DESENVOLVIMENTO DE DETECTOR DERIVA/ANOMALIA PARA A CONSTRUÇÃO DE ESTEIRAS DE MLOPS EFICIENTES

Luiz Felipe Tavolaro Ayres de Albuquerque (IC) e Gustavo Scalabrini Sampaio (Orientador)

PIBIC CNPq

Resumo

Modelos de aprendizado de máquina frequentemente enfrentam o desafio de manter a precisão em ambientes sujeitos a mudança de comportamento ou anomalias isoladas. Identificar corretamente esses dois eventos demonstra-se uma problemática que gera, com frequência, falsos positivos e retreinamentos de modelos desnecessários. Tendo isso em vista, este trabalho tem como objetivo propor uma arquitetura capaz de detectar e diferenciar esses eventos de maneira precisa e automatizada. A metodologia se deu pela construção de um pipeline em *Python,* estruturado com múltiplos filtros de validação baseados na combinação de técnicas estatísticas, como a “regra do boxplot” e o *ADWIN*, e cruzamentos com base de dados históricos. O algoritmo foi conteinerizado em uma *API Flask* e avaliado em quatro diferentes cenários. Os resultados demonstram que os filtros aplicados funcionam como uma barreira que protege o sistema de falsos positivos, permitindo que o sistema identifique as derivas de conceito em todos os casos testados. A pesquisa conclui que a arquitetura proposta agrega robustez às esteiras de *MLOps*, garantindo retreinamentos apenas mediante a mudanças reais no padrão de comportamento histórico na distribuição de dados.

Palavras-chave: *Derivas de Conceito. Anomalias. Aprendizagem de Máquina*

Abstract

Machine learning models often face the challenge of maintaining accuracy in environments subject to behavioral shifts or isolated anomalies. Correctly distinguishing between these two events is a problematic task that frequently leads to false positives and unnecessary model retraining. With this in mind, this study aims to propose an architecture capable of accurately and automatically detecting and differentiating these events. The methodology involved building a Python pipeline structured with multiple validation filters—based on a combination of statistical techniques such as the "boxplot rule" and ADWIN—and cross-referencing with historical data. The algorithm was containerized within a Flask API and evaluated across four different scenarios. The results demonstrate that the applied filters act as a barrier protecting the system from false positives, enabling the identification of concept drift in all tested cases. The research concludes that the proposed

architecture enhances the robustness of MLOps pipelines, ensuring retraining occurs only in response to genuine changes in historical behavioral patterns within the data distribution.

Keywords: *Concept Drifts. Anomalies. Machine Learning*

1- Introdução

Com os avanços tecnológicos voltados para ciência de dados, a democratização e a popularidade de modelos inteligência artificial (IA) e o contínuo estudo dos processos de aprendizado de máquina, novos modelos de apoio a tomada de decisão, entretenimento e interação por meio de linguagem natural, vêm se tornando parte do dia a dia da população. Em sistemas de IoT, por exemplo, com os avanços tecnológicos relacionados ao tema e o consequente crescimento na geração de dados, técnicas de aprendizagem de máquina têm sido cada vez mais aplicadas nesse contexto (ILIć; STOJANOVIć, 2023). Considerando esse cenário, a construção de modelos de IA sempre devem prezar pela qualidade e integridade dos dados para tentar extrair os melhores resultados possíveis. Nesse sentido, existem dois problemas que podem impactar negativamente os resultados dos modelos, sendo eles a deriva de conceito e a anomalia. A identificação e o tratamento de derivas de conceito e anomalias são temas que vêm sendo estudados fortemente nos últimos anos. No entanto, a detecção e diferenciação desses dois eventos ainda é um processo desafiador para a construção de sistemas baseados em IA, visto o obstáculo em diferenciar derivas de conceitos e mudanças de comportamento isoladas, gerando falsos positivos e retreinamentos desnecessários dos modelos.

A presente pesquisa tem por objetivo propor um sistema que aplique técnicas para realizar a detecção da deriva de modelo e de anomalia, realizar a diferenciação entre eventos e aplicar o tratamento adequado de acordo com o evento. Para alcançar esse objetivo, foram definidos os seguintes objetivos específicos:

- Investigar técnicas de identificação de derivas de conceito e anomalias;
- Selecionar parâmetros que melhoram o desempenho na identificação de derivas e anomalias;
- Estabelecer estratégias que serão tomadas quando identificada uma anomalia no conjunto de dados, e quando identificada uma deriva de conceito;
- Construir um sistema que identifique e diferencie derivas de conceito e anomalias no conjunto de dados e atue de forma específica para cada evento;

- Simular cenários que se caracterizem como uma deriva de conceito e anomalias a fim de avaliar o desempenho do sistema sobre as métricas definidas anteriormente;
- Avaliar o desempenho do modelo em momentos distintos, sendo eles:
- Distribuições de dados com os eventos.
- Distribuições de dados sem os eventos.

Tendo em vista que sistemas baseados em modelos de aprendizagem de máquina estão cada vez mais presentes no cotidiano da sociedade e os impactos que as derivas de conceito e anomalias podem acarretar a esses modelos, como tomadas de decisões imprecisas causadas pela redução na precisão de modelos preditivos, a construção de um sistema capaz de identificar e diferenciar esses eventos, bem como tratar adequadamente cada um deles é essencial para garantir o desempenho, a flexibilidade e a segurança desses sistemas. Nesse sentido, o trabalho proposto não apenas contribui com o estado da arte sobre estudos relativos ao tema em questão, quanto propõe um sistema que tem potencial de garantir modelos de aprendizagem de máquina mais confiáveis.

