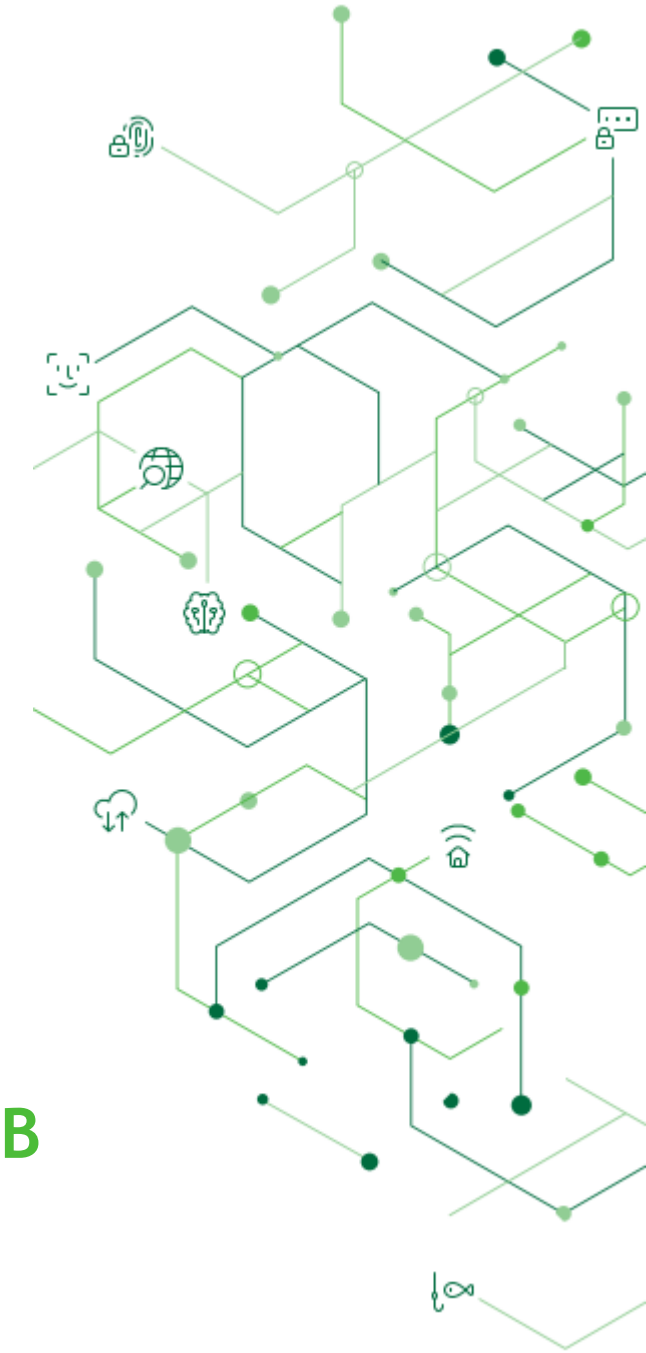
Federált tanulás és biztonsága

Kovács Gergely Zsolt



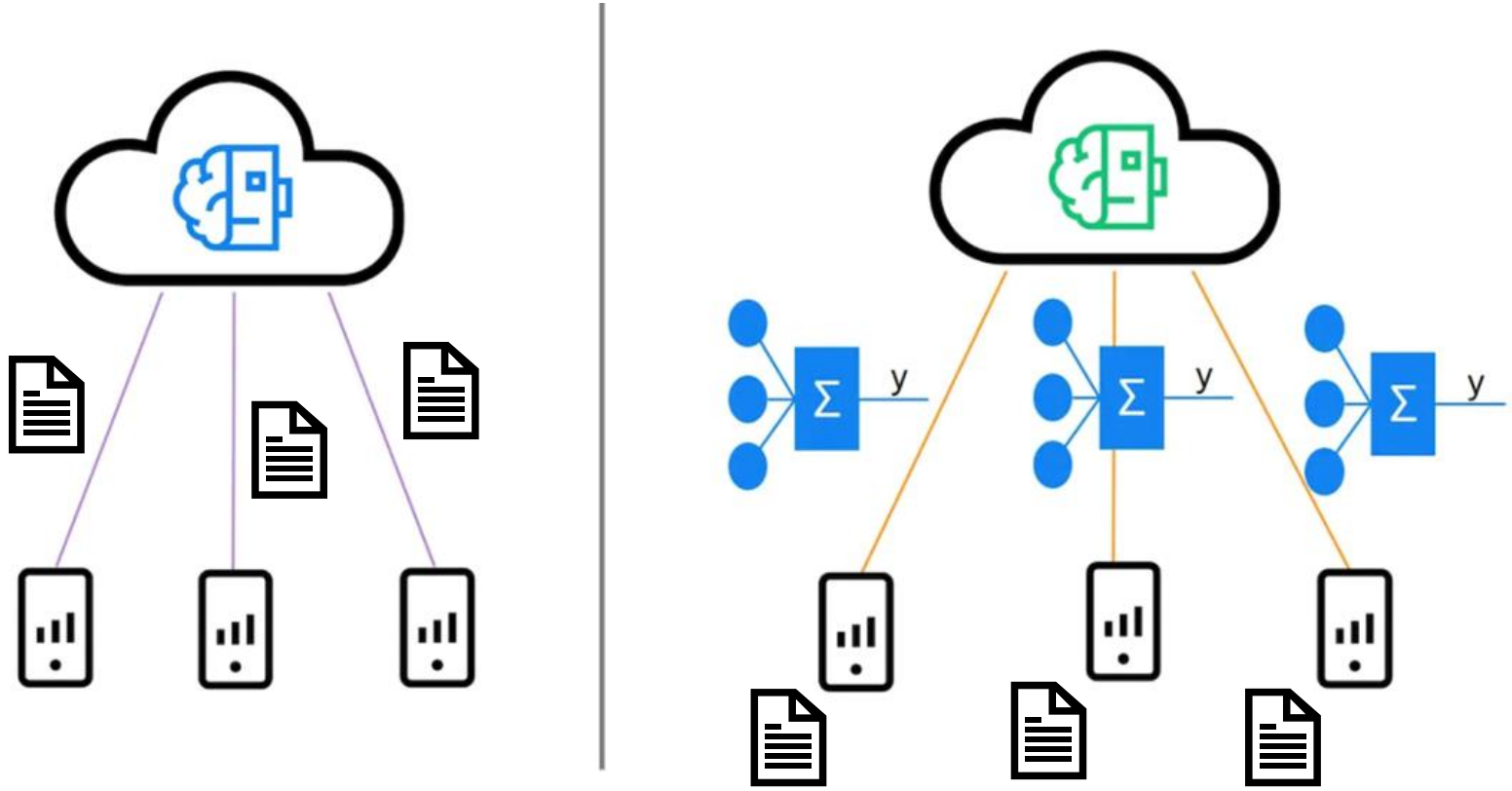
ELTE | IK
INFORMATIKAI KAR

