



УНИВЕРЗИТЕТ У НОВОМ САДУ
ФАКУЛТЕТ ТЕХНИЧКИХ
НАУКА У НОВОМ САДУ



Марко Митошевић

**Додавање подршке за
библиотеку Keras 3 у радно
окружење TensorFlow Federated**

ЗАВРШНИ РАД

Основне академске студије

Нови Сад, 2025

	УНИВЕРЗИТЕТ У НОВОМ САДУ • ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА 21000 НОВИ САД, Трг Доситеја Обрадовића 6	Број:
	ЗАДАТАК ЗА ЗАВРШНИ РАД	Датум:

(Податке уноси предметни наставник - ментор)

Студијски програм:	Софтверско инжењерство и информационе технологије		
Студент:	Марко Митошевић	Број индекса:	SV56/2021
Степен и врста студија:	Основне академске студије		
Област:	Електротехничко и рачунарско инжењерство		
Ментор:	Игор Дејановић		
НА ОСНОВУ ПОДНЕТЕ ПРИЈАВЕ, ПРИЛОЖЕНЕ ДОКУМЕНТАЦИЈЕ И ОДРЕДБИ СТАТУТА ФАКУЛТЕТА ИЗДАЈЕ СЕ ЗАДАТАК ЗА ЗАВРШНИ РАД, СА СЛЕДЕЋИМ ЕЛЕМЕНТИМА: <ul style="list-style-type: none"> - проблем – тема рада; - начин решавања проблема и начин практичне провере резултата рада, ако је таква провера неопходна; 			

НАСЛОВ ЗАВРШНОГ РАДА:


Додавање подршке за библиотеку Keras 3 у радно окружење TensorFlow Federated
--

ТЕКСТ ЗАДАТКА:

<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim aenean sit amet, adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim aenean sit amet, adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.</p>
--

Руководилац студијског програма:	Ментор рада:

Примерак за: <input type="checkbox"/> - Студента; <input type="checkbox"/> - Ментора
--

	УНИВЕРЗИТЕТ У НОВОМ САДУ • ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА 21000 НОВИ САД, Трг Доситеја Обрадовића 6
	КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

Редни број, РБР:	
Идентификациони број, ИБР:	
Тип документације, ТД:	Монографска документација
Тип записа, ТЗ:	Текстуални штампани материјал
Врста рада, ВР:	Дипломски - бечелор рад
Аутор, АУ:	Марко Митошевић
Ментор, МН:	Др Игор Дејановић, редовни професор
Наслов рада, НР:	Додавање подршке за библиотеку Keras 3 у радно окружење TensorFlow Federated
Језик публикације, ЈП:	српски/ћирилица
Језик извода, ЈИ:	српски/енглески
Земља публиковања, ЗП:	Република Србија
Уже географско подручје, УГП:	Војводина
Година, ГО:	2025
Издавач, ИЗ:	Ауторски репринт
Место и адреса, МА:	Нови сад, трг Доситеја Обрадовића 6
Физички опис рада, ФО: <small>(поглавља/страна/ цитата/табела/слика/графика/прилога)</small>	6/20/4/0/1/0/0
Научна област, НО:	Електротехничко и рачунарско инжењерство
Научна дисциплина, НД:	Примењене рачунарске науке и информатика
Предметна одредница/Кључне речи, ПО:	Keras, TensorFlow Federated, IDE
УДК	
Чува се, ЧУ:	У библиотеци Факултета техничких наука, Нови Сад
Важна напомена, ВН:	
Извод, ИЗ:	Овај документ представља упутство за писање завршних радова на Факултету техничких наука Универзитета у Новом Саду. У исто време је и шаблон за Turst.

Датум прихватања теме, ДП:	
Датум одбране, ДО:	01.01.2025
Чланови комисије, КО:	Председник: Др Петар Петровић, ванредни професор
	Члан: Др Марко Марковић, доцент
	Члан, ментор: Др Игор Дејановић, редовни професор

Потпис ментора

	UNIVERSITY OF NOVI SAD • FACULTY OF TECHNICAL SCIENCES 21000 NOVI SAD, Trg Dositeja Obradovića 6
	KEY WORDS DOCUMENTATION