O restante do documento está organizado da seguinte maneira: Na seção dois será detalhado o referencial teórico, iniciando com as bases conceituais sobre os significados de anomalias e derivas de conceito, assim como exemplos práticos e as consequências que esses eventos têm em sistemas de aprendizagem de máquina, em seguida serão apresentados trabalhos relacionados ao tema desse estudo. A seção três detalha a metodologia utilizada para o desenvolvimento da solução proposta. Já a seção quatro apresenta os resultados do projeto e a seção cinco encerra o documento com uma conclusão.

2- Referencial Teórico

Levando em consideração a crescente utilização de inteligência artificial em sistemas presentes no dia a dia da sociedade, torna-se essencial o entendimento das etapas envolvidas na criação de modelos de aprendizagem de máquina. Esses modelos tem por objetivo tomar decisões ou realizar previsões baseados no conhecimento adquirido através do treinamento baseado em dados coletados historicamente. Entretanto, devido a mudanças ao longo do tempo no ambiente o qual esses sistemas estão inseridos, bem como no processo de coleta de dados, eventos como derivas de conceito e anomalias podem ocorrer,

alterando a distribuição dos dados de entrada, comprometendo o desempenho do modelo. A seguir, serão apresentados conceitos chaves e trabalhos anteriores sobre o tema proposto.

2.1- Anomalias

Anomalias podem ser entendidas como eventos encontrados em um conjunto de dados que fogem do padrão esperado, tendo em vista o histórico de dados disponível. Esses desvios de padrão podem indicar erros na coleta dos dados ou acontecimentos raros. Exemplificando, encontrar uma anomalia ao analisar os acessos a determinado recurso em um sistema, pode indicar uma tentativa de invasão. No cenário de sistemas baseados em inteligência artificial, o acontecimento de anomalias pode causar falhas na tomada de decisão ou previsões incorretas, tornando assim o monitoramento e o tratamento de anomalias fatores importantes na tentativa de garantir a qualidade e confiabilidade a esses sistemas (PARK, 2018).

2.2- Deriva de conceito

Em um cenário de fluxo de dados contínuos, derivas de conceito são caracterizadas por mudanças na distribuição de valores de novas entradas em relação ao padrão observado no histórico. Essas mudanças frequentemente estão relacionadas com alterações no ambiente que os sistema está inserido, na maneira que os dados são coletados ou em falhas no processo. Por exemplo, em um cenário de coleta de dados de temperatura do ambiente, uma deriva de conceito pode indicar que o sensor utilizado para registrar a temperatura mudou ou sofreu descabrilização. Em sistemas que tem por objetivo tomar decisões ou realizar previsões baseadas nos dados recebidos através de streaming, derivas de conceito podem diminuir o desempenho dos modelos utilizados no processo em questão, sendo o tratamento das derivas de conceito um tema importante na criação desses sistemas (ILIć; STOJANOVIć, 2023).

2.3 - Trabalhos relacionados

Para ter um entendimento adequado do estado da arte na área de pesquisa ao qual o sistema proposto está inserido, foram pesquisados e analisados artigos científicos relacionados. O processo de busca aconteceu na base de artigo IEEE Xplorer (IEEE, 2025), foram escolhidos por meio da análise inicial do título e resumo quinze artigos coletados de fevereiro à abril de 2025, dos quais destacaram-se os trabalhos de El Hairach, Bellamine e Amal Tmiri (2023), Kai Wang, Ke Li, Quanhu Wang, Jinglong Jia e Tong Sun (2024), Dingsheng Deng (2020), Aleksandra I. Stojnev Ilić e Dragan Stojanović (2023), Ian Whitehouse, Rodrigo Yepez-Lopez e Roberto Corizzo (2023), Nur Laila Ab Ghani, Izzatdin

Abdul Aziz e Mazlina Mehat (2020), Elouataoui Widad, Elmendili Saida e Youssef Gahi(2023), Morris Stallmann, Anna Wilbik e Gerhard Weiss(2024).

Hairach, Bellamine e Tmiri (2023), apresentam um estudo que propõe uma maneira de comparar diferentes algoritmos de aprendizado de máquina não supervisionados para a detecção de anomalias em módulos fotovoltaicos (PVs). O trabalho entende que falhas nos sistemas, como hotspots, caixas de junção superaquecidas ou desconexões parciais, pioram o desempenho dos equipamentos que tem como objetivo a geração de energia solar. Atualmente, os métodos para encontrar esses problemas utilizam técnicas como termografia, inspeções visuais e curvas corrente-tensão (I-V), porém eles não apresentam resultados animadores, visto as limitações devido a necessidade de intervenção humana e dificuldade na escalabilidade da solução. Para tentar resolver o problema apresentado, os pesquisadores testaram os algoritmos DBSCAN, k-means, Isolation Forest e Local Outlier Factor (LOF), em dados de corrente elétrica coletados dos equipamentos. Os resultados mostram que os métodos Density-Based Spatial Clustering of Applications with Noise (DBSCAN) e K-Means obtiveram bom desempenho quando ajustamos parâmetros essenciais dos modelos (epsilon e threshold). Já o LOF demonstra alta precisão na detecção de anomalias, porém depende de conhecimento prévio sobre a contaminação para obter resultados relevantes. O trabalho destaca a importância de métodos não supervisionados para cenários onde não temos um conjunto de dados rotulados para treino.

