O'REILLY®

Helion

MLOps dla biznesu

Wdrażanie i skalowanie modeli uczenia maszynowego

Mark Treveil
Zespół Dataiku

Tytuł oryginału: Introducing MLOps: How to Scale Machine Learning in the Enterprise

Tłumaczenie: Piotr Rajca

ISBN: 978-83-289-3882-3

© 2026 Helion S.A.

Authorized Polish translation of the English edition of *Introducing MLOps*
ISBN 9781492083290 © 2021 Dataiku.

This translation is published and sold by permission of O'Reilly Media, Inc.,
which owns or controls all rights to publish and sell the same.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiejkolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także ko piowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/mlobiz
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

- Kup książkę
- Poleć książkę
- Oceń książkę

- Księgarnia internetowa
- Lubię to! » Nasza społeczność

Spis treści

Wstęp **9**

Część I. MLOps: Co to takiego i dlaczego jest ważne? 11

1. Dlaczego teraz i na jakie wyzwania odpowiada? **13**
Definicja MLOps i związane z nimi wyzwania 14
Operacje MLOps w celu ograniczenia ryzyka 17
Ocena ryzyka 17
Ograniczanie ryzyka 18
Operacje MLOps w odpowiedzialnym rozwoju sztucznej inteligencji 19
MLOps w dużej skali 20
Podsumowanie 20

2. Ludzie MLOps **23**
Eksperci dziedzinowi 25
Naukowcy ds. danych 27
Inżynierowie danych 29
Inżynierowie oprogramowania 30
Specjaliści DevOps 30
Menadżerowie ryzyka modeli i audytorzy 31
Architekci uczenia maszynowego 32
Podsumowanie 32

3. Kluczowe funkcje MLOps **35**
Wprowadzenie do uczenia maszynowego 35
Tworzenie modeli 36
Wyznaczanie celów biznesowych 36
Źródła danych i analiza eksploracyjna 36
Projektowanie i dobór cech 37

Kup książkę Poleć książkę

Trenowanie i ocenianie 38
Powtarzalność 38
Odpowiedzialna sztuczna inteligencja 38
Wdrażanie i uruchamianie 39
Rodzaje wdrożeń i zawartość modeli 40
Wymagania wdrożeniowe dla modeli 41
Monitorowanie 41
Zagadnienia DevOps 42
Wyzwania dla naukowców ds. danych 42
Kwestie biznesowe 43
Powtarzanie i cykl życia 44
Powtarzanie 44
Pętla sprzężenia zwrotnego 45
Zarządzanie 47
Zarządzanie danymi 48
Zarządzanie procesem 49
Podsumowanie 50

Część II. MLOps: Jak to zrobić? 51

4. Tworzenie modeli 53
Czym jest model uczenia maszynowego? 54
W teorii 54
W praktyce 55
Niezbędne komponenty 56
Różne algorytmy uczenia maszynowego, różne wyzwania MLOps 56
Eksploracja danych 58
Projektowanie i dobór cech 58
Techniki inżynierii cech 59
Jak dobór cech wpływa na strategię MLOps? 60
Eksperymentowanie 61
Ocena i porównywanie modeli 63
Wybór miar oceny 63
Weryfikacja zachowania modelu 65
Wpływ odpowiedzialnej sztucznej inteligencji na modelowanie 65
Zarządzanie wersjami i możliwości odtwarzania 68
Podsumowanie 70

Kup książkę Poleć książkę

5. Przygotowanie do wdrożenia 71
Środowiska uruchomieniowe 72
Dostosowanie na drodze od środowisk rozwojowych do produkcyjnych 72
Dostęp do danych przed weryfikacją i wdrożeniem w środowisku produkcyjnym 74
Końcowe przemyślenia na temat środowisk uruchomieniowych 74
Ocena ryzyka modelu 75
Cel walidacji modelu 75
Źródła ryzyka w modelach uczenia maszynowego 75
Zapewnienie jakości w uczeniu maszynowym 76
Kluczowe aspekty testowania 77
Możliwości odtwarzania i weryfikacji 78
Bezpieczeństwo uczenia maszynowego 79
Ataki adwersarialne 79
Inne luki w zabezpieczeniach 80
Ograniczanie ryzyka modeli 81
Zmieniające się środowiska 81
Współdziałanie modeli 82
Niewłaściwe zachowanie modelu 83
Podsumowanie 84

6. Wdrażanie w środowisku produkcyjnym 85
Potoki CI/CD 85
Tworzenie artefaktów uczenia maszynowego 87
Czym jest artefakt uczenia maszynowego? 87
Potok testowy 87
Strategie wdrażania 89
Rodzaje wdrażania modeli 89
Co brać pod uwagę podczas wdrażania modeli w środowisku produkcyjnym? 90
Utrzymanie w środowisku produkcyjnym 91
Konteneryzacja 91
Rozbudowa wdrożeń 93
Wymagania i wyzwania 95
Podsumowanie 95

7. Monitorowanie i pętla zwrotna 97
Jak często należy ponownie szkolić modele? 98
Zrozumienie degradacji modelu 101
Ocena danych rzeczywistych 101
Wykrywanie zmian wejściowych 103
Wykrywanie dryfu w praktyce 104
Przykładowe przyczyny dryfu danych 104
Metody wykrywania dryfu w danych wejściowych 105

Kup książkę Poleć książkę

Pętla sprzężenia zwrotnego 107
Rejestrowanie 108
Ocenianie modelu 108
Ocena online 111
Podsumowanie 113

8. Zarządzanie modelami ... 115
Kto decyduje o potrzebnych zasadach zarządzania organizacją? 115
Dostosowanie zarządzania do poziomu ryzyka 117
Obecne przepisy kształtujące zarządzanie MLOps 118
Regulacje farmaceutyczne w USA: Dobre praktyki 118
Zarządzanie ryzykiem modeli finansowych 119
Przepisy o ochronie danych osobowych RODO i CCPA 120
Nowa fala regulacji dotyczących sztucznej inteligencji 121
Pojawienie się odpowiedzialnej sztucznej inteligencji 122
Kluczowe aspekty odpowiedzialnej sztucznej inteligencji 123
Element 1: Dane 123
Element 2: Stronniczość 124
Element 3: Inkluzywność 125
Element 4: Zarządzanie modelami na dużą skalę 126
Element 5: Nadzór 126
Szablon nadzoru nad operacjami uczenia maszynowego 127
Krok 1: Zrozumienie i klasyfikacja przypadków użycia analizy danych 128
Krok 2: Ustalenie stanowiska etycznego 128
Krok 3: Określenie zakresów odpowiedzialności 129
Krok 4: Ustalenie zasad zarządzania 130
Krok 5: Włączenie zasad do procesu MLOps 131
Krok 6: Wybór narzędzi do scentralizowanego zarządzania 133
Krok 7: Angażowanie i dokształcanie 134
Krok 8: Monitorowanie i udoskonalanie 134
Podsumowanie 135

Część III. MLOps: Przykłady z rzeczywistego świata 137

9. MLOps w praktyce: Zarządzanie ryzykiem kredytowym klientów ... 139
Kontekst: Biznesowy przypadek użycia 139
Tworzenie modeli 140
Aspekty stronniczości modeli 140
Przygotowanie do wdrożenia 141
Wdrożenie w środowisku produkcyjnym 142
Podsumowanie 143