otpbank

KIBERLAB

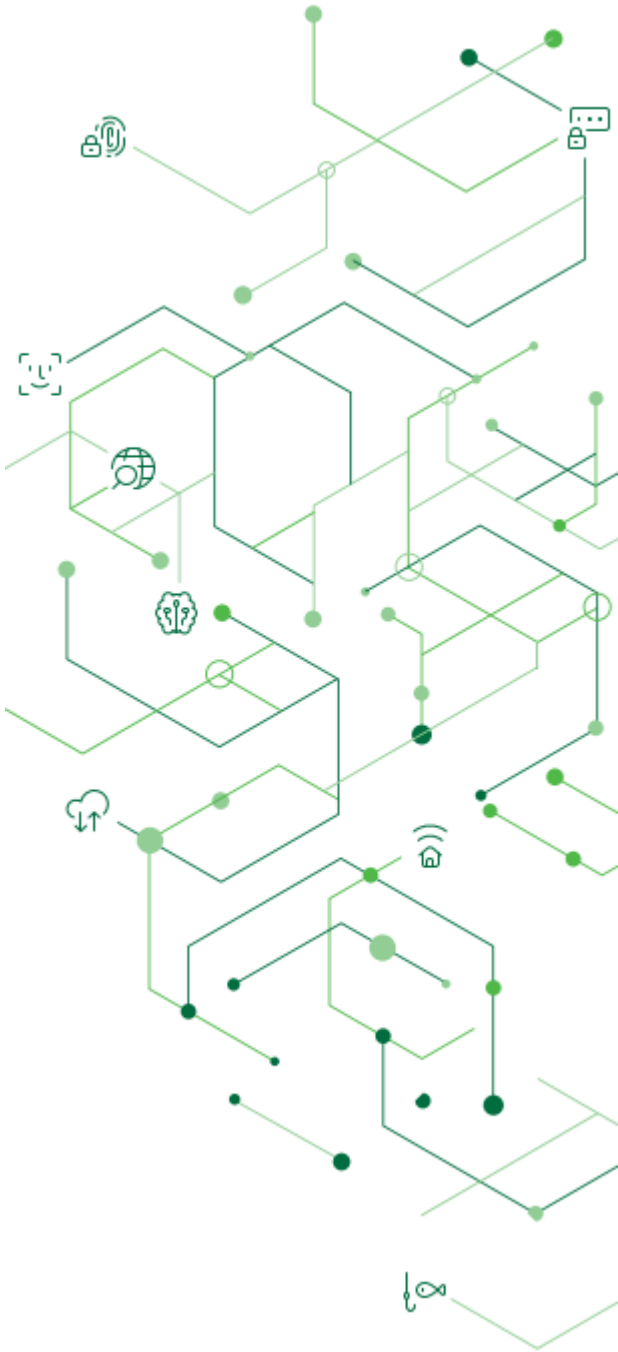
EKÖP
Egyetemi Kutatói Ösztöndíj Program

Centralizált és federált tanulás

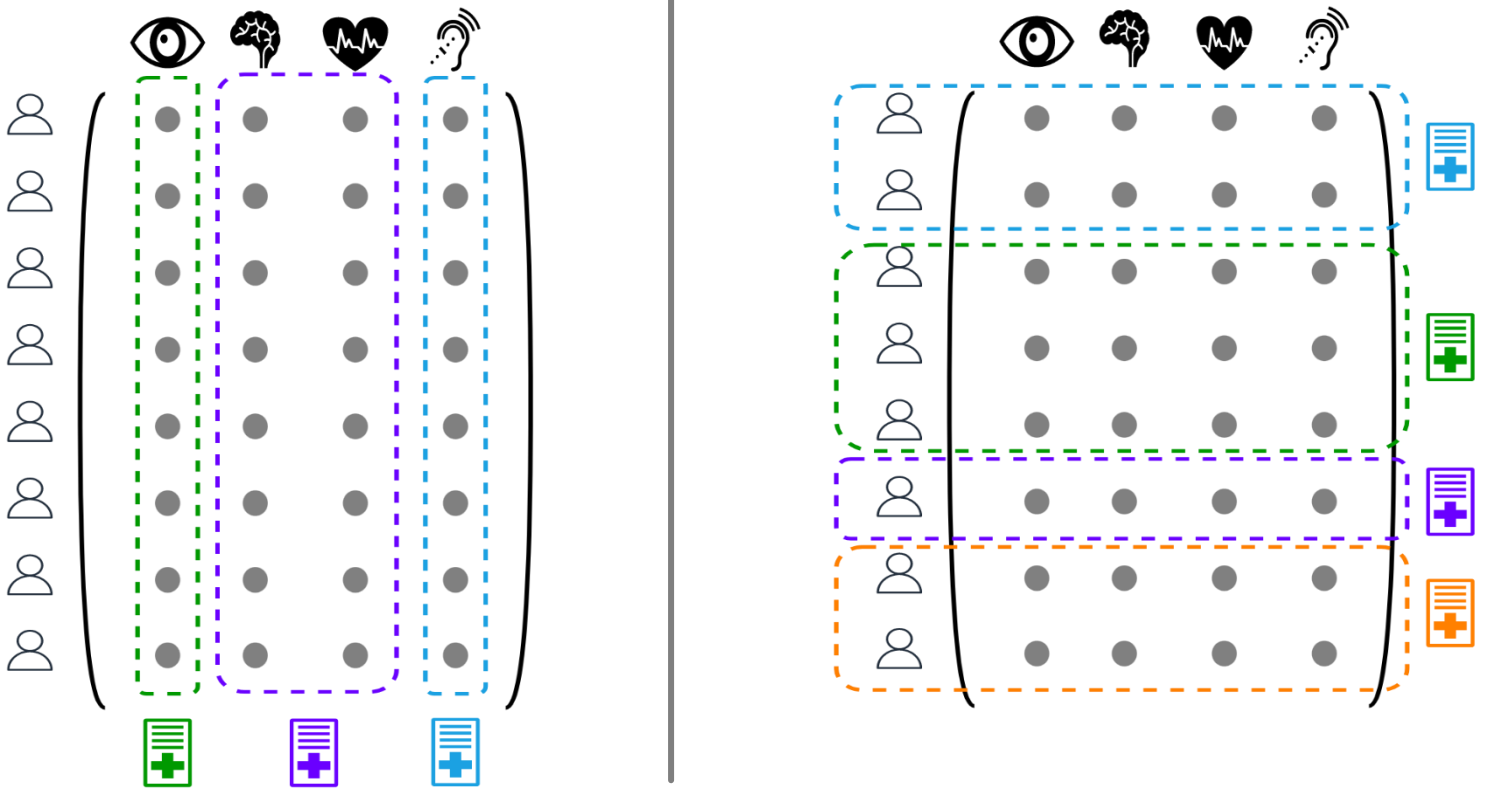


https://www.marktechpost.com/2021/11/28/ericsson-and-uppsala-university-team-up-to-research-air-quality-prediction-using-machine-learning-and-federated-learning/

