Slovenská technická univerzita v Bratislave
Ústav informatiky, informačných systémov a softvérového inžinierstva

Fakulta informatiky a informačných technológií
2023/2024

STU FIIT

ZADANIE BAKALÁRSKEJ PRÁCE

Autor práce:	Hlib Kokin
Študijný program:	informatika
Študijný odbor:	informatika
Evidenčné číslo:	FIIT-16768-117991
ID študenta:	117991
Vedúci práce:	Ing. Oleksandr Lytvyn
Vedúci pracoviska:	doc. Ing. Valentino Vranić, PhD.
Názov práce:	**Ladenie ML hyperparametrov so zachovaním súkromia**
Jazyk, v ktorom sa práca vypracuje:	slovenský jazyk
Špecifikácia zadania:	Strojové učenie umožňuje dosahovať významné výsledky vo viacerých oblastiach. Použiteľnosť výsledkov priamo závisí na kvalitu a reprezentatívnosť dát použitých na tréningovej fáze, ktoré často môžu obsahovať súkromne informácie. Diferenciálne súkromie (angl. Differential Privacy) je jedným zo spôsobov na ochranu súkromia údajov pre strojové učenie. Analyzujte problematiku nastavenia hyperparametrov v strojovom učení s použitím diferenciálneho súkromia. Preskúmajte dostupné riešenia. Implementuje modul na trénovanie vami zvolených modelov strojového učenia na dátach s aplikovaním diferenciálneho súkromia. Vyhodnoťte úspešnosť natrénovaného modelu strojového učenia pomocou dostupných metrík s ohľadom na bilanciu medzi mierou ochrany súkromia a praktickou použiteľnosťou dat. Literatúra: - Papernot, Nicolas, and Thomas Steinke. "Hyperparameter tuning with renyi differential privacy." arXiv preprint arXiv:2110.03620 (2021) - Priyanshu, Aman, et al. "Efficient Hyperparameter Optimization for Differentially Private Deep Learning." arXiv preprint arXiv:2108.03888 (2021). - Abadi, Martin, et al. "Deep learning with differential privacy." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016.
Rozsah práce:	40
Termín odovzdania práce:	21. 05. 2024
Dátum schválenia zadania práce:	
Zadanie práce schválil:	