Kup książkę Poleć książkę

10. MLOps w praktyce: Silniki rekomendacji dla marketingu 145
Rozwój systemów rekomendacji 145
Znaczenie uczenia maszynowego 146
Wysyłać czy pobierać? 146
Przygotowanie danych 147
Projektowanie i zarządzanie eksperymentami 147
Trenowanie i wdrażanie modeli 148
Skalowalność i możliwość dostosowania 149
Strategia monitorowania i ponownego szkolenia 150
Ocenianie w czasie rzeczywistym 150
Możliwość włączania i wyłączania rekomendacji 150
Struktura i strategia wdrażania potoków 151
Monitorowanie i informacje zwrotne 152
Ponowne trenowanie modeli 152
Aktualizowanie modeli 152
Działa w nocy, śpi w ciągu dnia 153
Możliwość ręcznego sterowania modelami 153
Opcja automatycznego sterowania modelami 153
Monitorowanie wydajności 154
Podsumowanie 154

11. MLOps w praktyce: Prognozowanie zużycia 157
Systemy zasilania 157
Gromadzenie danych 159
Określenie problemu: Stosować uczenie maszynowe czy nie? 160
Rozdzielczość przestrzenna i czasowa 160
Implementacja 162
Modelowanie 163
Wdrożenie 165
Monitorowanie 165
Podsumowanie 166

Kup książkę Poleć książkę

Kup książkę Poleć książkę

ROZDZIAŁ 3.

Kluczowe funkcje MLOps

Mark Treveil

Praktyki MLOps mają wpływ na wiele różnych ról w organizacji, a co za tym idzie, na wiele etapów cyklu życia uczenia maszynowego. Ten rozdział przedstawia w stosunkowo ogólny sposób pięć kluczowych elementów MLOps: tworzenie, wdrażanie, monitorowanie, iterację i zarządzanie. Zamieszczone w nim informacje będą podstawą dla zagadnień opisywanych w rozdziałach od 4. do 8., które są poświęcone prezentacji bardziej technicznych szczegółów i wymagań tych elementów MLOps.

Wprowadzenie do uczenia maszynowego

Aby zrozumieć kluczowe aspekty MLOps, należy najpierw poznać zasady działania uczenia maszynowego i jego specyfikę. Wybór algorytmu (czyli sposób budowania modeli uczenia maszynowego), choć często pomijany w kontekście procesów MLOps, może mieć na nie bezpośredni wpływ.

W swojej istocie uczenie maszynowe to dziedzina zajmująca się algorytmami komputerowymi, które nie są jawnie definiowane w formie kodu, lecz zamiast tego automatycznie uczą się i doskonalą w oparciu o zdobywane doświadczenia. Algorytmy analizują dane przykładowe, zwane danymi treningowymi, aby na ich podstawie zbudować model programowy zdolny do dokonywania predykcji.

Na przykład model rozpoznawania obrazów może identyfikować typ licznika energii elektrycznej na zdjęciu, wyszukując kluczowe wzorce odróżniające poszczególne typy liczników. Innym przykładem jest model rekomendacji ubezpieczeń, który, bazując na wcześniejszym zachowaniu podobnych klientów, może sugerować dodatkowe produkty ubezpieczeniowe, które dany klient najprawdopodobniej kupi.

W obliczu nowych, niewidzianych wcześniej danych, czy to zdjęcia, czy klienta, model uczenia maszynowego wykorzystuje wiedzę zdobytą w trakcie treningu, aby dokonać najlepszej możliwej predykcji, zakładając, że nowe dane są w pewien sposób powiązane z poprzednimi.

Kup książkę Poleć książkę

Algorytmy uczenia maszynowego wykorzystują szeroki zakres technik matematycznych, a modele mogą przybierać różne formy — od prostych drzew decyzyjnych, przez algorytmy regresji logistycznej, aż po znacznie bardziej złożone modele głębokiego uczenia (szczegółowe informacje na temat modeli uczenia maszynowego można znaleźć w rozdziale 4. w podrozdziale pt. „Czym jest model uczenia maszynowego?").

Tworzenie modeli

Przyjrzyjmy się nieco dokładniej całościowemu procesowi tworzenia modeli uczenia maszynowego, aby lepiej zrozumieć jego elementy składowe, które po wdrożeniu mogą mieć wpływ na procesy MLOps.

Wyznaczanie celów biznesowych

Proces tworzenia modelu uczenia maszynowego zazwyczaj zaczyna się od określenia celu biznesowego. Może to być na przykład ograniczenie liczby oszukańczych transakcji do poziomu poniżej 0,1% lub umożliwienie identyfikacji twarzy osób na zdjęciach w mediach społecznościowych. Celom biznesowym naturalnie towarzyszą docelowe wskaźniki wydajności, wymagania dotyczące infrastruktury technicznej oraz ograniczenia kosztowe. Wszystkie te czynniki można ująć w postaci kluczowych wskaźników efektywności (ang. *key performance indicators*, KPI), które umożliwią monitorowanie wydajności biznesowej modeli w środowisku produkcyjnym.

Ważne jest, aby zdawać sobie sprawę, że projekty uczenia maszynowego nie powstają w próżni. Zazwyczaj są one częścią większego przedsięwzięcia, które z kolei wpływa na technologie, procesy i ludzi. Oznacza to, że część procesu ustalania celów obejmuje również zarządzanie zmianą, co może nawet dostarczać wskazówek dotyczących sposobu przygotowania modelu uczenia maszynowego. Na przykład wymagany stopień przejrzystości będzie miał duży wpływ na wybór algorytmów i może wymusić konieczność dostarczania nie tylko samych prognoz, lecz także związanych z nimi wyjaśnień, dzięki którym prognozy te będą mogły być przekształcane w wartościowe decyzje biznesowe.

Źródła danych i analiza eksploracyjna

Po zdefiniowaniu jasnych celów biznesowych nadchodzi czas, aby zebrać ekspertów dziedzinowych oraz naukowców ds. danych i rozpocząć proces tworzenia modelu uczenia maszynowego. Zaczyna się on od poszukiwania odpowiednich danych wejściowych. Znalezienie danych może wydawać się proste, ale w praktyce często okazuje się, że jest to najbardziej żmudna część całego procesu.

Kluczowe pytania dotyczące pozyskiwania danych do budowy modeli uczenia maszynowego to:

- Jakie istotne zbiory danych są dostępne?
- Czy te dane są wystarczająco dokładne i wiarygodne?
- W jaki sposób zainteresowane strony mogą uzyskać dostęp do tych danych?

Kup książkę Poleć książkę

- Jakie właściwości danych (zwane *cechami*) można uzyskać poprzez połączenie wielu źródeł?
- Czy te dane będą dostępne w czasie rzeczywistym?
- Czy istnieje potrzeba oznaczenia części danych jako „danych wzorcowych” (ang. *ground truth*), które będą miały być przewidywane, czy może lepiej zastosować uczenie nienadzorowane? Jakie koszty, pod względem czasu i zasobów, pociąga za sobą podjęcie każdej z tych decyzji?
- Jakiej platformy należy użyć?
- W jaki sposób dane będą aktualizowane po wdrożeniu modelu?
- Czy samo wykorzystanie modelu zmniejszy reprezentatywność danych?
- W jaki sposób będą mierzone kluczowe wskaźniki efektywności, ustalone na etapie określania celów biznesowych?

Ograniczenia związane z zarządzaniem danymi rodzą jeszcze więcej pytań, takich jak:

- Czy do tego celu można wykorzystać wybrane zbiory danych?
- Jakie są warunki użytkowania?
- Czy istnieją dane osobowe, które muszą zostać usunięte lub zanonimizowane?
- Czy istnieją cechy, takie jak płeć, których prawnie nie można wykorzystać w danym kontekście biznesowym?
- Czy mniejszości są wystarczająco dobrze reprezentowane, aby model miał taką samą skuteczność dla każdej grupy?