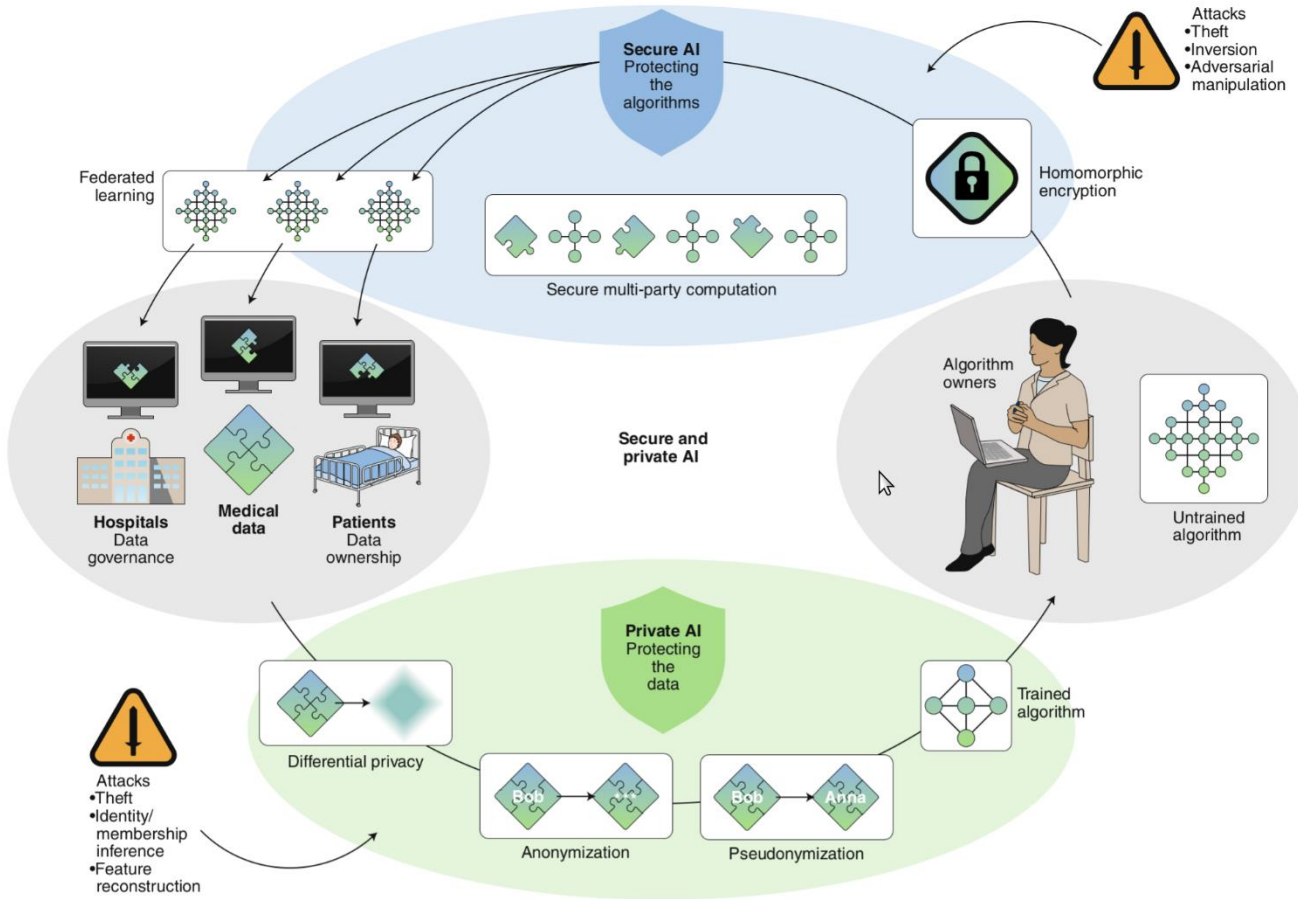
Típusai



Vertikális – horizontális

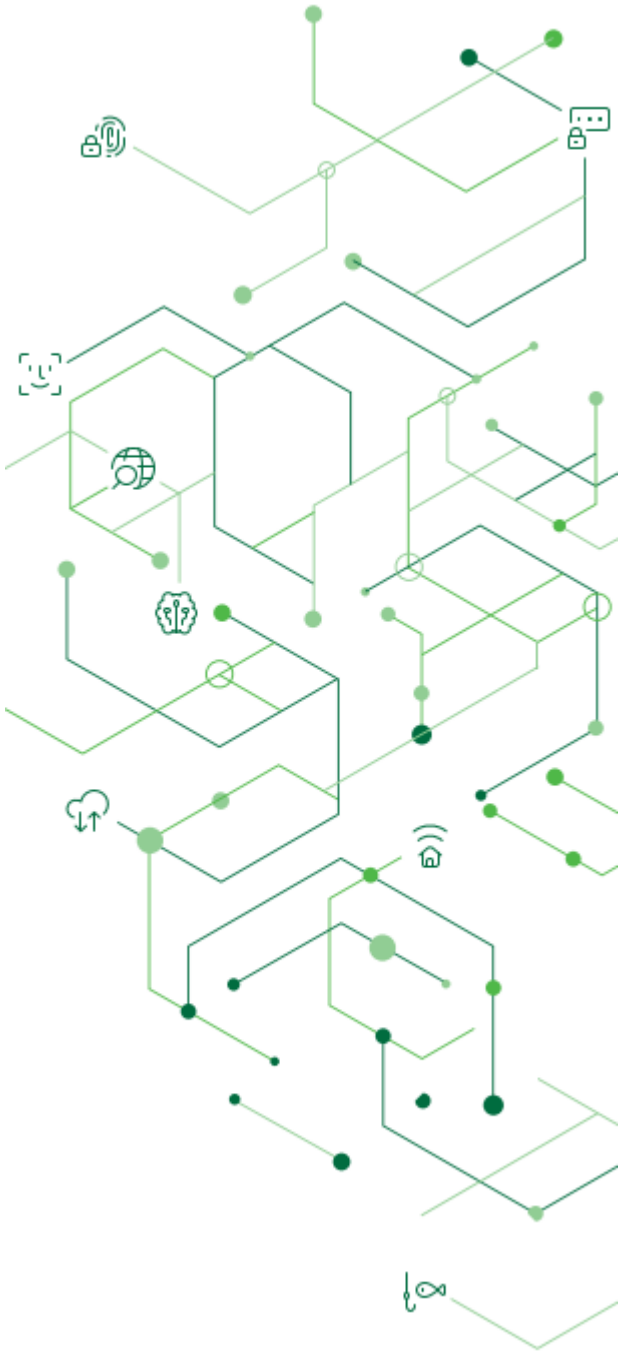


Biztonsági követelmények és módszerek

