Detecção de Fraude de Crédito

Pedro Henrique Tamashiro Faria
Unifesp
Universidade Federal de São Paulo
São José dos Campos
Pedro.Tamashiro@unifesp.br

Felipe Baz Mitsuishi
Unifesp
Universidade Federal de São Paulo
São José dos Campos
Felipe.Mitsuishi@unifesp.br

I. Resumo

Este artigo aborda a detecção de fraudes de crédito, levando em consideração um contexto de crescente digitalização financeira e sofisticadas técnicas fraudulentas. Com o aumento das transações digitais e o crescimento dos números de transações fraudulentas, utilizando de clonagem de cartões, roubo de identidade, o estudo propõe o uso de inteligência artificial (IA) para melhorar a identificação dessas fraudes. A pesquisa visa explorar diversas técnicas de machine learning, para analisar um dataset de transações de crédito e superar o grande desafio do desbalanceamento dos dados. O objetivo principal é encontrar uma inteligência artificial capaz de detectar de forma precisa as fraudes, ocasionando em uma redução das perdas financeiras e aumentar a segurança das transações.

Palavras-chave: Detecção de Fraude de Crédito, Inteligência Artificial, Machine Learning, Balanceamento de Dados, Anomalias, Python.

II. INTRODUÇÃO E MOTIVAÇÃO

É notável a crescente da tecnologia nos dias de hoje, e com ela o aumento das transações financeiras realizadas no cotidiano, seja por com a praticidade do Pix, ou até mesmo com a popularização dos NFT's de Crédito nos celulares, a partir desse aumento da digitalização dos serviços financeiros, a quantidade de dados gerados e a velocidade das transações também aumentaram de forma exponencial, consequentemente, trouxe consigo o um aumento das fraudes, principalmente quando se fala de Fraudes de Crédito, segundo a InfoMoney, em 2021 o Brasil um aumento de 33% na tentativa de no 1º semestre do ano, explanando a seriedade do tema

A fraude em si pode ser de várias maneiras, seja clonagem de cartão, falsificação de informações ou até mesmo roubo de identidade, sendo o ato extremamente prejudicial para o usuário, que acaba por ocasionar uma perda considerável de capital por meio destes.

Por conta disso, nos foi criada a necessidade de abordar o assunto de maneira mais incisiva, e assim desenvolvendo uma IA, capaz de verificar a autenticidade de uma transação, evitando assim a possibilidade de alguma informação irreal seja passada para frente, afinal com o avanço da tecnologia, a diversidade de golpes, assim como a elaboração dos mesmos, vem sendo aumentada, tendo uma necessidade constante de evolução, tanto da prevenção, quanto dos meios de detecção destas fraudes.

III. CONCEITOS FUNDAMENTAL

A. Fraudes de Crédito

As Fraudes de crédito se referem às ações ilícitas onde um indivíduo ou entidade utiliza de informações de crédito de outra pessoa sem autorização, com a intenção de obter alguma vantagem financeira. As fraudes de crédito podem ocorrer de diversas formas, incluindo, mas não se limitando a transações não autorizadas, roubo de identidade e falsificação de documentos de crédito.

B. Detecção de Fraudes

A detecção de Fraudes é um procedimento de identificação de atividades fraudulentas em um conjunto de dados de transações. Esse processo é crucial para o setor bancário, visto que minimiza as perdas financeiras e protege a integridade das instituições financeiras. As técnicas de detecção de Fraudes podem ser divididas em 2 abordagens, as baseadas em regras e as baseadas em machine learning.

C. Abordagens Baseadas em Regras

Essa abordagem utiliza-se de um conjunto de regras heurísticas, pré-estabelecidas, que visa identificar comportamentos suspeitos. Embora simples de implementar, essas abordagens muitas vezes falham em detectar as fraudes novas ou evolutivas.

D. Abordagens Baseadas em Machine Learning

Utilizando-se de modelos estáticos e algoritmos de aprendizado para identificar padrões e anomalias em volumes de dados extensos. Essas abordagens são mais eficazes na detecção e prevenção de fraudes.

