

**Wydział Elektrotechniki, automatyki, informatyki i inżynierii biomedycznej.**

Praca dyplomowa magisterska

*Federacyjne uczenie maszynowe*

*Federated machine learning*

Autor: *Mikołaj Skrzyniarz*

Kierunek studiów: *Informatyka i Systemy Inteligentne*

Opiekun pracy: *dr inż. Piotr Szwed*

Kraków, 2022

Spis treści

[1. Wstęp 3](#_Toc98424807)

[1.1. Cel pracy 5](#_Toc98424808)

[1.2. Zakres pracy 5](#_Toc98424809)

[2. Wprowadzenie teoretyczne 6](#_Toc98424810)

[2.1. Czym jest federacyjne uczenie maszynowe? 6](#_Toc98424811)

[2.1.1. Rozproszone uczenie maszynowe 6](#_Toc98424812)

[2.1.1. Federacyjne uczenie maszynowe 7](#_Toc98424813)

[3. Opis realizacji tematu pracy 8](#_Toc98424814)

[4. Podsumowanie 8](#_Toc98424815)

[5. Bibliografia 8](#_Toc98424816)

# 1. Wstęp

Dziedziny zajmujące się zagadnieniami związanymi z sztuczną inteligencją istnieją w świecie technologii i nauki od dłuższego czasu. Ich popularność stale rośnie a sztuczna inteligencja powiązana jest z takimi obszarami jak matematyka, statystyka, nauki o danych (ang. *data science)*, duże zbiory danych (ang. *big data)* oraz z oczywistych względów – informatyka (ang. *computer science*). Trudno się temu dziwić, wszystkie te zagadnienia niejako przeplatają się nawzajem – poruszają podobne problemy oraz wymagają zbliżonych umiejętności.

W przeciągu ostatnich dwudziestu lat termin sztuczna inteligencja ewoluował z nauki wzbudzającej ogromną ciekawość wśród ludzi do praktycznej technologii, powszechnie używanej w celach komercyjnych. Ten postęp spowodowany jest rosnącą dostępnością systemów umożliwiające prowadzenie różnego rodzaju skomplikowanych obliczeń, materiałów naukowych oraz świadomością jak i wiedzą uczonych, studentów jak i wszystkich pracowników branż technologicznych. Ta z kolei prowadzi do powstawania nowych, bardziej rozbudowanych i zaawansowanych algorytmów. W efekcie liczba firm stosujących rozwiązania bazujące na mechanizmach sztucznej inteligencji w ubiegłych czasach wzrosła diametralnie. Wizja komputerowa (ang. *computer vision)*, przetwarzanie języka naturalnego, rozpoznawanie mowy, wykrywanie schorzeń oraz różnego rodzaju anomalii to tylko niektóre z wielu przykładów użycia, a z prostych mechanizmów wspomagających podejmowanie decyzji korzystamy, świadomie lub nie, tak naprawdę na co dzień.

Uczenie maszynowe jest największym obszarem szeroko rozumianej sztucznej inteligencji. Może być rozumiany jako zajmujący się szukaniem rozwiązania problemu polegającego na stworzeniu urządzenia, które będzie osiągało lepsze wyniki w skali ustalonej wcześniej metryki poprzez naukę w oparciu o doświadczenie oraz decyzje podejmowane w przeszłości. Przykładem może być wykrywanie schorzenia na podstawie zdjęć rentgenowskich danego narządu. Celem jest poprawne przydzielenie etykiet „zdrowy” i „chory” dla każdego ze zdjęć. By to osiągnąć dany algorytm musi nauczyć się rozróżniać zdjęcia na podstawie określonych cech. To z kolei odbywa się w procesie uczenia, podczas którego dany model poddaje się próbom na zbiorze uczącym, zawierającym dane służące jako wzorzec, mające już przydzielone etykiety [2].

Tradycyjny proces uczenia z uwzględnieniem danych zbieranych urządzenia rozproszone polega na agregacji takich danych na wspólnym urządzeniu pełniącym rolę serwera, wytrenowaniu modelu oraz propagacji gotowego modelu między urządzeniami. Głównym problemem takiego modelu jest fakt, że dane istnieją w formie odizolowanych obiektów oraz ich bezpieczeństwo jak i prywatność, które mogą być naruszone podczas procesu agregacji. Rozwiązaniem tego może być zastosowanie federacyjnego uczenia maszynowego, zaproponowanego przez firmę kilka lat temu przez firmę *Google* [3]. W teorii skuteczność wytrenowanego w ten sposób modelu powinna być zbliżona do tradycyjnej metody przy zachowaniu większego bezpieczeństwa całego procesu oraz niższego ryzyka wycieku danych.