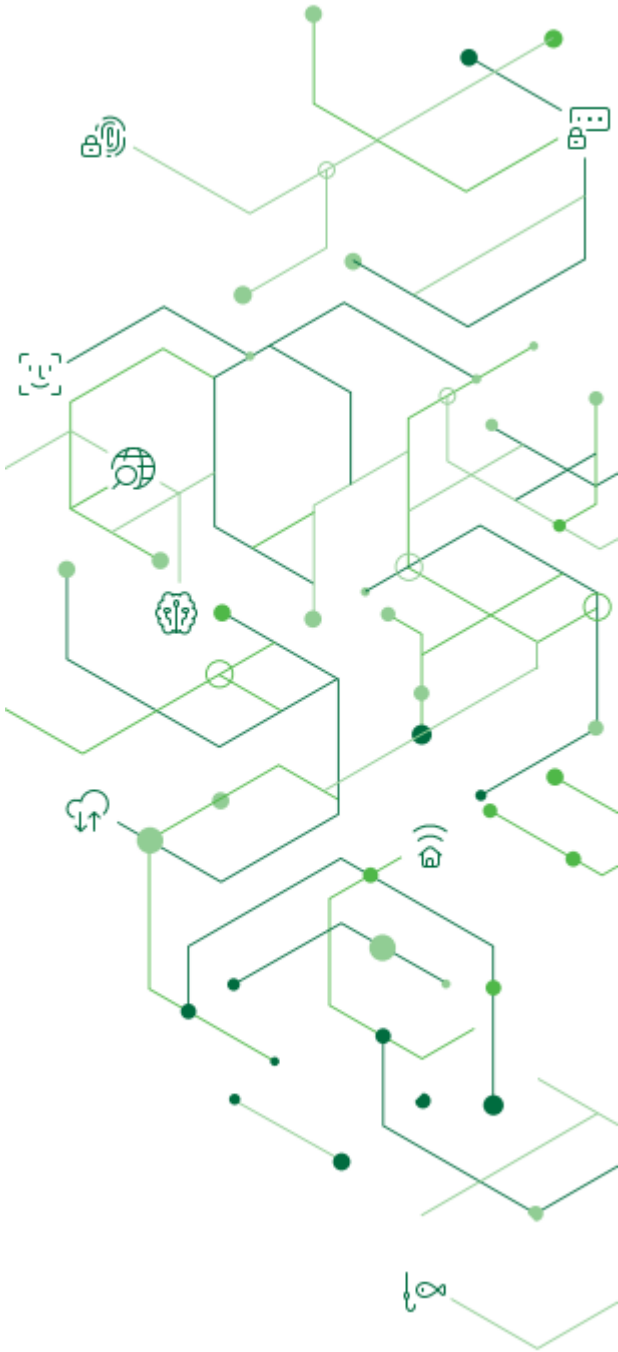


Célok

- Biztonsági kockázatok kerülése
- Üzleti titkok védelme
- Jogszabályi megfelelés
- Különböző helyen / formában tárolt adatok