E. Machine Learning

O machine learning, ou aprendizado de máquina, é um subconjunto da área de inteligência artificial, que se concentra na confecção de sistemas que aprendem, e melhoram seu desempenho, com base nos dados que consomem.

F. Desbalanceamento dos Dados

As fraudes representam uma minúscula fração das transações totais, assim resultando em um conjunto de dados altamente desbalanceado, o que pode levar a modelos tendenciosos em favor das classes majoritárias(Transações lícitas)

G. Evolução das Técnicas de Fraude

Com a evolução contínua de novas técnicas de fraude para evitar a detecção de fraudes, é exigido que os modelos sejam altamente adaptativos e atualizáveis.

H. Custos de Falsos Positivos

A detecção de transações legítimas como fraudulentas pode gerar uma experiência negativa para o cliente, resultando na perda de confiança na instituição financeira. Por outro lado, deixar de identificar uma transação ilícita

como fraudulenta pode acarretar grandes perdas financeiras para a instituição, além de comprometer a confiança dos clientes.

IV. TRABALHOS RELACIONADOS

Existem alguns trabalhos na literatura que se dedicaram a discorrer sobre o tema de fraude de crédito, como por exemplo:

A. *"A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective",*

"A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective", de 2021, foi um artigo que focou na explicação de detecção de fraudes de créditos, categorizando as abordagens com dados e técnicas, ele avalia diferentes modelos de aprendizagem de máquina, além de abordagens híbridas, mostrando suas vantagens e limitações.

B. *"Detecção de Fraude em Transações com Cartão de Crédito Utilizando Algoritmos de Machine Learning"*

"Detecção de Fraude em Transações com Cartão de Crédito Utilizando Algoritmos de Machine Learning", de 2023, publicado por uma Brasileira, ele compara a diferente eficiência de alguns modelos de aprendizagem de máquina, entre eles estão, SVM, Random Forest e Redes Neurais, comparando um com o outro.o

C. *"Anomaly Detection in Credit Card Transactions by Using a Combination of Machine Learning and Data Mining Techniques"*

"Anomaly Detection in Credit Card Transactions by Using a Combination of Machine Learning and Data Mining Techniques", Propõem um Sistema híbrido de técnicas de mineração de dados, utilizando aprendizado de máquina para detecção de anomalias em transações de crédito. O estudo utiliza alguns modelos de algoritmo como K-Means, DBSCAN e SVM, destacando a vantagem de métodos combinados sobre técnicas isoladas.

D. *"Credit Card Fraud Detection Using Deep Learning"*

Outro trabalho relevante na área é o estudo "Credit Card Fraud Detection Using Deep Learning" que explora o uso de redes neurais profundas para a identificação de fraudes. Este estudo demonstra como técnicas avançadas de deep learning, como LSTM (Long Short-Term Memory) e autoencoders, podem ser aplicadas para detectar padrões temporais e anomalias em dados transacionais. A utilização de redes neurais profundas oferece uma perspectiva interessante, pois permite a captura de padrões complexos que podem não ser detectados por algoritmos mais tradicionais.

E. *"Economic Impacts of Fraud Detection Systems in Banking."*

O impacto econômico das fraudes de crédito também foi amplamente discutido no artigo "Economic Impacts of Fraud Detection Systems in Banking." Este estudo avalia o custo-benefício de implementar sistemas avançados de detecção de fraudes, levando em consideração não apenas as perdas financeiras diretas evitadas, mas também o impacto indireto na confiança do cliente e na reputação da instituição financeira. A análise econômica fornece uma justificativa sólida para o investimento contínuo em tecnologias de detecção de fraudes, destacando a importância de desenvolver soluções eficientes e escaláveis.

V. OBJETIVO

Este trabalho tem como objetivo desenvolver uma IA capaz de identificar fraudes de transações de crédito de quaisquer bases apresentadas, de maneira eficiente e precisa, diminuindo a possibilidade de alguma operação ilícita realizada, passar despercebida pelo sistema dos bancos, sendo capaz de reduzir perdas financeiras e melhorar a segurança de transações realizadas, tanto por instituições bancárias, quanto pela população como um todo.