Accession number, ANO :	
Identification number, INO :	
Document type, DT :	Monographic publication
Type of record, TR :	Textual printed material
Contents code, CC :	
Author, AU :	Marko Mitosevic
Mentor, MN :	Igor Dejanović, Phd., full professor
Title, TI :	Adding support for the Keras 3 library to the TensorFlow Federated framework
Language of text, LT :	Serbian
Language of abstract, LA :	Serbian
Country of publication, CP :	Republic of Serbia
Locality of publication, LP :	Vojvodina
Publication year, PY :	2025
Publisher, PB :	Author's reprint
Publication place, PP :	Novi Sad, Dositeja Obradovica sq. 6
Physical description, PD : (chapters/pages/ref./tables/pictures/graphs/appendixes)	6/20/4/0/1/0/0
Scientific field, SF :	Electrical and Computer Engineering
Scientific discipline, SD :	Applied computer science and informatics
Subject/Key words, S/KW :	Keras, TensorFlow Federated, IDE
UC	
Holding data, HD :	The Library of Faculty of Technical Sciences, Novi Sad, Serbia
Note, N :	
Abstract, AB :	This document provides guidelines for writing final theses at the Faculty of Technical Sciences, University of Novi Sad. At the same time, it serves as a Typst template.

Accepted by the Scientific Board on, ASB :				
Defended on, DE :	01.01.2025			
Defended Board, DB :	President:	Petar Petrović, Phd., assoc. professor		
	Member:	Marko Marković, Phd., asist. professor		
	Member, Mentor:	Igor Dejanović, Phd., full professor		
		<table><tr><td>Menthor's sign</td></tr><tr><td></td></tr></table>	Menthor's sign	
Menthor's sign				



УНИВЕРЗИТЕТ У НОВОМ САДУ • ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА
21000 НОВИ САД, Трг Доситеја Обрадовића 6

ИЗЈАВА О НЕПОСТОЈАЊУ СУКОБА ИНТЕРЕСА

Изјављујем да нисам у сукобу интереса у односу ментор – кандидат и да нисам члан породице (супружник или ванбрачни партнер, родитељ или усвојитељ, дете или усвојеник), повезано лице (крвни сродник ментора/кандидата у правој линији, односно у побочној линији закључно са другим степеном сродства, као ни физичко лице које се према другим основама и околностима може оправдано сматрати интересно повезаним са ментором или кандидатом), односно да нисам зависан/на од ментора/кандидата, да не постоје околности које би могле да утичу на моју непристрасност, нити да стичем било какве користи или погодности за себе или друго лице било позитивним или негативним исходом, као и да немам приватни интерес који утиче, може да утиче или изгледа као да утиче на однос ментор-кандидат.

У Новом Саду, дана _____

Ментор

Кандидат

Садржај

1	Увод	1
1.1	Мотивација	1
1.2	Циљеви рада	2
1.3	Организација рада	2
2	Теоријске основе	3
2.1	Федеративно учење	3
2.2	Оптимизована диференцијална приватност	4
3	Стање у области	7
4	Закључак	9
	Биографија	17
	Литература	19

1.1 Мотивација

Модерна интегрисана развојна окружења (*Integrated Development Environment*, IDE) имају велики број функционалности које помажу програмерима да ефикасно рукују пројектима великог обима. Једна од кључних функционалности у IDE-овима, попут *IntelliJ IDEA*, је претрага *Search Everywhere* (SE), која кориснику на једном месту омогућава да претражи све функционалности окружења, као и све датотеке и њихов садржај унутар пројектне структуре [1].

Корисници често не знају тачно име функционалности коју желе да пронађу, што отежава претрагу. Како би се овај проблем ублажио, истражују се решења модела машинског учења (ML) која могу да предвиде име жељене функционалности. Коришћењем ових модела могуће је направити препоруку претраге, чиме би се олакшало коришћење функционалности SE. Препорука би била најефикаснија уколико би модел био трениран над претходним претрагама корисника и других корисника, као и над контекстом под којим је претрага позвана.

Тренирање модела над осетљивим корисничким подацима представља изазов у погледу приватности и поверљивости. Многе компаније морају чувати поверљивост свог кода и информационих система. Уредбе о заштити података корисника попут Опште уредбе о заштити података (*General Data Protection Directive*, GDPR), која је ступила на снагу у Европској Унији, забрањују обраду података без експлицитне сагласности корисника или адекватног правног основа [2]. Наведена ограничења онемогућавају директно слање података на централни сервер ради тренирања модела.