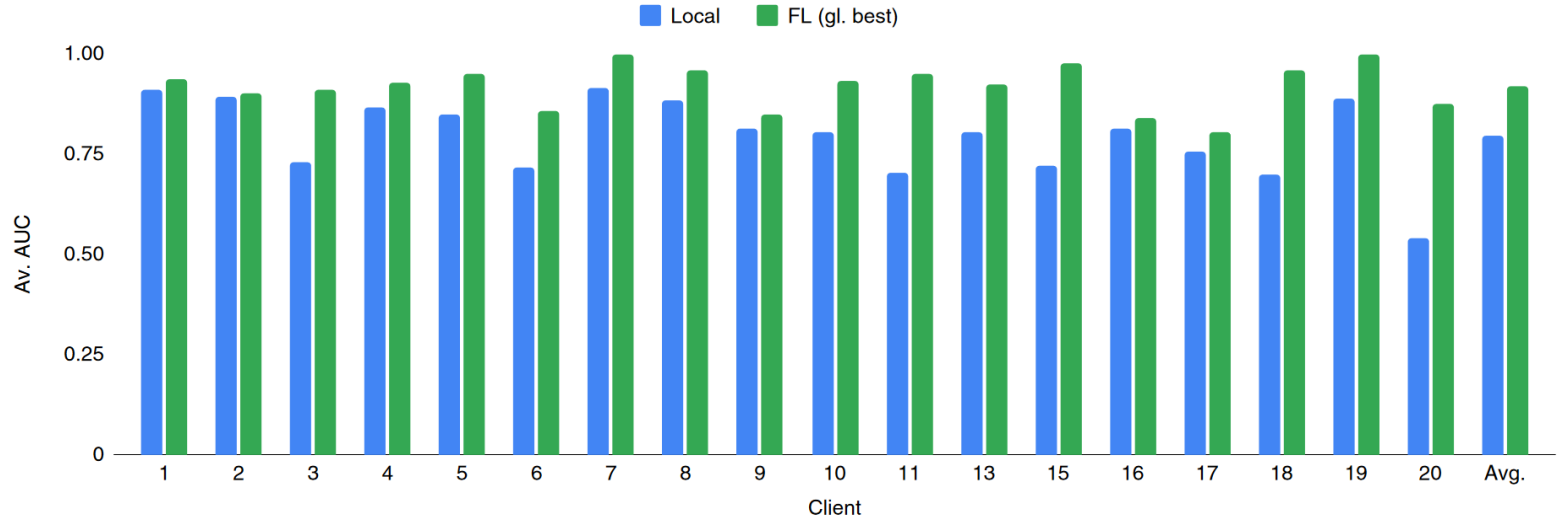
Gyakorlati példák



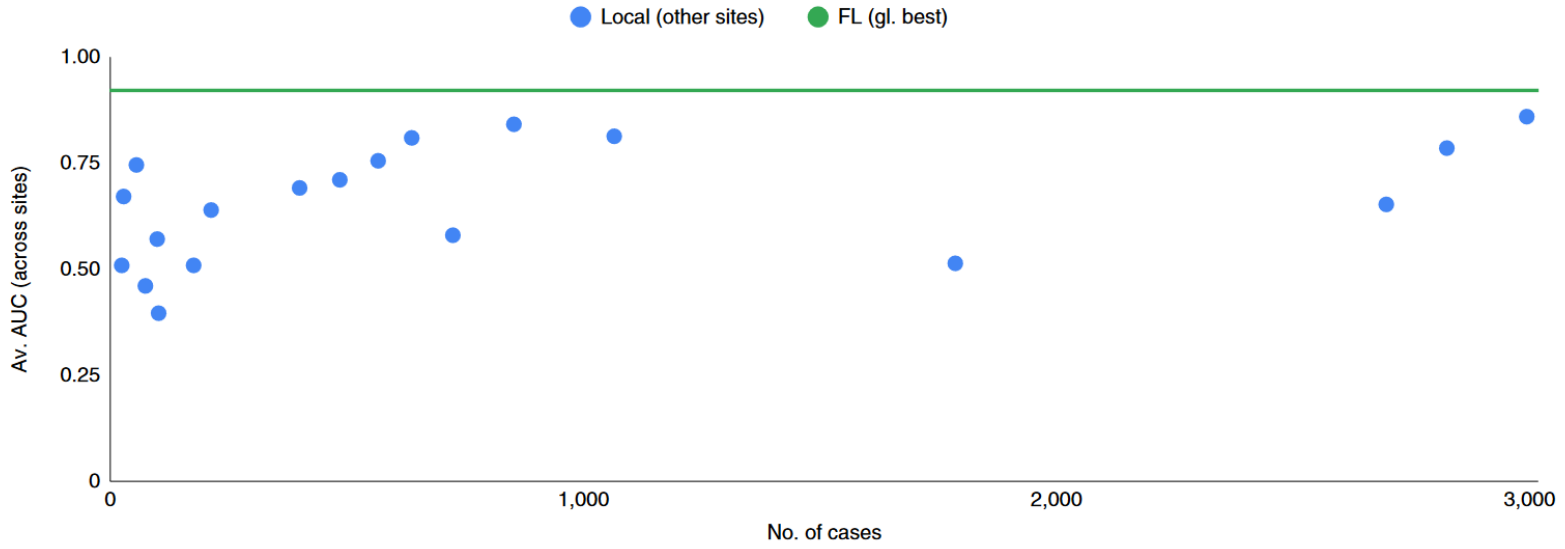
Gboard
Prediktív szövegbevitel

- Érzékeny felhasználói adatok
- Nagy számú eszköz
- Kevés hardvererőforrás