Utilizaremos alguns modelos para testar a eficiência da Inteligência Artificial, como: Isolation Florest, DBScan, XGBoost e One-Class SVM, além de 2 modelos possíveis de base de dados, onde na primeira, os dados estão balanceados, sendo 50% para dados com "Class" igual a 1, ou seja, dados fraudulentos, e 50% para dados de transações "Reais".

VI. METODOLOGÍA EXPERIMENTAL

A. *Bibliotecas Python*

Grande parte do nosso projeto em IA será realizado em Python, com o uso das bibliotecas, pandas, para manipulação do DataFrame e Sktlearn, para a elaboração de um modelo de aprendizagem de máquina.

Serão implementadas funções específicas da biblioteca Sklearn para manipulação do nosso DataFrame, com intenções diversas, como por exemplo reduzi-lo para podermos manuseá-lo da maneira adequada, não sendo necessário um tempo excessivo para trabalhar com nossa Inteligência Artificial.

Além das bibliotecas mencionadas, também será útil incorporar o uso do Matplotlib e do Seaborn para a visualização dos dados. Essas bibliotecas de visualização ajudarão na análise exploratória dos dados, permitindo a identificação de padrões e anomalias visuais que podem informar a construção e o ajuste dos modelos de machine learning. Visualizações claras podem destacar discrepâncias e relações que não são imediatamente aparentes nos dados brutos, facilitando um entendimento mais profundo do comportamento das transações e das fraudes.

Ademais, utilizaremos o Pandas para manipulação linear do nosso banco de dados, principalmente para visualização dele, facilitando o desenvolvimento da base.

B. *DataSets*

Utilizaremos uma base de transações de crédito, disponibilizada no site Kaggle, para criação da nossa IA, nela temos cerca de 285 mil transações, podendo ser uma boa fonte para o aperfeiçoamento da Inteligência, por ter uma boa variedade de dados, mesmo sendo bastante desequilibrado,

Podemos tratar a estabilidade do banco de dados para o melhor aprendizado da máquina, como por exemplo o balanceamento do peso da amostra, atribuindo diferentes peso para anomalias, e para pontos normais.

Esta será nossa principal fonte de dados, na qual será trabalhada para diminuição do tamanho, sem a perda de informações, mantendo sempre a mesma proporção de dados para o melhor aprendizado do modelo.

C. *Modelos de Aprendizagem*

Serão implementados em algumas tentativas iniciais do projeto alguns modelos de aprendizagem diversificados, a fim de definir qual será o que tem o melhor resultado para o objetivo esperado da Inteligência Artificial.

Entre os modelos utilizados, serão implementados a Floresta Isolada, onde o modelo funciona da seguinte forma, ele identifica anomalias através do conceito de isolamento de pontos de dados construindo várias árvores de decisão, onde cada árvore é formada a partir de amostras aleatórias do conjunto de dados. Dentro de cada árvore, os dados são divididos repetidamente por cortes aleatórios nos atributos até que todos os pontos estejam isolados. O comprimento do caminho necessário para isolar um ponto é então calculado e nos é dado com isso a divisão entre pontos "normais" e "anormais".

Além dele, será implementado o modelo O funcionamento do DBSCAN, que envolve a classificação dos pontos como pontos centrais, pontos de borda ou pontos de ruído. Pontos centrais têm pelo menos minPts, pontos dentro do raio ϵ. Os pontos de borda estão dentro do raio ϵ de um ponto central, mas não têm minPts pontos ao seu redor. Pontos de ruído não estão densamente conectados a nenhum cluster. O DBSCAN é eficaz para identificar clusters de forma arbitrária e é robusto na detecção de outliers, sendo útil em conjuntos de dados com forma irregular e ruídos.