Постоје технике ML које имају способност да чувају поверљивост тренинг података. Најпознатије су федеративно учење (*Federated Learning*, FL) [3] и диференцијална приватност (*Differential Privacy*, ODP) [4]. Ове технике се базирају на дистрибутивном ML којим се гарантује поверљивост података. Мана код тренутне имплементације FL је недостатак подршке за учитавање најновијих модела, који су потребни да тачно предвиде претрагу SE. Елиминисањем ове мане би се отворила могућност за шире коришћење FL у индустрији.

Циљ овог рада је додавање подршке за новије моделе у радно окружење отвореног кода *TensorFlow Federated* (TFF), које имплементира технику FL [5].

1.2 Циљеви рада

Главни циљ овог рада је да се имплементира функционална подршка за библиотеку *Keras* 3 унутар радног окружења TFF. Да би се то постигло, потребно је испунити следеће циљеве:

- Анализирати постојећу архитектуру TFF-а и њену зависност од библиотеке *Keras* 2.
- Рефакторисати компоненте TFF-а тако да се постигла компатибилност са верзијом 3 библиотеком *Keras*, уз очување компатибилности са верзијом 2.
- Имплементирати компоненту која омогућава јединствен начин руковања моделима и компонентама обе верзије библиотеке *Keras*.
- Имплементирати тестове за тестирање компатибилности библиотеке *Keras* 3 са рефакторисаним компонентама TFF.
- Евалуирати функционалну исправност имплементиране подршке проласком свих тестова.
- Демонстрирати предности интеграције *Keras* 3 коришћењем модела са знатно бољим перформансама (нпр. *Gemma* 3) у односу на *Keras* 2 моделе (нпр. GPT-2).

1.3 Организација рада

Рад је организован у пет поглавља. Прво поглавље, Увод, дефинише мотивацију и циљеве рада, уводећи читаоца у проблематику приватности података у машинском учењу и циљ рада. Друго поглавље, Теоријске основе, описује концепт федеративног учења, архитектуру и примену радног окружења TFF, као и библиотеке *Keras*. Треће поглавље, Имплементација подршке за *Keras* 3, описује детаље рефакторисања кода и увођење нових компатибилних функционалности. Четврто поглавље, Резултати и дискусија, представља евалуацију решења и поређење перформанси нових и старих модела. Пето поглавље, Закључак, сумира постигнуте резултате и предлаже правце за даља унапређења.

Глава 2

Теоријске основе

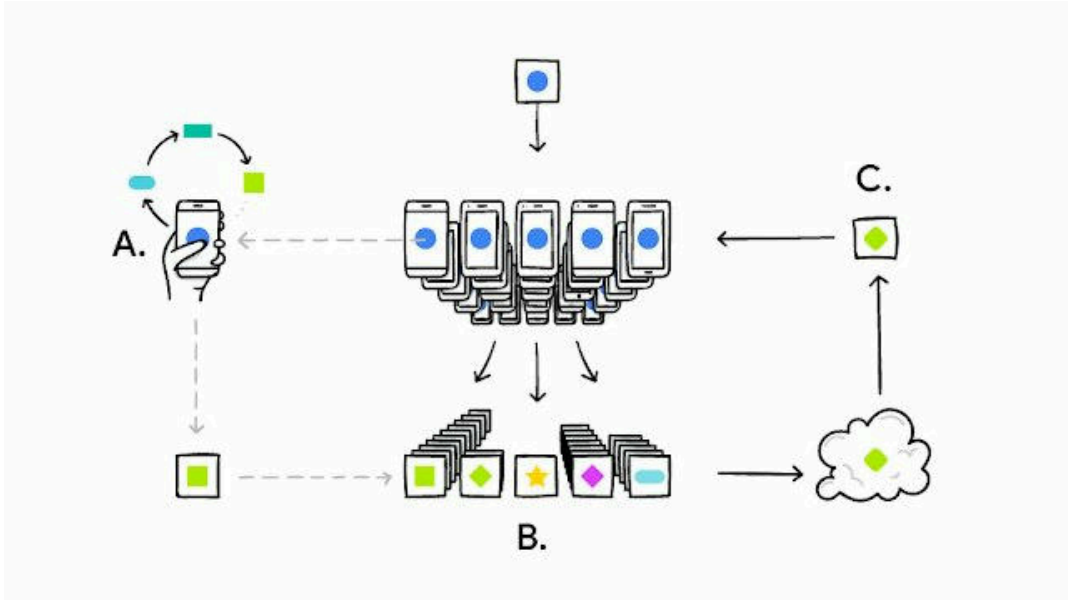
2.1 Федеративно учење

Федеративно учење (*Federated Learning*, FL) је техника машинског учења која омогућава децентрализовано тренирање модела над поверљивим подацима. За разлику од традиционалног централизованог приступа, где се сви подаци прикупљају на једном серверу, FL гарантује да подаци никада не напусте оригинални уређај. Овај приступ је кључан за очување поверљивости и усклађеност са регулативама за заштиту података [3].

