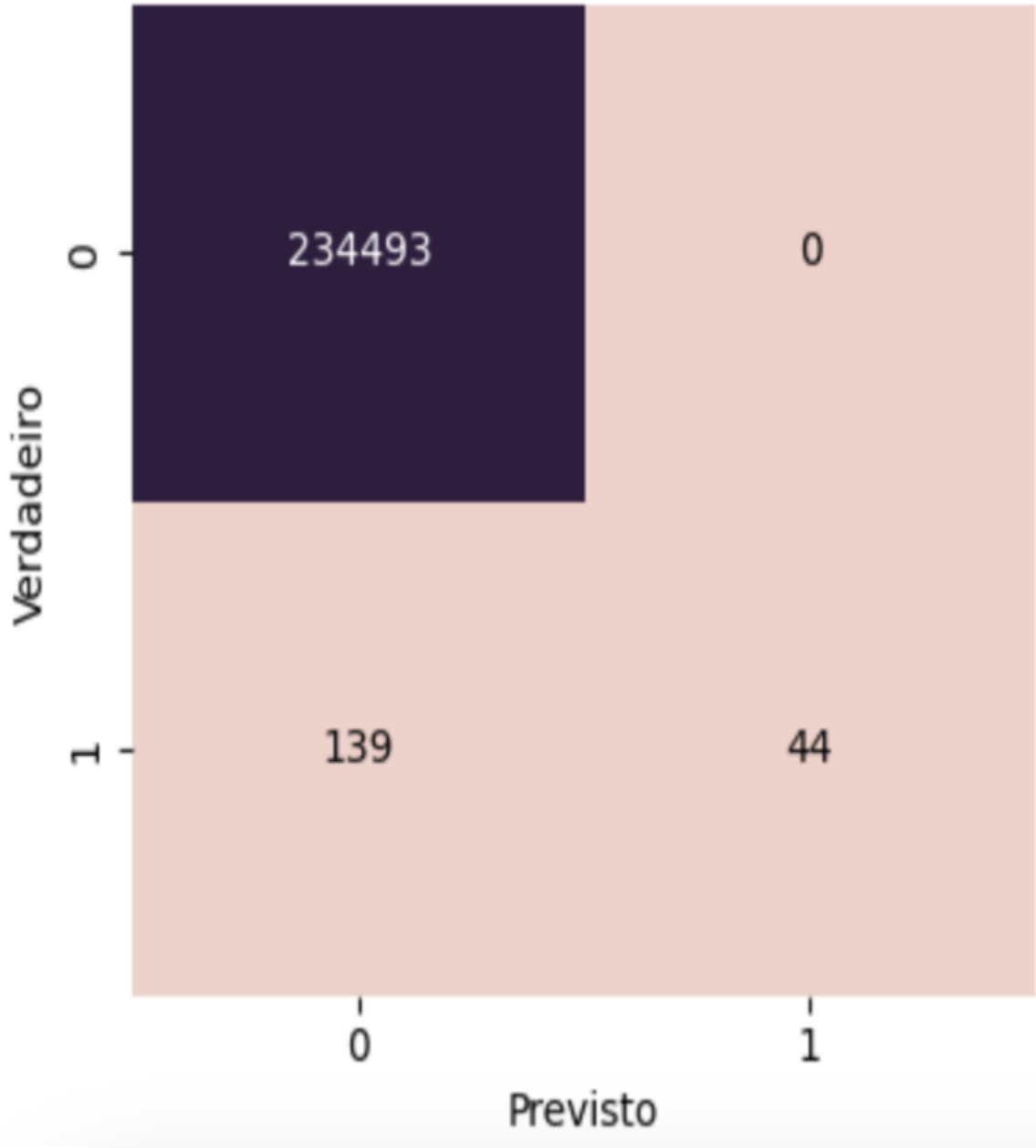
No contexto da detecção de fraudes financeiras, o Support Vector Machine (SVM) busca encontrar um hiperplano de separação otimizado entre diferentes classes de transações, permitindo a identificação eficaz de padrões suspeitos.