D. *Peso da Amostra*

Por termos um banco de dados bem desbalanceado, afinal é intuitivo pensar que termos bem mais transações verídicas do que fraudulentas, é necessário pensarmos que o peso de cada tipo de dado seja diferentes, onde a proporção de dados é 1 fraude para cada 10 mil transações, o peso da amostra do dado de Fraude, deve ser muito maior que o das 10 mil transações, a fim de balancear a amostra para o melhor aprendizado do modelo.

Podemos fazer isso de diversas formas, uma delas é aplicar uma espécie de "punição" a cada erro da máquina, e essa punição ser maior para cada transação de fraude não reconhecida pelo modelo.

No caso da nossa aplicação, optamos por diminuir a quantidade de dados presentes na nossa base de dados, porém mantendo toda a quantidade de casos de fraudes disponíveis, variando a proporção do nosso modelo, com mais, ou menos dados de transações positivas, tendo em vista que estas transações positivas são escolhidas de modo aleatório entre todas as 2

E. *Separação dos Dados*

Nossa Base Inicialmente possuí 284.807 transações realizadas no período de 2 dias na Europa com máquinas de cartão, dentre elas, apenas 492 são fraudulentas, ou seja, 0,172% da Base, com isso, além da separação dos dados, que será realizada entre, Balanceada e Desbalanceada, precisamos que os dados sejam únicos em cada teste, afim da Inteligência Artificial seja capaz de generalizar adequadamente para novos dados não vistos anteriormente.

Para isso, a base de dados deverá ser dividida entre Treino e Teste, no qual os dados de Teste, serão 25% da base dividida (já tratada com cerca de mil variáveis) e os dados de teste com 75% do total.

VII. Resultados/Discussões

Separamos diversos casos de análise para a Inteligência Artificial, foram compilados 2 vezes para cada um dos modelos, com as bases, balanceadas e desbalanceadas, com isso, podemos analisar individualmente cada um dos modelos, para visualizar sua performance, assim como sua consistência predita, com os testes práticos.

A. *Base Balanceada*

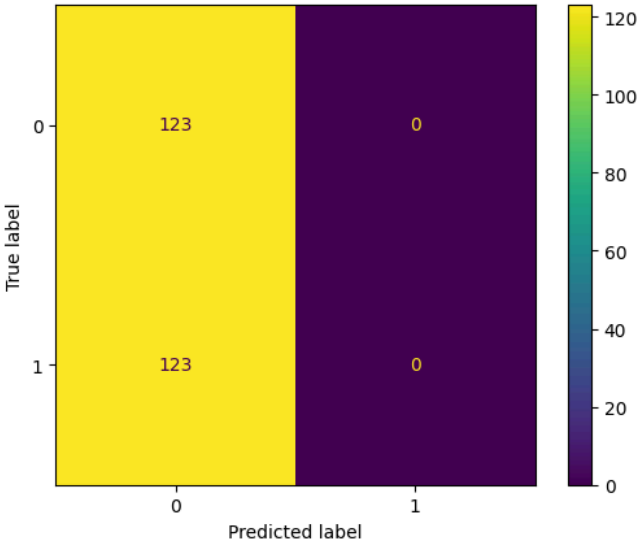
Para esse tipo de avaliação, utilizamos a base com um total de 492 transações fraudulentas e 492 transações "reais", ou seja, a base de dados está com a proporção de 50%, além disso, todos os dados de transações verdadeiras, são obtidos aleatoriamente entre toda a base de dados, podem ser qualquer permutação dos 280 mil dados.

Partindo deste princípio podemos começar com o caso base de análise, que é o modelo de Regressão Linear.

1) *Regressão Linear*

O modelo com esse tipo de dado, não teve êxito algum em realizar as tarefas em nenhum momento, tendo um total de 0 predições de dados com fraude para o resultado final, tendo uma precisão de 50%, em exclusivo pelo motivo da base estar balanceada, num cenário onde a Inteligência Artificial fosse implementada com esse modelo, ela apenas "Chutaria" todos os resultados como Falsos para fraude, não sendo confiável desta forma.