Систем федеративног учења функционише на принципу децентрализоване обуке. Сваки уређај (клијент) у систему поседује локалну копију дељеног модела. Локални модел се тренира искључиво коришћењем података који се налазе на том уређају. Након завршетка локалног тренинга, уређај не шаље своје приватне податке, већ само ажуриране тежине модела централном серверу.

Централни сервер има улогу агрегатора. Он прикупља ажуриране тежине од великог броја уређаја и агрегира резултате. Израчунати, побољшани глобални модел се затим шаље назад свим уређајима у систему, и циклус обуке се понавља. Процес се изводи итеративно, чиме се временом побољшавају перформансе дељеног модела, без употребе приватних података.

Потенцијалне области примене федеративног учења су индустрије које захтевају учење модела над поверљивим скуповима података великог броја корисника, као што су медицина, роботика и софтверско инжењерство. Најутицајнија примена FL-а над великим скупом података је предвиђање корисничког уноса на Gboard Android тастатури. На слици 1 приказан је примена FL за предвиђање корисничког уноса на Gboard Android тастатури [6].



Слика 1: Примена FL за предвиђање корисничког уноса на *Gboard Android* тастатури. Мобилни уређај локално тренира над претходним корисничким уносима и ажуриране тежине шаље централном серверу (А). Централни сервер агрегира примљене тежине (В) и шаље свим уређајима побољшан дељени модел (С) [6].

Кључна предност Федеративног учења је гарантована поверљивост података, јер подаци остају искључиво на оригиналним уређајима, што омогућава децентрализовано тренирање. Ова техника, заједно са оптимизованом диференцијалном приватношћу, базира се на дистрибутивном машинском учењу којим се ефикасно чува поверљивост тренинг података.

2.2 Оптимизована диференцијална приватност

Диференцијална приватност (Differential Privacy, DP) је математички дефинисан оквир који квантификује и гарантује приватност појединца у оквиру базе података. Основна идеја је увођење контролисаног шума у процес обраде података, тако да присуство или одсуство записа једног појединца у скупу података не може значајно утицати на коначни излаз анализе или модела. Овај концепт пружа гаранцију да нападач не може са сигурношћу закључити да ли је одређени појединац био део скупа података [7].

Математичка дефиниција DP се најчешће изражава параметрима ϵ (епсилон) и δ (делта). Алгоритам A је (ϵ, δ) диференцијално приватан ако за свака два скупа података која се разликују за само један узорак D и D' и за сваки излазни скуп резултата S важи следећа неједнакост [8]:

$$P[A(D) \in S] \leq e^\epsilon * P[A(D') \in S] + \delta$$

, где је P вероватноћа. Загарантовано је да се вероватноћа добијања било ког излаза не може променити за фактор већи од e^ϵ ако се један узорак дода или уклони.

Параметар ϵ одређује горњу границу промене вероватноће излаза приликом укључивања или изостављања једног узорака података. Нижа вредност ϵ означава бољу приватност, али потенцијално и мању тачност модела. За ϵ једнак нули излази су индентични и добија се загарантована приватност, што је у пракси немогуће достићи.

Параметар δ представља вероватноћу да горња граница ϵ неће бити задовољена. У идеалном теоријском случају δ тежи нули, чиме се добија диференцијална приватност која зависи само од параметра ϵ , док се у практичним применама поставља на малу вредност (нпр. 10^{-5}), која би требало да буде мања од инверзне вредности величине скупа података ($\frac{1}{\text{величина скупа података}}$), чиме се смањује ризик угрожавања приватности појединог узорака у скупу података.

Оптимизована диференцијална приватност (Optimized Differential Privacy, ODP) представља варијанту примене DP, која је специјализована за контекст машинског учења и великих, дистрибуираних система. Главни изазов код стандардне DP је постизање оптималног компромиса између приватности и тачности модела. ODP користи методе попут клиповања градијента (Gradient Clipping) [9] пре додавања шума, како би се смањио потребан ниво шума и одржала тачност модела, уз истовремено задовољавање дефинисане ϵ границе приватности.