## 1.1. Cel pracy

Celem niniejszej pracy było zaprojektowanie oraz przeprowadzenie eksperymentów mających na celu symulację federacyjnego uczenia maszynowego. Wyniki powinny zostać porównane z wynikami uzyskanymi przy użyciu tradycyjnego sposobu uczenia. W wykorzystanym podejściu samodzielni agenci trenują swoje modele przy użyciu obserwowanych danych. Modele te są okresowo agregowane, a następnie dystrybuowane wewnątrz grupy.

W pracy należało rozważyć różne tryby działania algorytmu, a także zaproponować metodę agregacji wag oraz parametry sterujące. Docelowy system miał być przetestowany na dużym zbiorze danych z użyciem modeli o różnym stopniu złożoności. W przypadku zastosowania *transfer learning* rdzeń modelu nie powinien podlegać modyfikacji.

## 1.2. Zakres pracy

TODO

# 2. Wprowadzenie teoretyczne

Celem drugiego rozdziału pracy jest zaznajomienie czytelnika z teorią na temat poruszanych pojęć oraz zagadnień. W oparciu o wykorzystane pozycje literaturowe wytłumaczone zostanie czym tak naprawdę jest federacyjne uczenie maszynowe, jakie są różnice względem tradycyjnego modelu uczenia oraz jakie wyróżniamy rodzaje opisywanej metody.

## 2.1. Rozproszone uczenie maszynowe

Tradycyjny model uczenia maszynowego nazywany jest także rozproszonym uczeniem maszynowym (ang. *distributed machine learning*). Jest to to wielowęzłowy system gdzie każdy węzeł symbolizuje pojedyncze urządzenie. Taka struktura umożliwia przetwarzanie dużych zbiorów danych, których powiększanie odbywa się poprzez dokładanie kolejnych węzłów. Taki sposób uczenia przewiduje agregację danych z wielu urządzeń w jeden zbiór, który następnie służy do nauki określonego typu modelu. Tak skonstruowany model zostaje następnie wysłany do każdego urządzenia korzystającego z danej aplikacji. Samo urządzenie zbiera dane w czasie rzeczywistym, a proces ich wysyłania do jednostki na której ma miejsce proces uczenia odbywa się okresowo. Jest to jedną z wad tego rodzaju uczenia – nie ma możliwości by zbierane przez urządzenie dane na bieżąco aktualizowały używany model. Niemniej jednak cały proces przeprowadzony w opisywany sposób skutkuje rosnącą skutecznością danego algorytmu. Taki typ uczenia jest w dobry pod względem uzyskiwanej skuteczności jednak wzbudza pewne obawy co do prywatności danych. Wszystkie urządzenia mobilne, IoT (ang. *internet of things*) kolekcjonują całą masę danych, w związku z czym zachowanie ich prywatności staje się co raz większym wyzwaniem.

Proces uczenia maszynowego na podstawie danych zebranych przez wiele urządzeń rozproszonych w oparciu o tradycyjną metodę możemy w uproszczeniu podzielić na trzy kroki (patrz rys. 2.1):

1. okresowe wysyłanie zgromadzonych przez urządzenia rozproszone danych do jednostki centralnej;
2. przeprowadzenie procesu uczenia na serwerze, przy użyciu zbioru testowego skonstruowanego poprzez agregację zebranych danych;
3. dystrybucja wytrenowanego modelu sztucznej inteligencji między urządzeniami korzystającymi z systemu [2].

A picture containing electronics

Description automatically generated

Rys. 2.1. Diagram przedstawiający tradycyjny model uczenia maszynowego.

## 2.2. Federacyjne uczenie maszynowe

Koncept federacyjnego uczenia maszynowe pierwszy raz światło dzienne ujrzał w 2016 roku, kiedy został zaprezentowany przez firmę *Google*. Głównym celem dla którego podjęto próby wynalezienia nowego sposobu uczenia maszynowego było zapewnienie bezpieczeństwa oraz zniwelowanie ryzyka utraty lub wycieku danych, używając zestawów danych znajdujących się na urządzeniach rozproszonych.

# 3. Opis realizacji tematu pracy

# 4. Podsumowanie

# 5. Bibliografia

**Opracowania książkowe**

1. TODO

**Dokumenty**

1. *Machine learning: Trends, perspectives, and prospects*, M.I. Jordan, T.M. Mitchell
2. *Federated Machine Lraning: Concept and Applications,* Yang Liu, Tianjian Chen, Yongxing Tong

**Źródła internetowe**

1. *TODO*