Ponieważ dane są kluczowym składnikiem zasilającym algorytmy uczenia maszynowego, przed próbą trenowania modeli zawsze warto dołożyć starań, by zrozumieć wzorce występujące w danych. Techniki eksploracyjnej analizy danych (ang. *exploratory data analysis*, EDA) mogą pomóc w tworzeniu hipotez na temat danych, identyfikacji wymagań dotyczących oczyszczania tych danych, jak również w procesie wyboru potencjalnie istotnych cech. Eksploracyjną analizę danych można wykonywać wizualnie, co zapewnia możliwości bardziej intuicyjnego określania wniosków, jak również statystycznie, jeśli wymagana jest większa dokładność.

Projektowanie i dobór cech

Eksploracyjna analiza danych w naturalny sposób prowadzi do inżynierii cech i ich selekcji. Inżynieria cech to proces przekształcania surowych danych z wybranych zbiorów w „cechy”, które lepiej reprezentują rozwiązywany problem. „Cechy” to tablice liczb o stałym rozmiarze, ponieważ tylko takie obiekty są zrozumiałe dla algorytmów uczenia maszynowego. Inżynieria cech obejmuje także czyszczenie danych, które, w kategoriach poświęcanego czasu, może stanowić największą część projektu uczenia maszynowego. Więcej szczegółowych informacji na ten temat można znaleźć w rozdziale 4., w podrozdziale pt. „Projektowanie i dobór cech”.

Kup książkę Poleć książkę

Trenowanie i ocenianie

Po przygotowaniu danych poprzez projektowanie i dobór cech kolejnym krokiem jest trenowanie modelu. Trenowanie i optymalizacja nowego modelu uczenia maszynowego jest procesem iteracyjnym — testowanych może być kilka algorytmów, cechy mogą być generowane automatycznie, wybrane cechy mogą być dostosowywane, a hiperparametry algorytmów mogą być dostrajane. Oprócz swojej iteracyjnej natury (a często właśnie z jej powodu) trenowanie jest również najbardziej wymagającym obliczeniowo etapem cyklu życia modelu uczenia maszynowego.

Śledzenie wyników każdego eksperymentu podczas iteracji szybko staje się złożonym zagadnieniem. Dla naukowców ds. danych nie ma nic bardziej frustrującego niż brak możliwości odtwarzania najlepszych wyników z powodu zapomnienia szczegółowych informacji konfiguracyjnych. Zastosowanie narzędzia do śledzenia eksperymentów może znacznie uprościć proces zapamiętywania danych, selekcji cech i parametrów modelu wraz z metrykami wydajności. Narzędzia tego typu pozwalają także na porównywanie eksperymentów, co z kolei ułatwia analizowanie różnic w wydajności.

Decyzja o tym, które rozwiązanie jest najlepsze, wymaga zarówno kryteriów ilościowych, takich jak dokładność czy średni błąd, jak i kryteriów jakościowych związanych z możliwościami wyjaśniania działania i wyników algorytmu lub łatwości jego wdrożenia.

Powtarzalność

Choć wiele eksperymentów może mieć raczej krótkotrwałą przydatność, to jednak istotne wersje modelu należy zachowywać do ewentualnego późniejszego wykorzystania. W tym kontekście sporym wyzwaniem jest zapewnienie możliwości odtwarzania modelu, co stanowi ważną koncepcję w nauce eksperymentalnej. W przypadku uczenia maszynowego chodzi o możliwość zapisania wystarczającej ilości informacji o środowisku, w którym model został opracowany, aby można było odtworzyć ten model od podstaw, tak by zwracał identyczne wyniki.

Bez zapewnienia takich możliwości odtwarzania naukowcy ds. danych mają niewielkie szanse na prowadzenie cyklicznych prac rozwojowych nad modelem, a co gorsza, prawdopodobnie nie będą w stanie przekazać go zespołowi DevOps, aby sprawdzić, czy to, co stworzono w laboratorium, da się wiernie odtworzyć w środowisku produkcyjnym. Prawdziwe możliwości odtwarzania modelu wymagają kontrolowania wersji wszystkich zasobów i parametrów, w tym danych użytych do trenowania i oceniania modelu, a także zapisu stanu środowiska programistycznego (więcej informacji na ten temat można znaleźć w rozdziale 4., w podrozdziale pt. „Zarządzanie wersjami i odtwarzalność”).

Odpowiedzialna sztuczna inteligencja

Możliwość odtworzenia modelu to tylko część wyzwania związanego z operacjonalizacją. Zespół DevOps musi również wiedzieć, jak zweryfikować model (tzn. sprawdzić, co model robi, jak należy go testować i jakich wyników można się spodziewać). W branżach podlegających ścisłym regulacjom często wymagane jest dokumentowanie jeszcze większej liczby szczegółowych informacji, w tym sposobu budowania i dostrajania modelu. W krytycznych przypadkach model może wymagać niezależnego przepisania i przebudowy.

Kup książkę Poleć książkę

Standardowym rozwiązaniem tego wyzwania komunikacyjnego wciąż pozostaje dokumentacja. Zadanie to można sobie jednak ułatwić przez wykorzystanie automatycznego generowania dokumentacji modelu, czyli użycie narzędzia, które automatycznie generuje dokumentacje każdego wytrenowanego modelu. Jednak w prawie wszystkich przypadkach część dokumentacji i tak trzeba będzie napisać ręcznie, aby wyjaśnić podjęte decyzje.

Ze względu na statystyczny charakter modeli uczenia maszynowego ich zrozumienie stanowi wyzwanie. Choć istnieją standardowe miary do oceniania skuteczności algorytmów modelowania, to jednak nie wyjaśniają one, w jaki sposób dokonywane są prognozy. Zrozumienie tego „jak" jest ważne dla sprawdzenia poprawności działania modelu lub lepszego zaprojektowania cech. Co więcej, wiedza ta może być konieczna do spełnienia wymagań dotyczących uczciwości (np. w odniesieniu do cech takich jak płeć, wiek czy rasa). Ten aspekt możliwości wyjaśniania działania modeli uczenia maszynowego jest powiązany z zagadnieniami odpowiedzialnej sztucznej inteligencji, o których wspomniano w rozdziale 1. i które zostaną szerzej opisane w rozdziale 4.

Techniki zapewniające możliwości wyjaśniania działania modeli uczenia maszynowego stają się coraz ważniejsze w miarę rosnących globalnych obaw dotyczących wpływu niekontrolowanej sztucznej inteligencji. Oferują one sposób na złagodzenie niepewności i zapobieganie niezamierzonym konsekwencjom. Do najczęściej stosowanych spośród tych technik należą:

- Wykresy częściowej zależności, które analizują marginalny wpływ cech na przewidywany wynik.
- Analizy podpopulacji, które badają, jak model traktuje określone podgrupy, i stanowią podstawę wielu analiz uczciwości.
- Indywidualne przewidywania modelu, takie jak wartości Shapleya[1], które wyjaśniają, jak wartość każdej cechy przyczynia się do konkretnej predykcji.
- Analiza „co-jeśli", która pomaga użytkownikowi modelu uczenia maszynowego zrozumieć wrażliwość prognozy na jej dane wejściowe.

Jak widzieliśmy w tym podrozdziale, mimo że tworzenie modelu odbywa się na bardzo wczesnym etapie, nadal jest to ważne miejsce do wdrożenia praktyk MLOps. Wszelkie prace związane z MLOps wykonane na początku, podczas etapu tworzenia modelu, ułatwią zarządzanie modelami na późniejszych etapach prac (szczególnie przy wdrażaniu w środowisku produkcyjnym).