(1) Gráfico Regressão Linear Balanceado

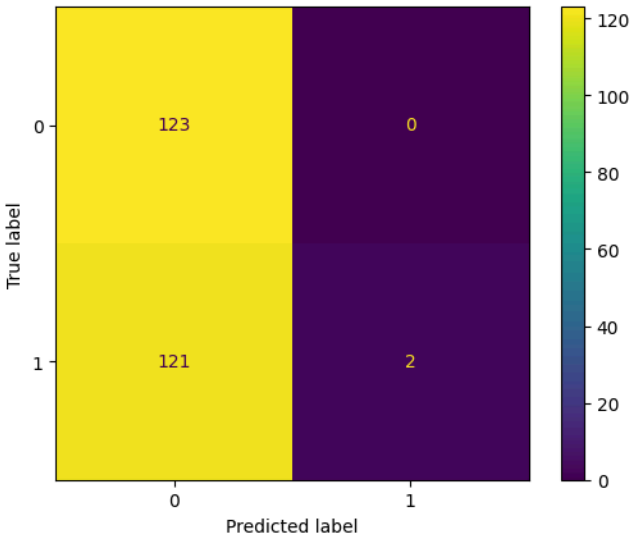


Tendo como base geral em todos os exemplos que "0" é negativo para fraude e "1" positivo para fraude, o modelo acabou sendo infeliz em sua resolução.

2) *Isolation Forest*

Dentro do contexto de aprendizado de máquina, o modelo da Floresta Isolada é utilizado consideravelmente para quantidades massivas de dados, porém quando temos uma base tão equilibrada quanto a dada para teste nesse 1º momento, o modelo acaba deixando a desejar, ficando com apenas 2 Verdadeiros para fraude, e o restante para Falsos, tendo consigo 100% de acerto com as predições de fraude, porém menos de 50% nas gerais.

(2) Gráfico Isolation Forest Balanceado

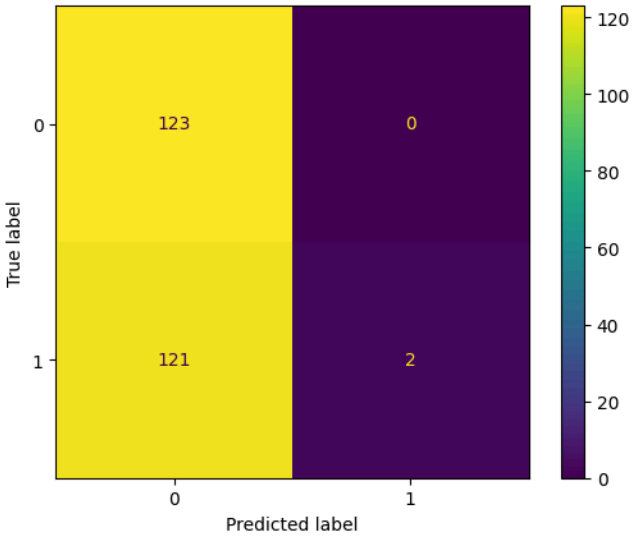


Seguimos com resultados pífios com relação ao modelo utilizado atualmente, com a distribuição balanceada.

3) One-Class SVM

Quando falamos de One-Class SVM quando os dados são majoritariamente equivalentes, ou seja, possuem todos as mesmas características e se encontram no mesmo grupo (com uma quantidade massiva de dados iguais e alguns outliers), o modelo se sai bem, porém quando tratamos de uma base equilibrada, onde temos uma proporção absurda de 1 para 1, este tipo de princípio acaba se perdendo um pouco na sua aplicação, como podemos ver no gráfico de calor.