Wang et al. (2024) aborda o tema de detecção de anomalias utilizando o modelo não supervisionado DBSCAN em conjunto com Northern Goshawk Optimization (NGO) na análise de transformadores. O pesquisador parte da premissa de que os equipamentos podem sofrer com mau funcionamento, como mau contato, falhas de conexão e sobretensão, podendo comprometer a economia energética e a segurança dos equipamentos. Métodos convencionais que envolvem detecção de anomalias através da determinação de um threshold demonstraram ser ineficientes, visto a baixa precisão e dificuldade de identificar categorias de falhas. A fim de resolver o problema proposto, o trabalho estuda o algoritmo DBSCAN em conjunto com o algoritmo NGO para a otimização dos parâmetros ε (raio de vizinhos) e *MinPts* (mínimo de pontos na vizinhança). O modelo foi treinado e avaliado sobre dados coletados de um transformador funcional durante um mês em conjunto com dados de um transformador com falhas em outro período do mesmo ano. Para avaliar o desempenho da abordagem proposta, o algoritmo NGO-DBSCAN foi comparado ao SS-DBSCAN e ao PSO-DBSCAN utilizando três métricas, sendo elas o

coeficiente de contorno, o CHI index e o DBI index, onde o algoritmo proposto no trabalho demonstrou ser o mais eficaz e efetivo na detecção de anomalias.

Deng (2020) apresenta uma abordagem de detecção de anomalias utilizando DBSCAN ao analisar dados de segurança de redes. Com os avanços tecnológicos da internet e da comunicação, crescem proporcionalmente as tentativas de invasão a sistemas e redes, as quais podem ser identificadas como anomalias ao comparar dados de acessos normais com dados de intrusos ao mesmo sistema, sendo assim a detecção de anomalias é um tema essencial na busca de garantir a segurança e a privacidade de dados. Métodos utilizados para a detecção de invasões são baseados na determinação de um “padrão normal de uso” do sistema e por isso demonstram dificuldades em detectar tipos de ataques desconhecidos. Para superar as limitações de métodos tradicionais, o autor estuda uma abordagem usando DBSCAN em comparação com K-Means, sob a ótica de tempo para identificação da anomalia e acurácia dos modelos. Foi utilizado um conjunto de dados textuais vetorizados que representam comportamentos normais e intrusivos dentro de um sistema. Os resultados destacam que o DBSCAN é mais rápido, tem maior acurácia e é menos sensível ao aumento no volume de dados.

Widad, Saida e Gahi (2023) pesquisam uma forma de detecção de anomalias de qualidade em conjuntos de dados grandes. Os autores entendem que a maioria dos métodos de detecção de anomalias trabalham sobre métricas estatísticas e não focam em irregularidades na qualidade do conjunto de dados. Para a solução desse cenário, os autores propõem um método que utiliza o algoritmo Isolation Forest combinado com um tratamento de dados realizado sob o conjunto observando seis métricas de qualidade de dados, sendo elas: acurácia, consistência, completude, conformidade, unicidade e legibilidade. Para validar a proposta os pesquisadores utilizam uma base de dados real de corridas de táxi e uma base de dados sintética, sobre a qual, o método proposto obteve alta precisão na detecção de anomalias (até 99,9%).

Ilić e Stojanović (2023) exploraram a detecção de derivas de conceito em sistemas baseados em IoT com streaming de dados bem como a adaptação de modelos ao encontrar um evento desse tipo. Tendo em vista que sistemas IoT operam em ambientes dinâmicos e sujeitos a derivas de conceito, o estudo da detecção dessas derivas se torna essencial para garantir a integridade de modelos preditivos. Para implementar uma maneira de detectar derivas e se adaptar a elas, o trabalho propõe a criação de um data stream com dados bidimensionais que simulam dados de sensores IoT, o qual contém diversas ocorrências de derivas de conceito. O conjunto de dados é formado por 150 observações com 10000

registros em cada. No estudo, foram utilizados e comparados 3 algoritmos na detecção dos eventos, em que foi observado que o PageHinkley demonstrou ser rápido no treinamento, porém registrou muitos falsos positivos; o KSWIN apresentou demora no processamento dos dados e não teve boa precisão; enquanto o ADWIN parece ser o mais viável, visto que processou os dados em 20 segundos e teve bom desempenho na detecção dos eventos.

Whitehouse, Yepez-Lopez e Corizzo (2023) propõem um workflow distribuído de detecção de derivas de conceitos e adaptação de modelos preditivos em um cenário de streaming de dados. Modelos preditivos estão cada vez mais sendo integrados em plataformas de big data; porém, não levar em consideração a ocorrência de derivas de conceito tornou-se uma grande armadilha no tema que pode tornar os modelos obsoletos no decorrer do tempo. Os métodos atuais para solucionar o problema em questão não consideram o cenário de big data, apresentam problemas de escalabilidade e não parecem ser adequados para o monitoramento e análise de dados em larga escala. Na pesquisa, os autores sugerem um workflow baseado em DDM (Drift Detection Method) com o framework Apache Spark, permitindo a execução paralela da deteção da deriva e da atualização dos modelos. Os experimentos foram realizados utilizando um modelo *Random Forest Classifier* treinado usando 2 conjuntos de dados de imagens, *Outdoor Stream* e *Rialto*. Ao analisar a solução proposta sobre as métricas de *Speedup* e *Scaleup* na identificação das derivas em cenários com 1,2,4,8 e 16 *workers*, constatou-se que a adição de workers nem sempre gera ganhos reais no tempo de execução, porém o workflow apresentou desempenho estável e viável na detecção de derivas de conceito no cenário de big data.