Wdrażanie i uruchamianie

Wdrażanie modeli w środowisku produkcyjnym stanowi kluczowy element metodyki MLOps, który niesie ze sobą zupełnie inne wyzwania techniczne niż samo tworzenie modelu. Jest to domena inżynierów oprogramowania i zespołu DevOps. Koniecznie należy zwrócić uwagę na wyzwania organizacyjne związane z zarządzaniem wymianą informacji między naukowcami ds. danych a tymi zespołami. Jak wspomniano w rozdziale 1., bez skutecznej współpracy między zespołami opóźnienia lub niepowodzenia we wdrażaniu są nieuniknione.

[1] *https://towardsdatascience.com/the-shapley-value-for-ml-models-f1100bff78d1/*.

Kup książkę Poleć książkę

Rodzaje wdrożeń i zawartość modeli

Aby zrozumieć, co dzieje się w tych fazach, warto cofnąć się o krok i zadać pytanie: co dokładnie trafia do środowiska produkcyjnego i z czego składa się model? Zazwyczaj można wyróżnić dwa rodzaje wdrożeń modeli uczenia maszynowego:

Model jako usługa lub model oceniający w czasie rzeczywistym

Zwykle model jest wdrażany w prostym środowisku, aby zapewnić możliwość udostępnienia interfejsu API REST. Punkt końcowy API (środki, dzięki którym API może uzyskać dostęp do zasobów potrzebnych do wykonania zadania) odpowiada na żądania w czasie rzeczywistym.

Model wbudowany

W tym przypadku model jest umieszczany wewnątrz aplikacji, która jest następnie publikowana. Typowym przykładem jest aplikacja, która pozwala na wsadowe ocenianie żądań.

To, z czego składają się modele gotowe do wdrożenia, zależy oczywiście od wybranej technologii, ale zazwyczaj obejmują one zestaw kodu (najczęściej napisanego w języku Python, R lub Java) oraz artefakty danych. Każdy z tych elementów może być uzależniony od konkretnych wersji środowiska uruchomieniowego lub pakietów, które muszą być zgodne ze środowiskiem produkcyjnym, ponieważ użycie różnych wersji może spowodować różnice w predykcjach modelu.

Jednym ze sposobów na zmniejszenie zależności od środowiska produkcyjnego jest eksportowanie modelu do przenośnego formatu, takiego jak PMML, PFA, ONNX lub POJO. Mają one na celu poprawę przenośności modelu między systemami i uproszczenie wdrażania. Wiąże się to jednak z pewnymi kosztami: każdy format obsługuje ograniczony zakres algorytmów, a czasami przenośne modele zachowują się w subtelnie inny sposób niż oryginalne. Dlatego decyzję o użyciu jednego z tych przenośnych formatów należy podejmować po dokładnym zrozumieniu kontekstu technologicznego i biznesowego.

Konteneryzacja

Konteneryzacja to coraz popularniejsze rozwiązanie problemów związanych z zależnościami przy wdrażaniu modeli uczenia maszynowego. Technologie kontenerowe, takie jak Docker, są lżejszą alternatywą dla maszyn wirtualnych, umożliwiając wdrażanie aplikacji w niezależnych, samodzielnych środowiskach, które dokładnie odpowiadają wymaganiom każdego modelu.

Umożliwiają one również płynne wdrażanie nowych modeli przy użyciu techniki wdrażania typu *blue-green*[2]. Zasoby obliczeniowe dla modeli można elastycznie skalować, wykorzystując wiele kontenerów. Z kolei do orkiestracji — zarządzania działaniem wielu kontenerów — można skorzystać z takich technologii jak Kubernetes, których z powodzeniem można używać zarówno w chmurze, jak i lokalnie.

[2] Dokładne wyjaśnienie tej techniki wymagałoby więcej miejsca, niż możemy na nie poświęcić w tej książce. Więcej informacji na jej temat można znaleźć na blogu Martina Fowlera, we wpisie pod adresem *https://martinfowler.com/bliki/BlueGreenDeployment.html*.

Kup książkę Poleć książkę

Wymagania wdrożeniowe dla modeli

A co z procesem przygotowania do wykorzystania produkcyjnego, pomiędzy zakończeniem tworzenia modelu a jego fizycznym wdrożeniem — co należy uwzględnić w jego kontekście? Jedno jest pewne: szybkie, zautomatyzowane wdrożenie jest zawsze preferowane w stosunku do pracochłonnych procesów.

W przypadku aplikacji samoobsługowych o krótkim czasie życia często nie ma potrzeby martwić się o testowanie i walidację. Jeśli maksymalne zapotrzebowanie na zasoby modelu można bezpiecznie ograniczyć za pomocą technologii takich jak Linux cgroups, to w pełni zautomatyzowane jednoetapowe wdrożenie może być całkowicie wystarczające. Tego lekkiego trybu wdrażania można używać nawet w przypadku konieczności obsługi prostych interfejsów użytkownika, tworzonych przy użyciu takich frameworków jak Flask. Oprócz zintegrowanych platform do nauki o danych i uczenia maszynowego niektóre systemy zarządzania regułami biznesowymi mogą również umożliwiać pewnego rodzaju autonomiczne wdrażanie podstawowych modeli ML.

Jednak w przypadkach krytycznych dla klienta wymagane jest zastosowanie bardziej solidnego potoku CI/CD. Zazwyczaj obejmuje on:

1. Upewnienie się, że zostały spełnione wszystkie standardy tworzenia kodu, dokumentacji i zatwierdzania.
2. Odtworzenie modelu w środowisku zbliżonym do produkcyjnego.
3. Ponowną walidację dokładności modelu.
4. Przeprowadzenie kontroli możliwości wyjaśniania działania rozwiązania i generowanych wyników.
5. Upewnienie się, że zostały spełnione wszystkie wymagania dotyczące zarządzania.
6. Sprawdzenie jakości wszelkich artefaktów danych.
7. Testowanie wykorzystania zasobów pod obciążeniem.
8. Osadzanie w bardziej złożonej aplikacji, w tym testy integracyjne.

W branżach podlegających ścisłym regulacjom (np. finansowej i farmaceutycznej) kontrole związane z zarządzaniem i przepisami będą rozbudowane i prawdopodobnie będą wymagać ręcznej interwencji. W podejściu MLOps, podobnie jak w DevOps, dąży się do jak największej automatyzacji potoku CI/CD. Nie tylko przyspiesza to proces wdrażania, ale także umożliwia przeprowadzenie bardziej rozbudowanych testów regresyjnych i zmniejsza prawdopodobieństwo wystąpienia błędów podczas wdrożenia.

Monitorowanie

Po wdrożeniu modelu do środowiska produkcyjnego kluczowe jest, aby pomimo upływu czasu wciąż działał on dobrze. Jednak określenie „dobre działanie” dla różnych osób może oznaczać co innego; w szczególności dotyczy to zespołu DevOps, naukowców ds. danych i działu biznesowego.

Kup książkę Poleć książkę

Zagadnienia DevOps

Problemy zespołów DevOps są dobrze znane i obejmują konieczność znajdowania odpowiedzi na takie pytania jak:

- Czy model wykonuje swoje zadanie wystarczająco szybko?
- Czy zużywa rozsądną ilość pamięci i czasu procesora?