У контексту дистрибутивног машинског учења, DP се може применити на два начина [10]:

- Локална диференцијална приватност (Local Differential Privacy, LDP): Шум се додаје директно на сирове податке или ажурирања модела на самом уређају (клијенту), чиме се добија заштита од злонамерног централног сервера.
- Централна диференцијална приватност (Central Differential Privacy, CDP): Шум се додаје на централном серверу, након што су прикупљени сви доприноси клијената. У FL, шум се додаје на тежине модела приликом агрегације.

Технике FL и DP су комплементарне. FL пружа технички механизам за децентрализацију тренинга и спречава прикупљање сирових података на серверу, док DP/ODP пружа математичку гаранцију да чак ни ажурирања модела не могу открити податке појединаца. Применом ODP на ажуриране тежине модела током процеса агрегације, спречава се да сервер може из модела закључити осетљиве информације о појединачним тренинг подацима. Ова комбинација је неопходна за изградњу модерних система машинског учења који су у потпуности усклађени са регулативама за заштиту података.

Глава 3

Стање у области

Даља поглавља садрже опис стања у области, коришћене технологије, опис дизајна и имплементације итд. Најбоље је да свако поглавље пишете у посебном `.typ` фајлу. Не заборавите да га укључите у главом фајлу `zavrсни-rad.typ` (претражити све `TODO` коментаре).

Глава 4

Закључак

У закључку дајте кратак преглед онога шта урађено, са освртом на проблеме који су решени, предности и мане решења и правце даљег развоја.

Списак слика

Слика 1	Примена FL за предвиђање корисничког уноса на <i>Gboard Android</i> тастатури. Мобилни уређај локално тренира над претходним корисничким уносима и ажуриране тежине шаље централном серверу (А). Централни сервер агрегира примљене тежине (В) и шаље свим уређајима побољшан дељени модел (С) [6]	4
---------	--	---

Списак листинга

Списак табела

Биографија

Овде написати своју кратку биографију.

Литература

- [1] JetBrains, „IntelliJ IDEA“. Приступљено: 12. Октобар 2025. [На Интернету]. Available at: <https://www.jetbrains.com/idea>
- [2] E. Union, „Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)“. Приступљено: 12. Октобар 2025. [На Интернету]. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- [3] G. Cloud, „Federated learning: a guide to what it is and how it works“. Приступљено: 12. Октобар 2025. [На Интернету]. Available at: <https://cloud.google.com/discover/what-is-federated-learning?hl=en>
- [4] M. A. I. U. D. T. Q. Maria Iqbal Asadullah Tariq, „FL-ODP: An Optimized Differential Privacy Enabled Privacy Preserving Federated Learning“. Приступљено: 12. Октобар 2025. [На Интернету]. Available at: <https://ieeexplore.ieee.org/document/10287349>
- [5] Google, „TensorFlow Federated: Machine Learning on Decentralized Data“. Приступљено: 12. Октобар 2025. [На Интернету]. Available at: <https://www.tensorflow.org/federated>
- [6] R. M. S. R. F. B. S. A. H. E. C. K. D. R. Andrew Hard Kanishka Rao, „Federated Learning for Mobile Keyboard Prediction“. Приступљено: 12. Октобар 2025. [На Интернету]. Available at: <https://arxiv.org/abs/1811.03604>
- [7] C. Dwork, „Differential Privacy“. Приступљено: 16. Октобар 2025. [На Интернету]. Available at: https://doi.org/10.1007/11787006_1
- [8] A. R. Cynthia Dwork, *The Algorithmic Foundations of Differential Privacy*. University of Pennsylvania, 2014.
- [9] I. G. B. M. I. M. K. T. L. Z. Martín Abadi Andy Chu, „Deep Learning with Differential Privacy“. Приступљено: 19. Октобар 2025. [На Интернету]. Available at: https://link.springer.com/chapter/10.1007/978-3-540-79228-4_1
- [10] E. D. C. U. C. L. D. A. T. I. Mohammad Naseri Jamie Hayes, „Local and Central Differential Privacy for Robustness and Privacy in Federated Learning“. Приступљено: 12. Октобар 2025. [На Интернету]. Available at: <https://arxiv.org/abs/2508.10000>

пљено: 19. Октобар 2025. [На Интернету]. Available at: <https://arxiv.org/abs/2009.03561>