COVID-19 Oxigénszükséglet



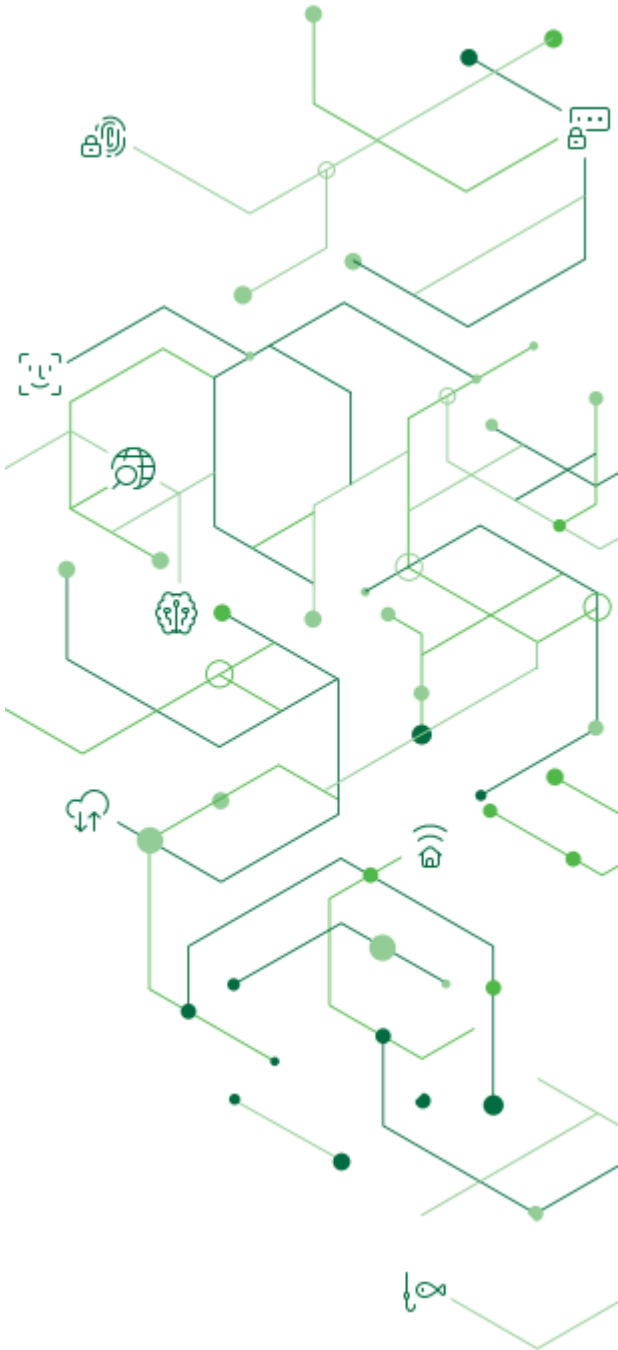
- Érzékeny adatok, jogi korlátok
- Különböző típusúak:
  - Szöveges: kor, vérnyomás, …
  - Képi: röntgenkép
- Túlteljesíti a lokális modelleket