Ghani, Aziz e Mehat (2020) realizaram uma revisão do estado da arte sobre a detecção de derivas de conceitos aplicados à mineração de dados em data streams. Com o desenvolvimento de tecnologias como IoT e celulares, o volume de dados gerados cresceu muito e tratando-se de ambientes que podem ser acometidos de mudanças físicas frequentes, sistemas que dependem dessas tecnologias estão propensos a sofrer com mudanças na distribuição dos dados ao longo do tempo, que por sua vez podem deteriorar o desempenho de algoritmos de aprendizado de máquina. Sendo assim, os autores estudaram métodos de detecção de derivas existentes e seu processo de aprendizagem em conjuntos de dados não rotulados por meio de 242 artigos diferentes coletados nas bases de dados, Scopus, Web of Science, IEEE, ACM e ScienceDirect, os quais passaram por alguns filtros relacionados a data de publicação, idioma e tipo, restando 15 artigos para uma análise mais detalhada. Após a análise dos artigos, os autores concluem que as abordagens podem ser classificados em dois tipos, sendo estatísticas (como Kolmogorov-Smirnov test, Jaccard

Distance, Plover Algorithm e Chernoff Bound) e de aprendizagem de máquina (como *Clustering Similarities*, *Confidence Vote*, *Margin Density* e *Novelty Detection test*), onde as mais utilizadas foram respectivamente Kolmogorov-Smirnov test, Clustering Similarities, Confidence Vote e Margin Density.

Stallmann, Wilbik e Weiss (2024) apresentam um método de detectar derivas de conceito utilizando uma abordagem não supervisionada em dados de sistemas Federated Learning (FL). Nesses sistemas, os dados não estão centralizados em um único ambiente, assim dificultando a identificação de uma mudança na distribuição geral do conjunto de dados. Buscando resolver essa problemática, os autores utilizaram o algoritmo Federated Fuzzy C-Means e a técnica Federated Fuzzy Davies-Bouldin-Index; dessa maneira, o sistema foi capaz de entender a distribuição dos dados em conjunto inicial e monitorar a mudança dessa distribuição ao longo do tempo, indicando se acontece uma deriva de acordo com um threshold. A metodologia foi avaliada sobre dados sintéticos de distribuições gaussianas e constatou-se que o método foi capaz de identificar as derivas mantendo baixos valores de falsos positivos.

3- Metodologia

O presente trabalho explora o desenvolvimento de um sistema capaz de detectar derivas de conceitos e anomalias sobre dados consumidos por modelos de aprendizagem de máquina com o objetivo de apontar o retreinamento desses modelos. Os trabalhos relacionados analisados puderam ajudar na definição da metodologia e das técnicas que serão exploradas no trabalho.

3.1- Desenvolvimento de geradores de dados e detectores simples

A princípio, foram implementados algoritmos de geração de dados sintéticos com o objetivo de simular ocorrências de anomalias e derivas de conceito. Dados sintéticos devem ser entendidos como conjuntos de dados gerados através de algoritmos computacionais e não coletados no mundo real; No contexto desta pesquisa o uso deles foi essencial para o fornecimento de um ambiente controlado, cuja previsibilidade e conhecimento prévio sobre mudanças de comportamento em suas distribuições permite uma validação objetiva sobre a eficácia dos detectores de derivas. Nessa fase também foram implementados diversos módulos de detectores específicos para a identificação desses eventos de maneira automatizada. O desenvolvimento dos algoritmos foi realizado em Python com o apoio das bibliotecas como *Scikit-learn e River*.

3.2- Escolha e implementação de técnica para identificação dos eventos

Utilizando os resultados obtidos na fase anterior, na detecção dos eventos utilizando as bases de dados sintéticas e os detectores, o projeto seguiu com a seleção de técnicas definitivas para identificação dos eventos.