(3) Gráfico One-Class SVM Balanceado

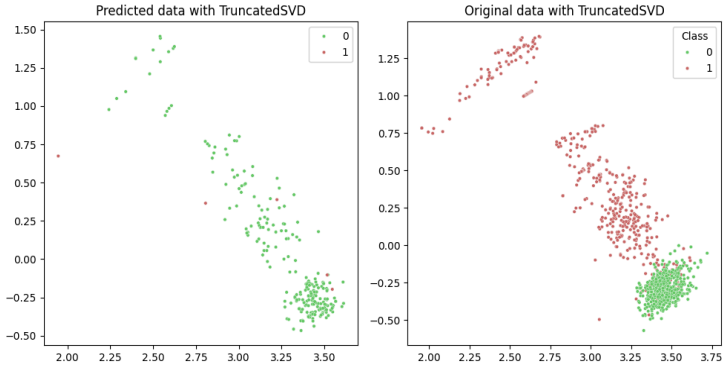


tivemos resultados equivalentes aos da floresta isolada, não sendo eficiente para o resultado esperado novamente.

4) Local Outlier Factory

Diferente dos outros modelos apresentados até agora, este foi o primeiro que acabou predizendo uma fraude de maneira equivocada, tendo um total de 80% de acerto com 5 predições de fraude no total, por ter um foco com conjuntos aglomerados de dados, o modelo acaba não sendo tão eficiente nesse momento, pelos dados não estarem totalmente agrupados, principalmente quando falamos dos dados de fraude que são no geral, outliers despadronizados.

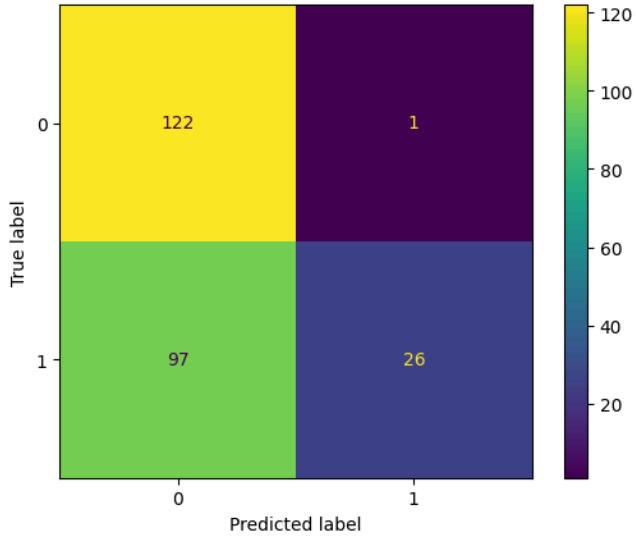
(4) A esquerda o gráfico gerado pela IA, e a direita os dados resposta do problema



5) DBSCAN

Este virá a ser o melhor resultado para o dataset Balanceado por vários motivos, mas principalmente pela distribuição dos dados verdade, onde os Falsos estão aglomerado em um extremo e os Verdadeiros Estão distribuídos pelo gráfico, dando a entender a despadronização dos dados, e como o DSBCAN se baseia na distância entre os pontos, acaba tendo uma melhor predição.

(5) Gráfico DBSCAN Balanceado



Como fica aparente no gráfico, em relação aos outros o DBSCAN teve um desenvolvimento melhor em relação a detecção de Fraudes, porém ainda deixa a deseja

6) XGBoost

Em relação ao XGBoost, o desenvolvimento dele neste processo foi de longe o mais decepcionante, tendo em vista o potencial que ele aparentava ter sobre modelos de dados balanceados, tendo em vista o modelo de “árvore” que ele segue, tendo um total de 0 predições de fraude, ficando nos 50% de acerto com 100% de predições para “transações sem fraude”