Pénzügyi szektor

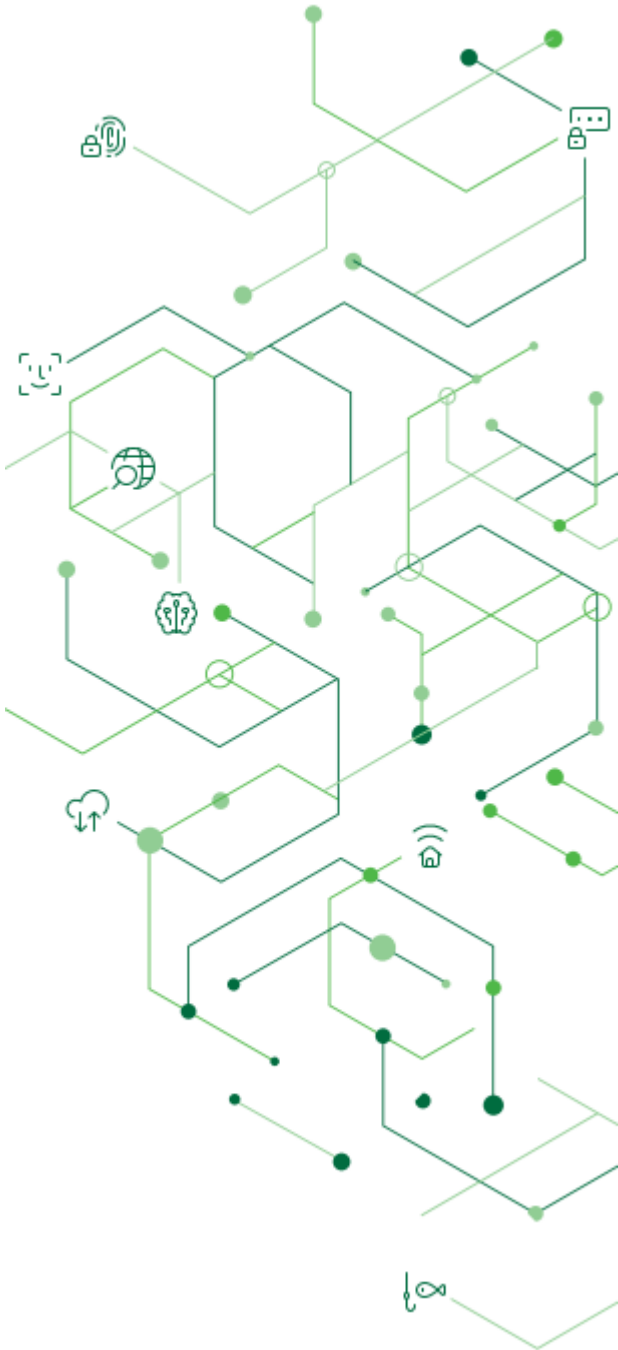
- Pénzügyi visszaélések
- Hitelkockázat becslése

- Egy bank különböző rendszereiben tárolt információk
- Különböző intézmények között



Köszönöm a figyelmet!

A KULTURÁLIS ÉS INNOVÁCIÓS MINISZTÉRIUM EKÖP-KDP-24 KÓDSZÁMÚ EGYETEMI KIVÁLÓSÁGI ÖSZTÖNDÍJ PROGRAMJÁNAK KOOPERATÍV DOKTORI PROGRAMJÁNAK A NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS ALAPBÓL FINANSZÍROZOTT SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.



ELTE IK INFORMATIKAI KAR

otpbank

KIBERLAB

EKÖP
Egyetemi Kutatói Ösztöndíj Program