Os resultados do modelo Support Vector Machine (SVM) indicam que a acurácia está fazendo previsões corretas para todas as instâncias no conjunto de dados. No entanto, as métricas de precisão, recall e F1 Score, apresentaram discrepâncias. A precisão indica que todas as transações rotuladas como suspeitas pelo modelo foram corretamente classificadas. No entanto, o recall está identificando apenas uma fração das transações fraudulentas disponíveis no conjunto de dados.

A alta capacidade do SVM em identificar corretamente transações normais, como evidenciado pelos verdadeiros negativos, não ocorre em falsos positivos. No entanto, a presença de falsos negativos sugere que o modelo pode estar perdendo algumas transações suspeitas, indicando a necessidade

de ajustes para melhorar o recall. A análise desses resultados da matriz de confusão compreende o desempenho do SVM na detecção de transações suspeitas, conforme ilustrado na Figura 9.

Figura 9 – Matriz de confusão SVM



Fonte: Do autor.

A baixa pontuação no recall pode indicar que o modelo está perdendo muitas transações fraudulentas, resultando em um desequilíbrio entre

precisão e recall. O F1 Score, que é a média harmônica entre precisão e recall, destaca a necessidade de otimização para equilibrar essas métricas. Embora a acurácia seja boa, a análise detalhada dessas métricas de modelo SVM pode se beneficiar de ajustes para melhorar sua capacidade de identificar transações suspeitas.

Dessa forma, a importância de ajustes no modelo pode fortalecer sua capacidade de identificar efetivamente transações suspeitas, concentrando esforços específicos no aumento do recall. Esse refinamento visa assegurar uma detecção abrangente de atividades fraudulentas, mantendo um equilíbrio aceitável com a precisão geral do modelo.

4 Análises e Discussões

Os resultados sobre a importância da detecção de transações suspeitas no setor financeiro, ressalta a necessidade de aplicação de técnicas de Machine Learning para garantir a integridade financeira. Ao adotar diferentes tipos de transações, como transferências, débitos, saques, pagamentos em dinheiro e transações com cartão de crédito, fica evidente os desafios enfrentados e a complexidade do problema na detecção de fraudes. O uso dos métodos de Árvores de Decisão, Naive Bayes e Support Vector Machine (SVM) utilizados para a elaboração desse trabalho, forneceu uma abordagem condizente adotada na identificação de atividades fraudulentas. A explicação sobre como cada método é aplicado em diferentes tipos de transações demonstra a adaptação dessas técnicas de Machine Learning para lidar com as particularidades apresentadas nos diferentes contexto do cenário, conforme a Tabela 2.

Tabela 2 – Métricas de Resultados

Modelo	Acurácia	Precisão	Recall	F1 Score	Média
Árvore de decisão	1.00	0.80	0.72	0.76	0.89
Naive Bayes	0.99	0.03	0.16	0.05	0.31
Support Vector Machine	1.00	1.00	0.24	0.39	0.66

Fonte: Do autor.

As métricas dos resultados para cada modelo utilizado na detecção de fraudes financeiras. Essas métricas avaliam o desempenho de cada modelo e compreende a eficácia na identificação de transações suspeitas. Pode-se observar que a Árvore de Decisão apresentou uma acurácia de 1.00, o que indica que todas as previsões feitas pelo modelo estavam corretas. No entanto, as métricas de precisão, recall e F1 Score apresentaram valores menores, o que indica que o modelo enfrentou dificuldades em identificar corretamente todas as transações suspeitas. Enquanto na precisão de 0.80

sugere que 80% das transações foram classificadas como suspeitas pelo modelo eram realmente fraudulentas, já no recall de 0.72 indica que o modelo foi capaz de identificar corretamente 72% das transações fraudulentas presentes no conjunto de dados. O F1 Score de 0.76, que é a média harmônica entre precisão e recall, fornece uma medida combinada do desempenho do modelo, levando em consideração tanto os falsos positivos quanto os falsos negativos.

