Abstrakt pro práci Federated learning od Martina Georgiu

Pokrok v oblasti strojového učení v posledních letech byl bezprecedentní, přesto je stále potřeba stále více dat pro trénování umělých neuronových sítí (artificial neural network, ANN). V sektorech jako je zdravotnictví je velice těžké, většinou nereálné, vytvořit jeden soubor dat, který by konsolidoval všechny pacientské informace z různých nemocnic. Proto lze jakékoli trénování ANN provádět výhradně lokálně na datech jedné dané nemocnice. Federativní učení (FL) je nový přístup, který lze v takovém prostředí použít a uchovat tak uživatelská data v soukromí. V této práci porovnáváme FL s jinými přístupy usilujícími o stejný cíl, zaměřujeme se na bezpečnost FL a prozkoumáváme konkrétní strategie pro FL. Nakonec jsme také vytvořili plně funkční open-source ukázku analýzy pih natrénovanou pomocí FL. Tu lze snadno rozšířit a použít i s jinými soubory dat a cíly.