

ShadowReg

Privacy-preserving linear regression model for sensitive data

Radosław Trzmielewski

PROBLEM

**Wiele instytucji
posiada dane
wrażliwe, których
nie mogą
przekazywać
innym.**

**Tradycyjne
uczenie modeli
wymaga
centralizacji
danych, co jest
często
niemożliwe.**

**Brak współpracy
między stronami
ogranicza jakość i
możliwości
modeli uczenia
maszynowego.**

ROZWIĄZANIE



Regresja liniowa trenowana bez ujawniania danych.

Dane pozostają lokalnie, a obliczenia odbywają się wspólnie dzięki Multi Party Computation

Dokładność modelu taka sama jak w klasycznej regresji.

W uczeniu maszynowym taki scenariusz określa się jako federated learning.

Secure Multi-Party
Computation (MPC)

Bezpieczny iloczyn
skalarmy

Iteracyjny solver
Conjugate Gradient
Descent

Arytmetyka fixed-
point

05

Python, AWS, Docker,
React

TECHNOLOGIA

ZASTOSOWANIE

W każdym z tych przypadków potrzebny jest model uczenia maszynowego, ale danych ujawnić nie można.

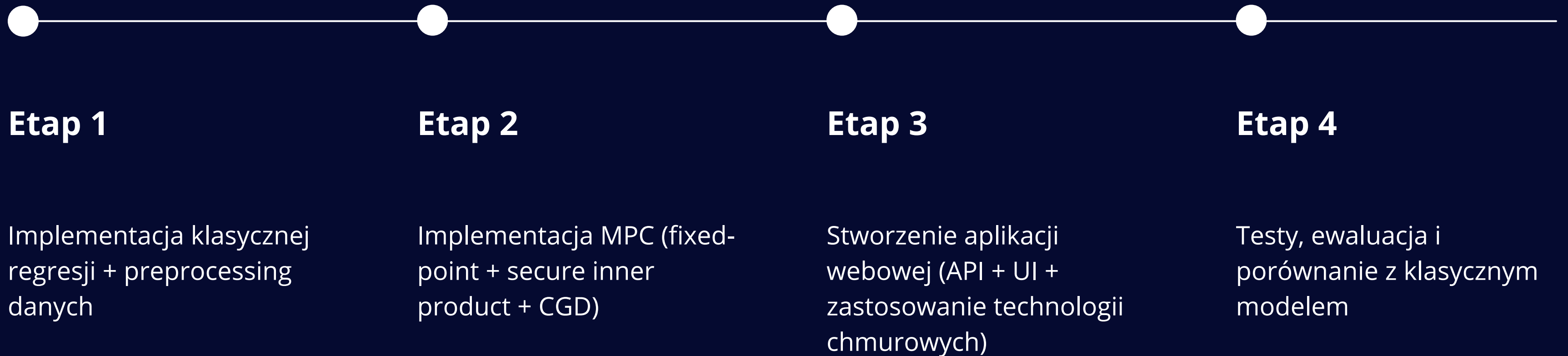
- Dane medyczne
- Dane finansowe
- Dane przemysłowe i sensoryczne
- Wspólne projekty badawcze między instytucjami

ARCHITEKTURA I KONKURENCJA

- Każda instytucja przechowuje dane lokalnie
- Dane są zamieniane na sekrety i przetwarzane przez warstwę MPC
- Wynikiem jest wspólny model regresji bez ujawniania danych postronnych
- Federated Learning (Google FL, PySyft)
- Rozwiązania z homomorficznym szyfrowaniem

ShadowReg wyróżnia się prostą architekturą i przejrzystością implementacji, co ułatwia audyt i praktyczne wdrożenie.

PLAN PROJEKTU



ELEVATOR PITCH

FOR organizations that work with sensitive or regulated data
WHO need predictive models but cannot share their datasets
ShadowReg IS a privacy-preserving linear regression system
THAT enables collaborative training without exposing raw data
UNLIKE traditional ML workflows that require centralization
my product **USES** MPC to provide strong privacy
with no loss in accuracy