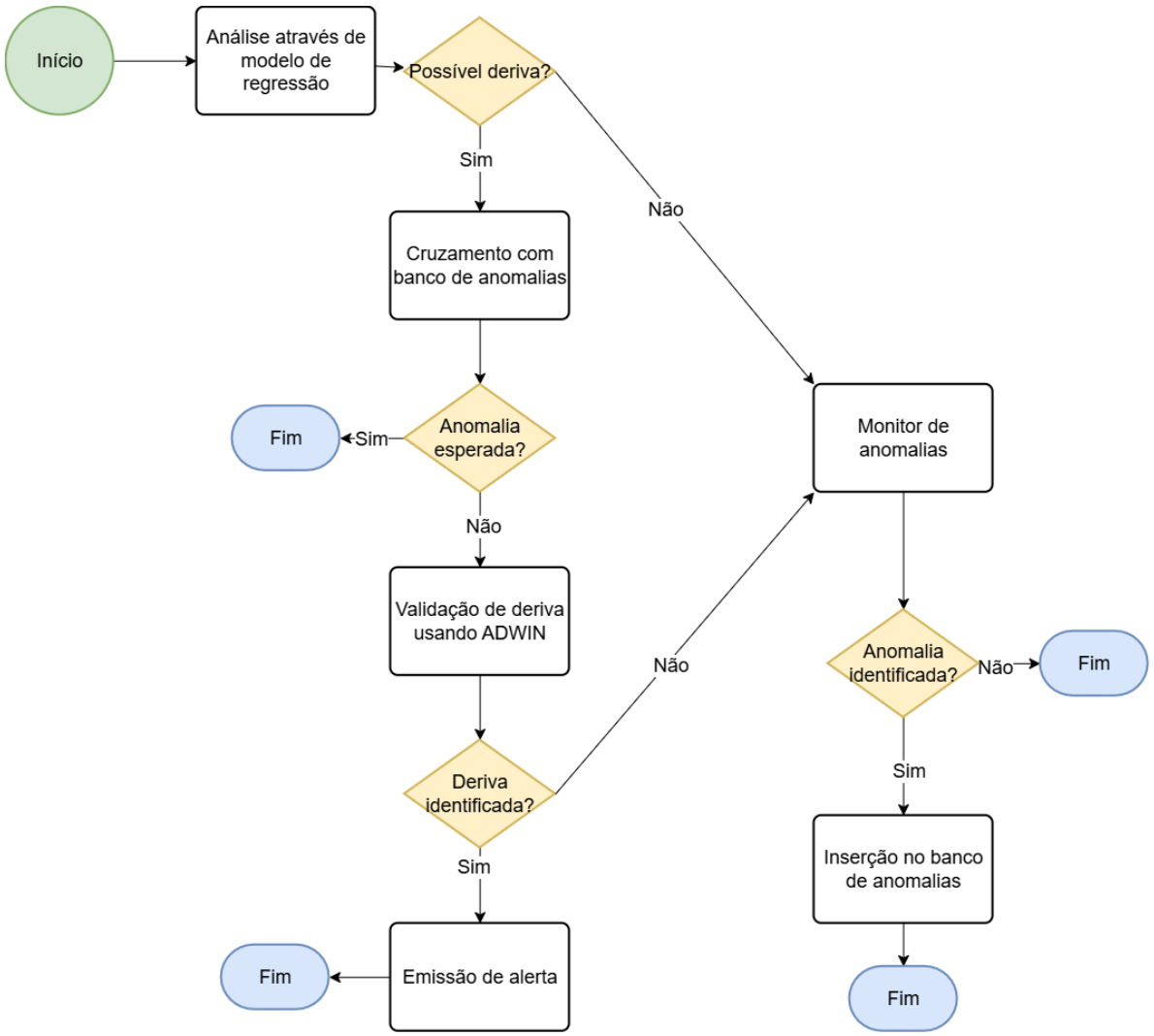
Para identificar anomalias, escolheu-se a implementação do método estatístico do Intervalo Interquartil (IQR), conhecido como “Regra do Boxplot”. Esta técnica analisa a dispersão entre as observações dentro de uma distribuição de dados, subtraindo o primeiro quartil (Q1) pelo terceiro quartil (Q3), assim estabelecendo o intervalo interquartil (IQR). Com base no valor desse intervalo, o algoritmo estabelece limites de aceitabilidade, sendo o limite inferior calculado por Q1 - 1,5 * IQR, e um limite superior, Q3 + 1,5 * IQR. Qualquer observação fora dos limites estabelecidos é classificada como anomalia.

Já para a detecção de derivas de conceito, a escolha se deu pelo algoritmo Adaptive Windowing (ADWIN). Este algoritmo analisa a distribuição de dados através de uma janela deslizante de tamanho variável e adaptada em razão da taxa de mudança dos dados. Ele divide a janela em duas, sendo uma histórica e outra contemplada pelos dados mais recentes. O sistema monitora a média de ambas as janelas e se a diferença entre elas ultrapassar um limite de confiança, assim indicando que a distribuição mudou estatisticamente, o algoritmo indica a deriva de conceito.

3.3- Estabelecer e implementar estratégias de detecção

A estrutura do algoritmo foi baseada em um fluxo de múltiplas etapas com o objetivo de mitigar falsos positivos, diferenciando anomalias “esperadas”, obtidas em um banco de anomalias do próprio sistema de reais derivas de conceito. A princípio, o fluxo de dados utiliza um modelo de regressão, que atua como primeiro filtro ao comparar a sua previsão com a distribuição real recebida pelo sistema. Em caso de uma possível deriva ser detectada, ou seja, o valor esperado pela previsão ser diferente do real, o dado é cruzado com um banco de anomalias conhecidas. Essa etapa impede que anomalias esperadas sejam erroneamente classificadas como mudanças de conceito. Se o dado não for identificado no banco, ele é submetido ao ADWIN, que irá validar e confirmar a deriva. Por outro lado, se a regressão não apontar uma possível deriva ou o ADWIN não confirmar a deriva, a amostra passa por um monitor de anomalias contínuas. Se esse monitor identificar um comportamento anômalo inédito, o dado é automaticamente registrado e inserido no banco de anomalias para verificações futuras. Todo o sistema foi implementado em Python e encapsulado em uma interface de programação de aplicações (API) utilizando o *framework* Flask. A Figura 1 apresenta o fluxograma do sistema proposto.

Figura 1 – Diagrama de decisão, ilustrando o funcionamento do sistema.



Fonte: Elaborado pelo autor.

3.4- Conteinerização do sistema

A etapa final de consolidação do projeto concentrou-se na conteinerização de todo o sistema desenvolvido. A aplicação, que engloba a API web, os algoritmos de detecção e os modelos preditivos, foi encapsulada em contêineres virtuais. Essa escolha arquitetônica teve como objetivo principal garantir a reprodutibilidade dos experimentos e o isolamento de todas as dependências e bibliotecas (como TensorFlow, PyTorch e Scikit-learn). Dessa forma, assegurou-se a alta portabilidade da solução, permitindo que a aplicação seja implantada, testada e executada de maneira consistente em diferentes infraestruturas computacionais, sem a necessidade de configurações manuais complexas do ambiente hospedeiro.