Znajdowanie odpowiedzi na takie pytanie to tradycyjne zadania monitorowania wydajności systemów IT, w którym zespoły DevOps mają już duże doświadczenie. Wymagania modeli uczenia maszynowego co do niezbędnych zasobów nie różnią się pod tym względem znacząco od tradycyjnego oprogramowania.

Skalowalność zasobów obliczeniowych może być ważnym czynnikiem na przykład przy ponownym trenowaniu modeli w środowisku produkcyjnym. Modele głębokiego uczenia mają znacznie większe wymagania pod względem zasobów niż prostsze drzewa decyzyjne. Ogólnie jednak wiedzę z zakresu monitorowania i zarządzania zasobami, którą dysponują zespoły DevOps, można łatwo wykorzystać do zarządzania modelami uczenia maszynowego.

Wyzwania dla naukowców ds. danych

Naukowcy ds. danych interesują się monitorowaniem modeli uczenia maszynowego z nowego, bardziej wymagającego powodu: modele te mogą wraz z upływem czasu tracić na skuteczności, ponieważ są w istocie odzwierciedleniem danych, na których zostały wytrenowane. Nie jest to problem występujący w tradycyjnym oprogramowaniu, stanowi natomiast nieodłączną cechę uczenia maszynowego. Operacje matematyczne wykorzystywane w rozwiązaniach uczenia maszynowego tworzą zwięzłą reprezentację istotnych wzorców występujących w danych treningowych, z założeniem, że przygotowane modele będą dobrym odzwierciedleniem rzeczywistości. Jeśli dane treningowe dobrze oddają rzeczywistość, model powinien być dokładny, a tym samym użyteczny.

Jednak świat rzeczywisty nie stoi w miejscu. Dane treningowe użyte do zbudowania modelu wykrywania oszustw pół roku temu nie będą odzwierciedlać nowego typu oszustw, które pojawiły się w ciągu ostatnich trzech miesięcy. Jeśli dana strona internetowa zacznie przyciągać coraz młodszych użytkowników, model generujący reklamy prawdopodobnie będzie tworzyć coraz mniej trafne ogłoszenia. W pewnym momencie wydajność stanie się nie do przyjęcia i konieczne będzie ponowne wytrenowanie modelu. To, jak szybko modele wymagają ponownego treningu, zależy od tempa zmian w rzeczywistym świecie i wymaganej dokładności modelu, ale także, co ważne, od łatwości zbudowania i wdrożenia lepszego modelu.

Zacznijmy jednak od zastanowienia się, jak naukowcy ds. danych mogą stwierdzić, że wydajność modelu się pogarsza. Nie zawsze jest to łatwe. Istnieją dwa popularne podejścia: jedno oparte na danych referencyjnych, a drugie na dryfie danych wejściowych.

Kup książkę Poleć książkę

Dane wzorcowe

Najprościej rzecz ujmując, dane wzorcowe (ang. *ground truth*) to poprawna odpowiedź na pytanie zadane modelowi — na przykład: „Czy ta transakcja kartą kredytową jest faktycznie oszustwem?".

Dysponując danymi wzorcowymi dla wszystkich predykcji dokonanych przez model, można ocenić, jak dobrze ten model działa.

Czasami są one dostępne już błyskawicznie po dokonaniu predykcji; tak dzieje się na przykład w modelach decydujących, które reklamy wyświetlić użytkownikom na stronie internetowej. Użytkownik prawdopodobnie kliknie w reklamy w ciągu kilku sekund lub wcale. Jednak w wielu przypadkach uzyskanie danych wzorcowych trwa znacznie dłużej. Jeśli model przewiduje, że transakcja jest oszustwem, to jak można to potwierdzić? W niektórych przypadkach weryfikacja może zająć jedynie kilka minut, na przykład poprzez wykonanie telefonu do posiadacza karty kredytowej. Ale co z transakcjami, które model uznał za prawidłowe, a w rzeczywistości były oszustwami? W ich przypadku pozostaje jedynie mieć nadzieję, że zostaną zgłoszone przez posiadacza karty podczas przeglądania miesięcznych transakcji, ale to może nastąpić nawet miesiąc po zdarzeniu (lub wcale).

W przykładzie z oszustwami dane wzorcowe nie pozwolą zespołom ds. danych na dokładne monitorowanie wydajności podczas normalnego, codziennego działania. Jeśli sytuacja wymaga szybkiej informacji zwrotnej, lepszym podejściem może być analiza zmian w danych wejściowych.

Dryf danych wejściowych

Dryf danych wejściowych opiera się na zasadzie, że model będzie przewidywał dokładnie tylko wtedy, gdy dane, na których został wytrenowany, są wiernym odzwierciedleniem rzeczywistości. Jeśli więc porównanie ostatnich zapytań kierowanych do wdrożonego modelu z danymi treningowymi wykazuje wyraźne różnice, istnieje duże prawdopodobieństwo, że wydajność modelu jest zagrożona. I właśnie to stanowi podstawę monitorowania dryfu danych wejściowych. Zaletą tego podejścia jest to, że wszystkie dane potrzebne do tego testu już istnieją, więc nie ma potrzeby czekać na dane referencyjne ani żadne inne informacje.

Identyfikacja dryfu jest jednym z najważniejszych elementów elastycznej strategii MLOps i może znacząco usprawnić całościowe wysiłki organizacji w zakresie sztucznej inteligencji. Szczegółowe informacje dotyczące różnych technicznych aspektów monitorowania modeli, które są istotne dla naukowców ds. danych, można znaleźć w rozdziale 7.

Kwestie biznesowe

Może się zdarzyć, że firma będzie mieć holistyczne podejście do kwestii monitorowania, a niektóre z jej obaw mogą dotyczyć pytań takich jak:

- Czy stosowanie modelu przynosi przedsiębiorstwu jakąś wartość?
- Czy korzyści z modelu przewyższają koszty jego opracowania i wdrożenia? (I jak możemy to zmierzyć?)

Kup książkę Poleć książkę

Część poszukiwania odpowiedzi na te pytania stanowią kluczowe wskaźniki efektywności zidentyfikowane dla pierwotnego celu biznesowego. Tam, gdzie to możliwe, powinny być one monitorowane automatycznie, ale rzadko kiedy jest to proste zadanie. Na przykład realizacja celu polegającego na zmniejszeniu liczby oszustw do poziomu poniżej 0,1% transakcji będzie zależna od ustalenia prawdziwego stanu rzeczy. Jednak nawet monitorowanie realizacji tego celu nie zapewnia możliwości odpowiedzenia na pytanie: jaki jest ostateczny zysk dla firmy wyrażony w złotówkach?

To odwieczne wyzwanie dla branży IT, a wraz z rosnącymi nakładami na uczenie maszynowe presja na naukowców ds. danych, by wykazywali wartość, będzie tylko rosła. W obliczu braku „miernika zysków" skuteczne monitorowanie biznesowych kluczowych wskaźników efektywności jest najlepszą dostępną opcją (więcej informacji na ten temat można znaleźć w rozdziale 10., w podrozdziale pt. „Projektowanie i zarządzanie eksperymentami"). W tym kontekście ważny jest wybór punktu odniesienia, który powinien umożliwiać rozróżnienie wartości generowanej konkretnie przez podprojekt uczenia maszynowego, a nie przez cały projekt. Na przykład wydajność uczenia maszynowego można ocenić w odniesieniu do modelu decyzyjnego opartego na regułach, bazującego na wiedzy eksperckiej, aby wyodrębnić wkład automatyzacji decyzji i samego uczenia maszynowego.