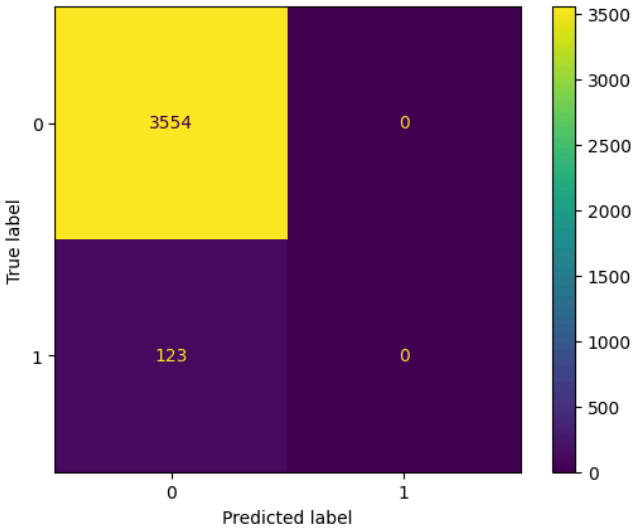
B. *Base Desbalanceada*

.Em contrapartida ao dataset balanceado, temos outra saída na qual os dados estejam distribuídos de maneira onde, 492 transações fraudulentas, simboliza 3,35% das transações totais de um banco, caracterizando uma base totalmente desbalanceada, a fim de testar os mesmo modelos em circunstâncias mais próximas à realidade.

1) *Regressão Linear*

O caso base como esperado, se manteve constante independente da distribuição da Base, não considerando nenhuma transação como fraudulenta, não tendo nenhuma confiança na sua execução no mundo real.

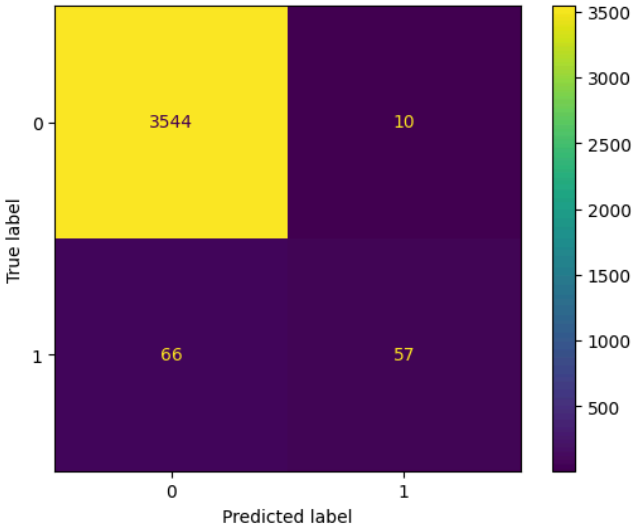
(6) Gráfico Regressão Linear Desbalanceado



2) *Isolation Forest*

Como esperado pelo modelo com bases desbalanceadas, ele apresentou uma melhora significativa quando os dados foram tratados de maneira não proporcional, saindo das 2 predições para 67, tendo uma precisão de 85% na localização de fraudes, porém ainda não é o esperado.

(7) Gráfico Isolation Forest Desbalanceado

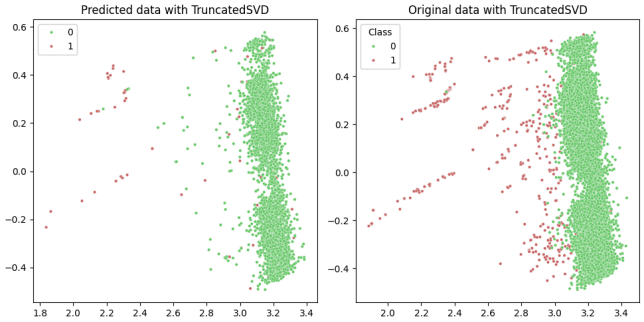


3) *One-Class SVM*

De todos os modelos além do caso padrão, o SVM foi o que menos progrediu com a alteração do tratamento de dados, o que é inesperado tendo em vista a praticidade no mesmo quando os dados são massivos e equivalentes.

Sua precisão foi de 68% na localização de Fraudes, ficando para trás do Isolation Forest, que não tem como foco a detecção de outliers.