Por outro lado, o Naive Bayes apresentou uma acurácia de 0.99, o que indica um alto nível de precisão em suas previsões. No entanto, as métricas de precisão, recall e F1 Score foram baixas. A precisão de 0.03 sugere que apenas 3% das transações classificadas como suspeitas pelo modelo eram realmente fraudulentas, enquanto o recall de 0.16 indica que o modelo foi capaz de identificar apenas 16% das transações fraudulentas presentes no conjunto de dados. O baixo F1 Score de 0.05 indica que o modelo teve dificuldade em equilibrar precisão e recall, resultando em um desempenho geral inferior.

Por fim, o Support Vector Machine (SVM) obteve uma acurácia de 1.00, indicando que todas as previsões feitas pelo modelo estavam corretas. No entanto, as métricas de precisão, recall e F1 Score apresentaram discrepâncias. A precisão de 1.00 indica que todas as transações classificadas como suspeitas pelo modelo foram corretamente identificadas como fraudulentas, enquanto o recall de 0.24 indica que o modelo foi capaz de identificar corretamente apenas 24% das transações fraudulentas presentes no conjunto de dados. O F1 Score de 0.39 apresenta o equilíbrio

entre precisão e recall, mostrando que o modelo alcançou uma performance intermediária em relação aos demais modelos.

Com isso, a análise dos resultados apresentada evidenciou o desempenho geral positivo da Árvore de Decisão, os desafios enfrentados pelo Naive Bayes na detecção de transações suspeitas e as discrepâncias nas métricas de precisão e recall do SVM. Essa análise detalhada dos resultados forneceu insights sobre as capacidades e limitações de cada um dos métodos na detecção de fraudes financeiras. No entanto, a interpretação dos resultados para o contexto geral de identificar fraudes financeiras é perspicaz, destacando a importância da confiança no modelo para a tomada de decisões críticas. Outro ponto em questão, foi a identificação de áreas para melhoria em cada método, como ajustes nos parâmetros para melhorar o desempenho do Naive Bayes e Support Vector Machine(SVM). Esses ajustes proporcionaram o entendimento de possíveis desafios enfrentados na detecção de fraudes financeiras e no compromisso de buscar soluções mais eficazes para lidar com esses problemas.

5 Considerações finais

Com base na análise dos resultados apresentados, fica evidente a importância crítica da detecção de transações suspeitas no setor financeiro e a necessidade de aplicação de técnicas de Machine Learning para garantir a integridade financeira. Os desafios enfrentados, juntamente com a complexidade de lidar com a detecção de fraudes, levam em consideração os diferentes tipos de transações, como transferências, débitos, saques, pagamentos em dinheiro e transações com cartão de crédito.

Os métodos de Árvores de Decisão, Naive Bayes e Support Vector Machine (SVM) utilizados neste estudo demonstraram abordagens condizentes para a identificação de atividades fraudulentas em diferentes contextos do cenário financeiro. As métricas de desempenho dos modelos ofereceram uma visão clara, e destacou tanto os pontos fortes quanto as limitações de cada abordagem. A Árvore de Decisão mostrou um desempenho geral positivo, com alta acurácia, embora tenha enfrentado desafios na identificação precisa de todas as transações suspeitas, como demonstrado pelas métricas de precisão, recall e F1 Score. Por outro lado, o Naive Bayes exibiu uma acurácia alta, mas teve dificuldades em equilibrar precisão e recall, resultando em um desempenho inferior na detecção de transações fraudulentas. O Support Vector Machine (SVM) alcançou uma alta acurácia e uma precisão excelente, mas enfrentou desafios em identificar corretamente um número de transações fraudulentas, conforme apresentado pelo baixo recall.

A análise detalhada desses resultados forneceu insights muito bons sobre as capacidades e limitações de cada método na detecção de fraudes financeiras. Além disso, destacou a importância da confiança nos modelos para a tomada de decisões críticas no ambiente financeiro. É importante ressaltar que a interpretação desses resultados deve considerar o contexto geral da detecção de fraudes financeiras, e a busca de melhoria, como a necessidade contínua de aprimoramento e ajustes nos modelos. Esses esforços de aprimoramento são fundamentais para enfrentar os desafios em constante evolução e garantir a eficácia das soluções adotadas na detecção e prevenção de atividades fraudulentas no setor financeiro.

REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL, F. Aprenda mineração de dados: teoria e prática. [S.l.]: Alta Books Editora, 2016. v. 1. Citado 2 vezes nas páginas 12 e 13.