Powtarzanie i cykl życia

Opracowywanie i wdrażanie ulepszonych wersji modelu to kluczowy element cyklu życia MLOps, a zarazem jedno z większych wyzwań. Istnieje wiele powodów tworzenia nowej wersji modelu. Jednym z nich jest pogorszenie się jego wydajności z powodu dryfu modelu, o czym była mowa wcześniej. Czasami zachodzi potrzeba dostosowania się do zmienionych celów biznesowych i kluczowych wskaźników efektywności, a innym razem naukowcy ds. danych po prostu znajdują lepszy sposób zaprojektowania modelu.

Powtarzanie

W niektórych dynamicznie zmieniających się środowiskach biznesowych nowe dane treningowe pojawiają się codziennie. Codzienne ponowne trenowanie i wdrażanie modelu często jest zautomatyzowane, aby zapewnić, że model jak najdokładniej odzwierciedla najnowsze doświadczenia.

Ponowne trenowanie istniejącego modelu z wykorzystaniem najnowszych danych to najprostszy scenariusz iteracji nowej wersji modelu. Jednak nawet gdy nie ma zmian w doborze cech czy algorytmie, wciąż istnieje wiele pułapek. W szczególności:

- Czy nowe dane treningowe wyglądają zgodnie z oczekiwaniami? Kluczowa jest zautomatyzowana walidacja nowych danych za pomocą predefiniowanych metryk i kontroli.
- Czy dane są kompletne i spójne?
- Czy rozkłady cech są ogólnie podobne do tych w poprzednim zbiorze treningowym? Pamiętaj, że celem jest udoskonalenie modelu, a nie jego radykalna zmiana.

Kup książkę Poleć książkę

Po zbudowaniu nowej wersji modelu kolejnym krokiem jest porównanie jej metryk z aktualnie działającą wersją. Wymaga to oceny obu modeli na tym samym zbiorze danych, niezależnie od tego, czy jest to poprzednia, czy najnowsza wersja. Jeśli metryki i kontrole sugerują duże różnice między modelami, zautomatyzowane skrypty nie powinny być używane, a zamiast nich usprawnienia należy wprowadzać ręcznie.

Nawet w „prostym" scenariuszu automatycznego ponownego trenowania z użyciem nowych danych istnieje potrzeba stosowania wielu roboczych zbiorów opartych na uzgadnianiu ocen (z informacjami traktowanymi jako dane wzorcowe, gdy staną się one dostępne), czyszczenia i walidacji danych, poprzedniej wersji modelu oraz zestawu starannie przemyślanych kontroli. Ponowne trenowanie w innych scenariuszach prawdopodobnie będzie jeszcze bardziej skomplikowane, co sprawia, że automatyczne wdrażanie modeli uczenia maszynowego jest raczej mało prawdopodobne.

W ramach przykładu rozważmy ponowne trenowanie spowodowane wykryciem znacznego dryfu danych wejściowych. W jaki sposób można ulepszyć model? Jeśli dostępne są nowe dane treningowe, to ponowne trenowanie z wykorzystaniem tych danych jest rozwiązaniem zapewniającym najwyższy stosunek korzyści do kosztów i może wystarczyć. Jednak w środowiskach, w których uzyskanie prawdziwych wartości jest powolne, ilość dostępnych nowych danych może być niewielka.

W takim przypadku konieczna jest bezpośrednia interwencja naukowców ds. danych, którzy muszą zrozumieć przyczynę dryfu i ustalić, jak można dostosować istniejące dane treningowe, aby dokładniej odzwierciedlały najnowsze dane wejściowe. Ocena modelu wygenerowanego w oparciu o takie zmiany jest trudna. Naukowiec musi poświęcić czas na ocenę sytuacji — czas, który rośnie wraz z ilością długu modelowania (ang. *modeling debt*) — a także oszacować potencjalny wpływ na wydajność i zaprojektować niestandardowe środki łagodzące. Na przykład usunięcie określonej cechy lub próbkowanie istniejących wierszy danych treningowych może prowadzić do lepiej dostrojonego modelu.

Pętla sprzężenia zwrotnego

W dużych przedsiębiorstwach najlepsze praktyki DevOps zazwyczaj zakładają, że środowisko oceny modelu w czasie rzeczywistym i środowisko ponownego trenowania modelu są oddzielne. W rezultacie ocena nowej wersji modelu w środowisku treningowym może być niedokładna.

Jednym ze sposobów na zmniejszenie tej niepewności jest zastosowanie techniki testowania typu *shadow* (ang. *shadow testing*). Polega ona na wdrożeniu nowej wersji modelu w środowisku produkcyjnym obok istniejącego modelu. Wszystkie bieżące oceny są obsługiwane przez dotychczasową wersję modelu, ale każde nowe żądanie jest następnie obsługiwane przez nową wersję modelu, przy czym wyniki są rejestrowane, lecz nie zwracane do użytkownika. Po ocenieniu wystarczająco dużej liczby żądań obsłużonych przez obie wersje modeli wyniki można porównać statystycznie. Technika testowania typu *shadow* daje również ekspertom dziedzinowym lepszy wgląd w przyszłe wersje modelu, co może ułatwić płynne zamienianie używanych modeli.

Kup książkę Poleć książkę

W przypadku omawianego wcześniej modelu generowania reklam nie jest możliwe stwierdzenie, czy reklamy wybrane przez model są dobre, czy złe, bez wyświetlenia ich użytkownikowi końcowemu i zapewniania mu możliwości kliknięcia w nie. W tym przypadku zastosowanie testowania typu *shadow* daje ograniczone korzyści, a częściej stosowane są testy A/B.

W przypadku testów A/B oba modele są wdrażane w środowisku produkcyjnym, a żądania od użytkowników są rozdzielane pomiędzy nie. Każde żądanie jest przetwarzane przez jeden lub drugi model, lecz nie przez oba. Wyniki obu modeli są rejestrowane na potrzeby późniejszej analizy (ale nigdy dla tego samego żądania). Wyciągnięcie statystycznie istotnych wniosków z testu A/B wymaga starannego zaplanowania testu.

Zagadnienia związane z testami A/B zostały dokładniej opisane w rozdziale 7., a na razie, w ramach podsycenia ciekawości, napiszemy, że najprostsza forma testu A/B jest często nazywana testem o ustalonym horyzoncie (ang. *fixed-horizon test*). Wynika to z faktu, że w poszukiwaniu statystycznie istotnego wniosku trzeba poczekać, aż zostanie przetestowana starannie określona liczba próbek. Próby „podglądania" wyniku przed zakończeniem testu będą niewiarygodne. Jeśli jednak test jest przeprowadzany w środowisku komercyjnym, każda zła prognoza prawdopodobnie będzie mieć swoją cenę, więc brak możliwości wcześniejszego zakończenia testu może być kosztowny.

Działania na krawędzi

Iteracyjne działania modelu uczenia maszynowego wdrożonego na milionach urządzeń, takich jak smartfony, czujniki czy samochody, stawia inne wyzwania niż działania realizowane w środowisku korporacyjnym. Jedno z podejść polega na przekazywaniu wszystkich informacji zwrotnych z milionów instancji modelu do centralnego punktu i centralnym trenowaniu modelu. Ta metoda jest stosowana w systemie autopilota Tesli[3], który działa w ponad 500 000 samochodów. Pełne wytrenowanie około 50 sieci neuronowych stosowanych w samochodach Tesli zajmuje 70 000 godzin pracy GPU.