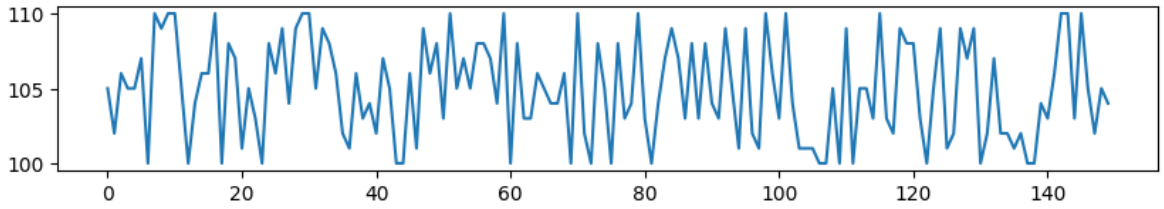
3.5- Simulação de cenários

O projeto foi finalizado avaliando o desempenho do algoritmo em cenários diversos, utilizando bases de dados sintéticas com ocorrências de derivas de conceito e anomalias. Para esse fim, foram criados 4 cenários distintos, os quais foram introduzidos no sistema, descritos a seguir.

3.5.1 - Distribuições sem anomalias ou derivas de conceito

Esse cenário representa o comportamento ideal do fluxo de dados em ambiente estável, assim a distribuição de dados se manteve constante, não havendo observações com ruídos ou mudanças de comportamento, conforme ilustrado na Figura 2.

Figura 2 – Fluxo contínuo de dados simulado em ambiente estável, isento de anomalias pontuais ou derivas de conceito.

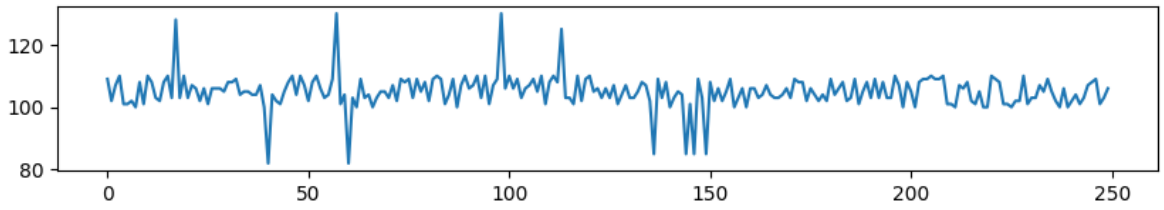


Fonte: Elaborado pelo autor.

3.5.2 - Distribuições com anomalias

Cenário onde encontram-se observações anômalas, criadas utilizando os limites do método IQR, esporadicamente, sem causar alteração no padrão histórico dos dados. A Figura 3 exemplifica visualmente o comportamento dessa série temporal.

Figura 3 – Comportamento do fluxo de dados com a injeção esporádica de anomalias isoladas.

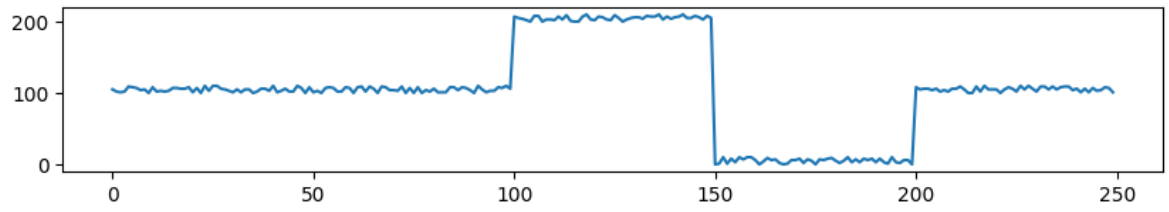


Fonte: Elaborado pelo autor.

3.5.3 - Distribuições com derivas de conceito

Cenário onde são observadas alterações na estrutura da distribuição histórica dos dados a partir de determinado momento. padrão este evidenciado no gráfico da Figura 4.

Figura 4 – Simulação de alteração estrutural na distribuição estatística dos dados, caracterizando uma deriva de conceito.

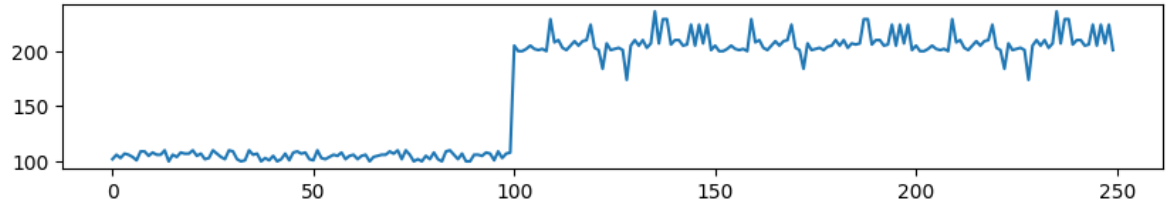


Fonte: Elaborado pelo autor.

3.5.4 - Distribuições com anomalias e derivas de conceito

Este cenário contempla tanto anomalias, quanto derivas de conceito em sua distribuição, cuja distribuição resultante é exibida na Figura 5.

Figura 5 – Fluxo de dados simulado contendo a ocorrência concomitante de anomalias isoladas e derivas de conceito.



Fonte: Elaborado pelo autor.