BENZ, G. L. Sistema de apoio à detecção de fraudes em e-commerce. 2017. Citado 2 vezes nas páginas 14 e 15.

BHATTACHARYYA, S. et al. Data mining for credit card fraud: A comparative study. Decision support systems, Elsevier, v. 50, n. 3, p. 602–613, 2011. Citado na página 13.

CORTES, C.; VAPNIK, V. Support-vector networks. Machine learning, Springer, v. 20, p. 273–297, 1995. Citado na página 13.

CRISTOVÃO, R. B.; BUSCAGLIA, G. C. Detecçao de fraude no comércio eletr^onico brasileiro. Anais, 2022. Citado 2 vezes nas páginas 10 e 12.

FREITAS, A. L.; JUNIOR, O. S. Machine learning: desafios para um brasil competitivo. Revista da Sociedade Brasileira de Computação, v. 38, n. 01, 2019. Citado na página 7.

GAMA, J. et al. Concept drift in decision-tree learning for data streams. In: Proceedings of the Fourth European Symposium on Intelligent Technologies and their implementation on Smart Adaptive Systems, Aachen, Germany, Verlag Mainz. [S.l.: s.n.], 2004. p. 218–225. Citado na página 12.

GUIMARÃES, M. A. Detecção de fraude em aplicativos de e-commerce. Universidade Presbiteriana Mackenzie, 2022. Citado na página 7.

HAYKIN, S. Redes neurais: princípios e prática. [S.l.]: Bookman Editora, 2001. Citado na página 11.

JUNIOR, J. C. P. Modelos para detecção de fraudes utilizando técnicas de aprendizado de máquina. Tese (Doutorado), 2018. Citado na página 7.

JÚNIOR, J. F. et al. Mineração de dados para detecção de fraudes em transações eletrônicas. Universidade Federal de Minas Gerais, 2012. Citado 2 vezes nas páginas 7 e 15.

KOWALCZYK, A. Support vector machines succinctly. Syncfusion Inc, 2017. Citado na página 13.

LIMA, S. C. d. Detecção de fraudes em pagamentos com cartão de crédito utilizando técnicas de aprendizado de máquina. Serra, 2023. Citado 2 vezes nas páginas 13 e 14.

MATTOS, L. D. Aplicação de técnicas de machine learning no apoio à detecção de fraudes em pagamentos online. 2022. Citado na página 7.

MOHRI, M.; ROSTAMIZADEH, A.; TALWALKAR, A. Foundations of machine learning.[Sl]. [S.l.]: The MIT Press, 2012. Citado na página 12.

PÁSCOA, M. I. F. Os desafios da Machine Learning: Aplicação ao Mercado Financeiro. Tese (Doutorado) — Universidade de Coimbra, 2018. Citado na

página 11.

PICCIN, L. E. Métodos de detecção de fraude em cartões de crédito: um estudo comparativo. Universidade Federal de São Carlos, 2022. Citado 2 vezes nas páginas 10 e 12.

ROZA, B. E.; PEGORARO, M. A. G. Classificador de phishing utilizando algoritmo de naive bayes. 004, 2020. Citado na página 15.

SOCCA Junior, J. R. (2024). A proficuidade dos sistemas ERP no âmbito da análise de negócios. Revista Tópicos, 2(10).

SOUSA, J. S. d. Estudo comparativo entre modelos para detecção de fraudes em cartões de crédito. 2021. Citado 2 vezes nas páginas 12 e 14.

ZHANG, C.; MA, Y. Ensemble machine learning: methods and applications. [S.l.]: Springer, 2012. Citado na página 11.

[1] Bacharel em Engenharia da Computação, em Ciência da Computação, Licenciado em Matemática, Pós-Graduado em Business Intelligence e Analytics e MBA em Big Data. Mestrando em Business Administration pela Miami University of Science and Technology (EUA).
joaoricardo@me.com

Lista de abreviaturas e siglas

ML - Machine Learning

IA - Inteligência Artificial

AM - Aprendizado de Máquina

SVM - Support Vector Machine

NB - Naive Bayes