Firma Google, tworząc swoje oprogramowanie dla klawiatur smartfonów — GBoard[4] — przyjęła inne podejście. Zamiast centralnego trenowania każdy smartfon trenuje model lokalnie i wysyła do Google podsumowanie znalezionych ulepszeń. Te ulepszenia ze wszystkich urządzeń są uśredniane, a na podstawie uzyskanych wyników jest aktualizowany wspólny model. Takie podejście oparte na uczeniu federacyjnym oznacza, że osobiste dane użytkownika nie muszą być gromadzone centralnie, ulepszony model na każdym telefonie może być używany natychmiast, a ogólne zużycie energii maleje.

Coraz częściej stosowaną alternatywą dla „częstościowych" testów o ustalonym horyzoncie są testy bayesowskie, a w szczególności testy wielorękiego bandyty, których celem jest zapewnienie możliwości szybszego wyciągania wniosków. Testy wielorękiego bandyty są testami adaptacyjnymi: algorytm decydujący o podziale między modelami dostosowuje się do bieżących

[3] *https://www.tesla.com/AI*.

[4] *https://research.google/blog/federated-learning-collaborative-machine-learning-without-centralized-training-data/*.

Kup książkę Poleć książkę

wyników i zmniejsza obciążenie słabo działających modeli. Chociaż ta technika testowania jest bardziej złożona, może ona zmniejszać koszty biznesowe związane z kierowaniem ruchu do słabo działającego modelu.

Zarządzanie

Nadzór korporacyjny to zestaw mechanizmów kontrolnych stosowanych w przedsiębiorstwie w celu zapewnienia, że wypełnia ono swoje obowiązki wobec wszystkich interesariuszy — od akcjonariuszy i pracowników po społeczeństwo i władze państwowe. Obowiązki te obejmują zobowiązania finansowe, prawne i etyczne. U podstaw wszystkich trzech leży fundamentalna zasada uczciwości.

Najłatwiejsze do zrozumienia są zobowiązania prawne. Przedsiębiorstwa podlegały regulacjom na długo przed pojawieniem się uczenia maszynowego. Wiele przepisów dotyczy konkretnych branż; na przykład regulacje finansowe mają na celu ochronę społeczeństwa i szerszej gospodarki przed niewłaściwym zarządzaniem finansami i oszustwami, podczas gdy branża farmaceutyczna musi przestrzegać zasad chroniących zdrowie publiczne. Na praktyki biznesowe wpływają również szersze przepisy chroniące wrażliwe grupy społeczne i zapewniające równe szanse w zakresie takich kryteriów jak płeć, rasa, wiek czy religia.

W ostatnim czasie rządy na całym świecie wprowadziły regulacje mające chronić społeczeństwo przed skutkami wykorzystywania danych osobowych przez przedsiębiorstwa. Ogólne rozporządzenie o ochronie danych (RODO) z 2016 roku oraz kalifornijska ustawa o ochronie prywatności konsumentów (CCPA) z 2018 roku są typowymi przykładami tego trendu, a ich wpływ na uczenie maszynowe — które całkowicie zależy od danych — jest ogromny. Na przykład RODO ma na celu ochronę danych osobowych przed niewłaściwym wykorzystaniem przemysłowym, a przez to ograniczenie potencjalnej dyskryminacji jednostek.

Zasady RODO

RODO określa zasady przetwarzania danych osobowych, a warto zauważyć, że CCPA została stworzona w oparciu o podobne założenia, choć istnieją między nimi pewne istotne różnice[5]. Przetwarzanie obejmuje zbieranie, przechowywanie, modyfikowanie i wykorzystywanie danych osobowych. Te zasady to:

- zgodność z prawem, rzetelność i przejrzystość;
- ograniczenie celu;
- minimalizacja danych;
- dokładność;
- ograniczenie ilości przechowywanych informacji;
- integralność i poufność (bezpieczeństwo);
- odpowiedzialność.

[5] Więcej informacji na temat różnic pomiędzy RODO i CCPA można znaleźć w publikacji dostępnej pod adresem *https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf*.

Kup książkę Poleć książkę

Rządy zaczynają teraz interesować się regulacjami związanymi z uczeniem maszynowym, mając nadzieję na złagodzenie negatywnych skutków stosowania takich rozwiązań. Unia Europejska przoduje w tej kwestii, planując prace ustawodawcze nad zdefiniowaniem dopuszczalnych zastosowań różnych form sztucznej inteligencji. Nie chodzi tu koniecznie o ograniczenie jej użycia; na przykład może to umożliwić korzystne zastosowania technologii rozpoznawania twarzy, które są obecnie ograniczone przez przepisy o ochronie prywatności. Jasne jest jednak, że podczas wdrażania kolejnych rozwiązań z zakresu uczenia maszynowego firmy będą musiały uwzględnić kolejne regulacje.

Czy firmy dbają o moralną odpowiedzialność wobec społeczeństwa, wykraczającą poza formalne przepisy? Coraz częściej odpowiedź brzmi „tak", co widać w obecnym rozwoju wskaźników efektywności środowiskowej, społecznej i ładu korporacyjnego. Zaufanie ma znaczenie dla konsumentów, a jego brak jest niekorzystny dla biznesu. Wraz z rosnącym aktywizmem społecznym w tej dziedzinie firmy angażują się w ideę odpowiedzialnej sztucznej inteligencji, czyli etycznego, przejrzystego i odpowiedzialnego stosowania technologii AI. Zaufanie ma znaczenie również dla akcjonariuszy, a w niedalekiej przyszłości można się spodziewać pełnego ujawniania ryzyk związanych z uczeniem maszynowym.

Stosowanie dobrych praktyk zarządzania w obszarze MLOps jest wyzwaniem. Procesy są złożone, technologia nieprzejrzysta, a zależność od danych fundamentalna. Inicjatywy związane z zarządzaniem w kontekście praktyk MLOps można ogólnie podzielić na dwie kategorie:

Zarządzanie danymi

Struktura zapewniająca odpowiednie wykorzystanie i zarządzanie danymi.

Zarządzanie procesami

Wykorzystanie jasno zdefiniowanych procesów w celu zapewnienia, że wszystkie aspekty zarządzania zostały uwzględnione we właściwym momencie cyklu życia modelu oraz że prowadzony jest pełny i dokładny rejestr działań.

Zarządzanie danymi

Zarządzanie danymi zajmuje się wykorzystywanymi danymi, zwłaszcza tymi służącymi do trenowania modeli, i może odpowiadać na pytania takie jak:

- Jakie jest pochodzenie danych?
- W jaki sposób pierwotne dane zostały zebrane i jakie są warunki ich użytkowania?
- Czy dane są dokładne i aktualne?
- Czy występują w nich dane osobowe lub inne rodzaje wrażliwych informacji, których nie należy wykorzystywać?

Projekty uczenia maszynowego zwykle obejmują złożone procesy przetwarzania danych, w tym czyszczenie, łączenie i przekształcanie. Zrozumienie pochodzenia danych jest skomplikowane, szczególnie na poziomie cech, ale niezbędne do zapewnienia zgodności z przepisami w stylu RODO. W jaki sposób zespoły — a w szerszej perspektywie: organizacje, ponieważ ma to znaczenie również na najwyższym szczeblu — mogą mieć pewność, że do trenowania danego modelu nie

Kup książkę Poleć książkę

wykorzystano żadnych danych osobowych? Anonimizacja lub pseudoanonimizacja danych nie zawsze wystarcza do właściwego zarządzania informacjami osobowymi. Jeśli procesy te nie zostaną przeprowadzone prawidłowo, nadal może być możliwe zidentyfikowanie konkretnej osoby i jej danych, co jest sprzeczne z wymogami RODO[6].