4 - Resultados e discussão

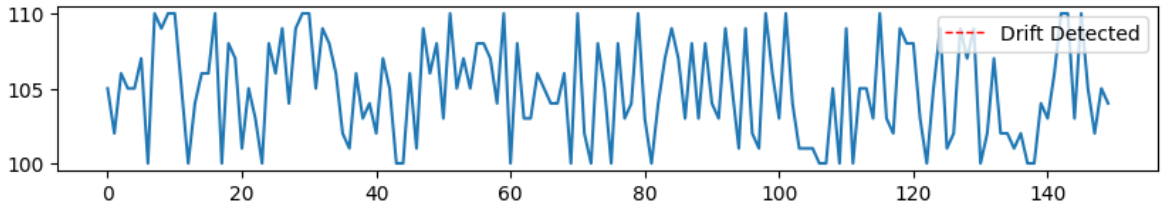
Os testes feitos para validar a arquitetura proposta apresentaram resultados promissores. Ao submeter o sistema a testes em cenários controlados, utilizando bases de dados integralmente sintéticas, a solução desenvolvida foi capaz de identificar com sucesso os eventos de derivas de conceito previamente injetadas nas bases de dados, descartando qualquer falso positivo.

Com o objetivo de ilustrar a eficácia do algoritmo, os resultados estão dispostos em acordo aos quatro cenários propostos na metodologia:

4.1.1 - Distribuições sem anomalias ou derivas de conceito

Ao processar a distribuição desse cenário, o sistema demonstrou estabilidade e nem o modelo de regressão, que funciona como primeiro validador de deriva de conceito foi ativado, sendo assim, o sistema não emitiu nenhum alarme. Os registros dessa operação estão apresentados na Figura 6.

Figura 6 – Comportamento estável do sistema operando no Cenário 1, sem emissão de alertas.

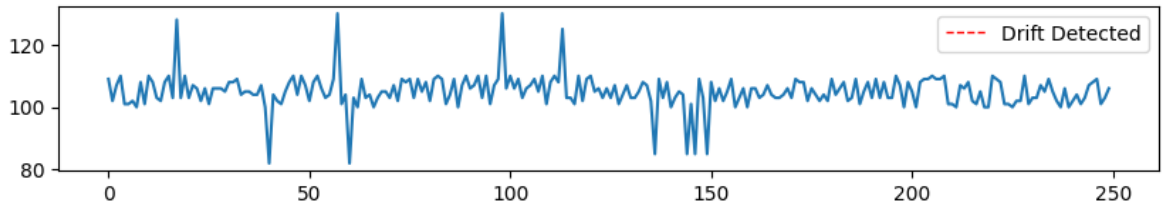


Fonte: Elaborado pelo autor.

4.1.2 - Distribuições com anomalias

No cenário onde temos a injeção de anomalias, o filtro baseado na regra do boxplot funcionou, enviando os registros para o banco de anomalias e nenhum desses eventos foi identificado com deriva de conceito, resultado ilustrado na Figura 7.

Figura 7 – Visualização do fluxo de dados com a injeção esporádica de anomalias, isoladas e tratadas pelo filtro estatístico sem gerar falsos positivos.

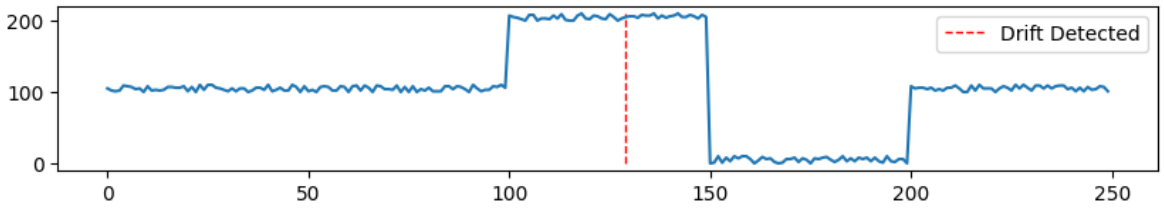


Fonte: Elaborado pelo autor.

4.1.3 - Distribuições com derivas de conceito

Nesse cenário, logo após o início da mudança de comportamento na distribuição, o sistema foi capaz de identificar o evento e emitir um alerta, que em cenário real, indicaria o retreinamento do modelo sob o qual esses dados seriam submetidos. O ponto exato dessa detecção é destacado na Figura 8.

Figura 8 – Distribuição de dados com ocorrência de deriva de conceito e marcação onde o sistema identifica o evento.



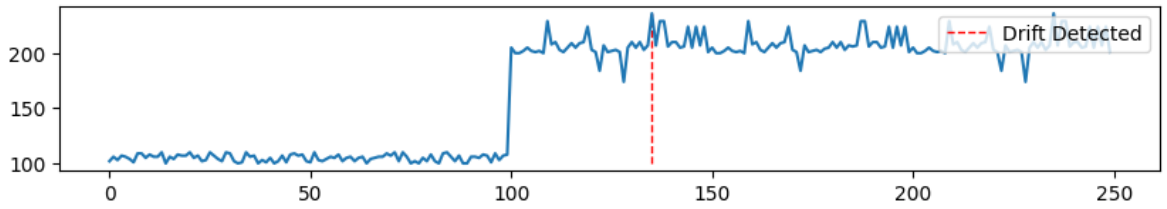
Fonte: Elaborado pelo autor.