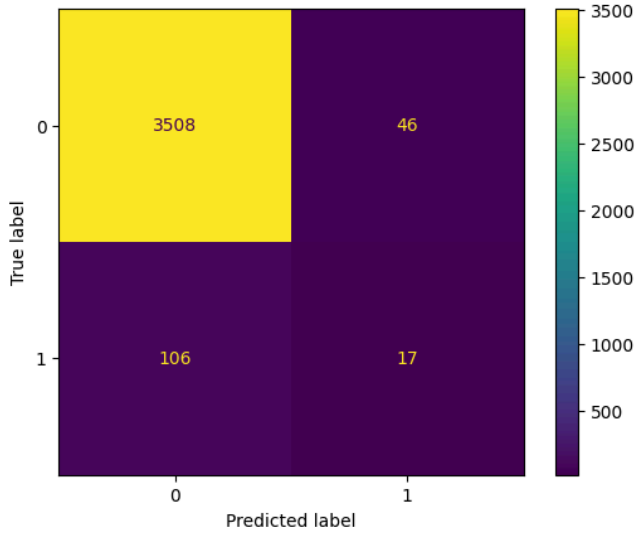
(8) A Esquerda o gráfico de visualização dos dados gerados pelo modelo de SVM e a direita a plotagem verdade



4) *Local Outlier Factory*

Este modelo, por ter a proposta de localizar Outliers e nosso problema apresentar tipos de dados que fogem de um padrão, que no geral não ocasionam um outlier, então não haveria como o "Local Outlier Factory" se sair tão bem quantos os outros, ficando com singelos 27% de resultado positivo.

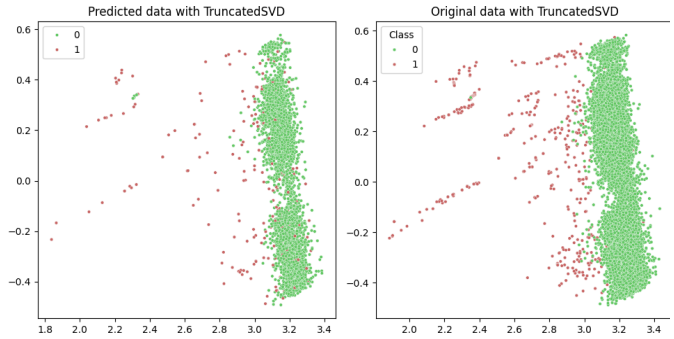
(9) Gráfico Local Outlier Factory Desbalanceado



5) *DBSCAN*

Disparado foi o melhor resultado para a IA, pois assim como na base balanceada, os dados seguem aglomerados em pontos específicos, facilitando ao modelo generalizar cada tipo de variável da melhor forma possível.

(10) Na Esquerda os dados gerados pelo DBSCAN e na direita os dados Verdade



6) XGBoost

Assim como no balanceado, não obteve nenhum resultado na predição dos dados fraudulentos, não sendo possível implementá-lo como uma possível opção para resolução deste problema.

VIII. Conclusões e Trabalhos Futuros

Neste trabalho, foram exploradas diversas abordagens para o problema da classificação de fraudes bancárias. Dentre os métodos utilizados, o DBSCAN foi o que se mostrou mais eficiente na identificação das fraudes. Essa performance destaca a capacidade do DBSCAN de lidar com uma distribuição extremamente desbalanceada.

As tentativas de balanceamento dos dados, não resultaram em aumentos significativos na acurácia do modelo. O que nos indica que o balanceamento dos dados pode não ser um fator determinante para melhoria do desempenho no contexto específico deste estudo.

Para trabalhos futuros, pode ser analisado mais profundamente as configurações de parametrização do DBSCAN, bem como uma análise aprofundada da relação entre a classe objetivo com seus atributos, a fim de melhorar o pré-processamento dos dados, visando verificar se há um aumento na precisão do modelo em identificar transações fraudulentas.

REFERÊNCIAS

[1] https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud
[2] https://seer.upf.br/index.php/rbca/article/view/13790
[3] “Detecção de Fraude em Transações com Cartão de Crédito Utilizando Algoritmos de Machine Learning”
[4] ‘Anomaly Detection in Credit Card Transactions by Using a Combination of Machine Learning and Data Mining Techniques"
[5] https://www.kaggle.com/code/janiobachmann/credit-fraud-dealing-with-imbalanced-datasets
[6] https://www.kaggle.com/code/joparga3/in-depth-skewed-data-classif-93-recall-acc-now