Nieodpowiednie uprzedzenia w modelach mogą pojawić się przypadkowo, mimo najlepszych intencji naukowców ds. danych. Pewien model uczenia maszynowego używany do rekrutacji zasłynął z dyskryminacji kobiet, gdyż niektóre szkoły — wyłącznie żeńskie — były słabiej reprezentowane w kadrze kierowniczej firmy, co odzwierciedlało historyczną dominację mężczyzn w organizacji[7]. Chodzi o to, że przewidywanie na podstawie doświadczeń jest potężną techniką, ale czasami konsekwencje są nie tylko nieskuteczne, ale także nielegalne.

Narzędzia do zarządzania danymi, które mogą rozwiązać te problemy, są dopiero w fazie początkowej. Większość z nich koncentruje się na odpowiedzi na dwa pytania dotyczące pochodzenia danych:

- Skąd pochodzą informacje zgromadzone w tym zbiorze danych i co to mówi o możliwościach jego wykorzystania?
- W jaki sposób ten zbiór danych jest używany i jakie mogą być konsekwencje jego modyfikacji?

W rzeczywistych procesach przygotowywania danych udzielenie odpowiedzi na żadne z tych pytań nie jest proste. Na przykład jeśli naukowiec ds. danych napisze funkcję w Pythonie, która przetwarza w pamięci kilka zbiorów wejściowych i generuje jeden zbiór wynikowy, jak można mieć pewność, z jakich informacji pochodzą poszczególne elementy nowego zbioru?

Zarządzanie procesem

Zarządzanie procesem koncentruje się na formalizacji kroków realizowanych w procesie MLOps i powiązaniu z nimi odpowiednich działań. Zazwyczaj są to przeglądy, zatwierdzenia i gromadzenie materiałów pomocniczych, takich jak dokumentacja. Zarządzanie procesem ma dwojakie cele:

- Zapewnienie, że każdy aspekt związany z zarządzaniem jest uwzględniany we właściwym momencie i odpowiednio realizowany. Na przykład modele nie powinny być wdrażane w środowisku produkcyjnym, dopóki nie przejdą wszystkich testów walidacyjnych.
- Umożliwienie nadzorowania ścisłego procesu MLOps z zewnątrz. Audytorzy, menedżerowie ryzyka, specjaliści ds. zgodności, jak również cała firma, mają interes w zapewnieniu możliwości śledzenia postępów i późniejszego przeglądania decyzji.

[6] W ramach poszukiwań dodatkowych informacji na temat anonimizacji i pseudoanonimizacji oraz analizy, dlaczego nie rozwiązują one wszelkich problemów związanych z prywatnością danych, zachęcamy do przeczytania publikacji pt. *Executing Data Privacy-Compliant Data Projects* przygotowanej przez zespół Dataiku i dostępnej na stronie *https://www.dataiku.com/product/key-capabilities/ai-governance/*.

[7] Chodzi o słynne zrezygnowanie przez firmę Amazon z systemu rekrutacyjnego bazującego na sztucznej inteligencji w związku z jego uprzedzeń względem kobiet: *https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/*.

Kup książkę Poleć książkę

Skuteczne wdrożenie zarządzania procesem jest trudne:

- Formalne procesy dla cyklu życia uczenia maszynowego rzadko kiedy można łatwo precyzyjnie zdefiniować. Zrozumienie całego procesu jest zwykle rozproszone między wieloma zaangażowanymi zespołami i często nie ma jednej osoby dysponującej szczegółową całościową wiedzą o rozwiązaniu.
- Aby proces mógł być stosowany skutecznie, każdy zespół musi być gotowy do jego pełnego przyjęcia.
- Jeśli proces jest zbyt skomplikowany dla niektórych przypadków użycia, zespoły z pewnością będą go omijać, co spowoduje utratę wielu korzyści.

Obecnie zarządzanie procesem jest najczęściej spotykane w organizacjach tradycyjnie obciążonych dużą ilością regulacji i wymogów zgodności, takich jak sektor finansowy. Poza nimi jest rzadkością. Wraz z przenikaniem uczenia maszynowego do wszystkich sfer działalności komercyjnej i rosnącym zainteresowaniem odpowiedzialnym AI będziemy potrzebować nowych i innowacyjnych rozwiązań tego problemu, które z powodzeniem będzie można stosować we wszystkich firmach.

Podsumowanie

Biorąc pod uwagę ten przegląd cech wymaganych dla praktyk MLOps i procesów, na które mają one wpływ, jest oczywiste, że nie jest to coś, co zespoły ds. danych — czy nawet całe organizacje operujące na danych — mogą zignorować. Nie jest to również coś, co można po prostu odhaczyć na liście („tak, stosujemy MLOps!”), lecz raczej złożona interakcja między technologiami, procesami i ludźmi, której prawidłowe wdrożenie wymaga dyscypliny i czasu.

Kolejne rozdziały szczegółowo opisują poszczególne komponenty cyklu życia modeli uczenia maszynowego, mające duże znaczenie dla praktyk MLOps, i wyjaśniają, jak każdy z nich powinien być realizowany, aby zbliżyć się do idealnego wdrożenia MLOps.

Kup książkę Poleć książkę


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

Praktyczny przewodnik po skalowaniu AI w przedsiębiorstwach

MLOps (ang. *machine learning operations*) to jedna z najszybciej rozwijających się dziedzin IT, łącząca uczenie maszynowe z praktykami DevOps. W erze cyfrowej transformacji, gdy organizacje coraz częściej wdrażają modele AI w środowiskach produkcyjnych, potrzeba skutecznego zarządzania cyklem życia modeli uczenia maszynowego staje się kluczowa. Książka **MLOps dla biznesu** odpowiada na rosnące zapotrzebowanie rynku na praktyczne przewodniki po tej złożonej tematyce, oferując kompleksowe podejście do skalowania rozwiązań AI w przedsiębiorstwach.

Autorzy prezentują pełny cykl życia modeli uczenia maszynowego — od tworzenia i walidacji, przez wdrażanie w środowisku produkcyjnym, po monitorowanie i zarządzanie. Szczegółowo omawiają kluczowe aspekty MLOps: automatyzację potoków CI/CD, strategie wdrażania, wykrywanie dryfu danych, zarządzanie ryzykiem i odpowiedzialną sztuczną inteligencję. Praktyczne studium przypadków z różnych branż — od finansów po energetykę — ilustruje rzeczywiste wyzwania i rozwiązania, z jakimi mierzą się zespoły implementujące MLOps na dużą skalę.

- Kompleksowy przegląd metodologii MLOps i jej kluczowych komponentów
- Praktyczne strategie wdrażania modeli w środowiskach produkcyjnych
- Techniki monitorowania wydajności modeli i wykrywania dryfu danych
- Zarządzanie ryzykiem i aspekty odpowiedzialnej sztucznej inteligencji
- Rzeczywiste studia przypadków z branży finansowej, marketingu i energetyki
- Najlepsze praktyki w zakresie automatyzacji i skalowania rozwiązań uczenia maszynowego
- Współpraca między zespołami data science, DevOps i biznesowymi

Mark Treveil i zespół Dataiku to uznani eksperci w dziedzinie uczenia maszynowego i analizy danych. Mają wieloletnie doświadczenie w projektowaniu i wdrażaniu rozwiązań AI w różnych branżach — od telekomunikacji po energetykę. Zespół Dataiku, wiodącej platformy do nauki o danych, regularnie publikuje treści edukacyjne i prowadzi szkolenia dla specjalistów z całego świata.

Helion
helion.pl
HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-3882-3
9 788328 938823
Cena: 69,00 zł