4.1.4 - Distribuições com anomalias e derivas de conceito

No último cenário, onde a distribuição de dados refletia ambos eventos, o sistema também foi capaz de identificar as anomalias e enviar para o banco de anomalias, bem

como emitir um alerta no momento que identifica a mudança de padrão no histórico dos dados, conforme evidenciado na Figura 9.

Figura 9 – Cenário com ocorrência de deriva de conceito e anomalias e marcação no alerta de deriva de conceito.



Fonte: Elaborado pelo autor.

4.2 - Análise dos resultado

A avaliação da arquitetura permite apontar vantagens importantes quando comparadas com implementações isoladas dos algoritmos utilizados no fluxo. O ponto central aqui é a solidez em propor um pipeline a prova de falsos positivos. No estado da arte, encontram-se muitos trabalhos onde os falsos positivos são um problema recorrente e ao adotar um passo intermediário com o banco de anomalias conhecidas antes do uso do ADWIN, agrega alta confiabilidade em manter modelos de aprendizagem de máquina que utilizam o monitor para garantir a qualidade dos dados estáveis, apenas sugerindo retreinamento em caso real de deriva de conceito.

Por outro lado, vale ressaltar que a arquitetura foi validada a partir da avaliação nos resultados de sua detecção a partir de dados sintéticos, os quais tendem a ser mais controlados em relação a dados do mundo real. Sendo assim, embora validada, a arquitetura deve ser observada em ambiente produtivo a fim de validar mais ainda sua eficácia.

5 - Considerações finais

O projeto teve como objetivo desenvolver um algoritmo capaz de detectar e diferenciar ocorrências de derivas de conceito e anomalias em fluxo de dados no contexto de modelos de aprendizagem de máquina. O trabalho foi motivado por desafios constantemente observados no estado da arte e no cotidiano de profissionais inseridos no contexto: a dificuldade de sistemas inteligentes em distinguir derivas de conceitos de ruídos e eventos isolados, o que frequentemente gera falsos positivos e retreinamentos desnecessários dos modelos. Para solucionar a problemática exposta, construiu-se uma arquitetura em Python, baseada em um fluxo com múltiplas etapas de validação contendo um filtro inicial baseado em regressão, seguindo com um cruzamento de dados suspeitos

com um banco de dados de anomalias conhecidas e finalizando com a validação da deriva empregando um modelo ADWIN na distribuição de dados analisada, além de monitorar anomalias utilizando a “regra do boxplot”.

Os resultados validaram a arquitetura do projeto, respondendo de forma positiva ao problema de pesquisa. Ao submeter diferentes distribuições de dados, as quais continham ocorrências dos diferentes eventos, o sistema demonstrou 100% de eficácia em identificar as derivas de conceito previamente injetadas.

A principal contribuição desta pesquisa é a proposta técnica de desambiguação robusta, utilizando técnicas já estabelecidas no estado da arte, como regressão, IQR e ADWIN. Essa abordagem demonstra que o tratamento prévio de anomalias conhecidas atua como uma barreira protetora para a integridade de detectores de deriva de conceito. Ademais, do ponto de vista da engenharia de software, a entrega de um sistema conteinerizado agrega valor pela sua reprodutibilidade técnica e facilidade de integração em infraestruturas existentes.

A partir dessas constatações, podem ser explorados diversos novos projetos. Primordialmente, sugere-se a implementação da arquitetura proposta em conjuntos reais de dados como sensores de dispositivos IoT, a fim de avaliar a eficácia da arquitetura com dados reais.

6 - Referências

DENG, D. Research on anomaly detection method based on dbscan clustering algorithm. In: 2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT). Shenyang, China: IEEE, 2020. p. 439–442.

GHANI, N. L. A.; AZIZ, I. A.; MEHAT, M. Concept drift detection on unlabeled data streams: A systematic literature review. In: 2020 IEEE Conference on Big Data and Analytics (ICBDA). Penang, Malaysia: IEEE, 2020. p. 61–65.

HAIRACH, M. L. E.; BELLAMINE, I.; TMIRI, A. Anomaly detection in pv modules: A comparative study of dbscan, k-means, isolation forest, and lof. In: 2023 7th IEEE Congress on Information Science and Technology (CiSt). Essaouira, Morocco: IEEE, 2023. p. 135–139.

ILIć, A. I. S.; STOJANOVIć, D. Concept drift detection and adaptation in iot data stream analytics. In: 2023 16th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS). Nis, Serbia: IEEE, 2023. p. 211–214.

STALLMANN, M.; WILBIK, A.; WEISS, G. Towards unsupervised sudden data drift detection in federated learning with fuzzy clustering. In: 2024 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE). Yokohama, Japan: IEEE, 2024. p. 1–8.

WANG, K. et al. Anomaly detection of transformer based on ngo and dbscan. In: 2024 4th Power System and Green Energy Conference (PSGEC). Shanghai, China: IEEE, 2024. p. 963–967.

WHITEHOUSE, I.; YEPEZ-LOPEZ, R.; CORIZZO, R. Distributed concept drift detection for efficient model adaptation with big data streams. In: 2023 IEEE International Conference on Big Data (BigData). Sorrento, Italy: IEEE, 2023. p. 5392–5397.

WIDAD, E.; SAIDA, E.; GAHI, Y. Quality anomaly detection using predictive techniques: An extensive big data quality framework for reliable data analysis. IEEE Access, Institute of Electrical and Electronics Engineers (IEEE), v. 11, p. 103306–103318, 2023.

Contatos: luiz.felipetaa@gmail.com e gustavo.sampaio@mackenzie.br