УНИВЕРЗИТЕТ У НОВОМ САДУ
ПРИРОДНО-МАТЕМАТИЧКИ ФАКУЛТЕТ

ИЗВЕШТАЈ О ОЦЕНИ МАСТЕР РАДА

I ПОДАЦИ О КОМИСИЈИ

1. Датум и орган који је именовао Комисију

05.04.2019. Веће Департмана за математику и информатику Природно-математичког факултета Универзитета у Новом Саду

2. **Састав Комисије са назнаком имена и презимена сваког члана, звања, назива уже научне области за коју је изабран у звање, датума избора у звање и назив факултета, установе у којој је члан комисије запослен:**

- др Срђан Шкрбић, редовни професор Природно-математичког факултета у Новом Саду, ужа научна област: информациони системи, изабран у звање: 15.10.2014. - председник
- др Драгана Бајовић, доцент Факултета техничких наука у Новом Саду, ужа научна област: телекомуникације и обрада сигнала, изабрана у звање: 01.12.2015. - ментор
- др Душан Јаковетић, доцент Природно-математичког факултета у Новом Саду, ужа научна област: математичко моделирање, изабран у звање: 15.11.2015. - члан

II ПОДАЦИ О КАНДИДАТУ

1. Име, име једног родитеља, презиме:

Јелена, Бранко, Новаковић

2. **Датум рођења, општина, република:**

18.12.1991., Крушевац, Србија

3. **Година уписа на дипломске академске студије, смер/усмерење:**

2016., Мастер математичар - примењена математика (модул: наука о подацима)

III НАСЛОВ МАСТЕР РАДА

Очување приватности у обради података: Истраживање о примени диференцијалне приватности у стаблима одлучивања.

V ПРЕГЛЕД МАСТЕР РАДА

Мастер рад „Очување приватности у обради података: Истраживање о примени диференцијалне приватности у стаблима одлучивања.“ садржи 8 поглавља: 1. Увод, 2. Технике очувања приватности, 3. Диференцијална приватност, 4. Диференцијална приватност у анализи података, 5. Стабло одлучивања, 6. Диференцијална приватност у стаблу одлучивања, 7. Симулација експеримената, 8. Закључак, подељених на мање секције. Рад садржи 18 графика, 3 листинга (цитирана кода), 2 алгоритма и једно додатно објашњење у виду апендикса. На крају, приложен је и списак коришћене литературе сачињен од 52 референце.

У овом раду приказујемо имплементацију два алгоритма диференцијалне приватности у оквиру стабла одлучивања. Алгоритме тестирамо на неколико јавно доступних скупова података и поредимо резултате.

IV ВРЕДНОВАЊЕ ПОЈЕДИНИХ ДЕЛОВА МАСТЕР РАДА

Прво поглавље представља увод у тематику рада, мотивацију за избор теме и опис остатка рада.

Друго поглавље пролази кроз технике очувања приватности настале пре диференцијалне приватности. Дефинишемо анонимизацију, К-анонимизацију, Т-блискост и Л-диверзитет, и описујемо које су предности и мане поменутих техника.

У трећем поглављу уводимо појам диференцијалне приватности. Поред саме дефиниције диференцијалне приватности, у овом поглављу дефинишемо и два најпознатија механизма (Лапласов и експоненцијални механизам) помоћу којих се диференцијална приватност спроводи у пракси. Такође, у овом поглављу уводимо и теореме композиције.

Четврто поглавље описује два основна приступа за имплементацију диференцијалне приватности у анализи података (интерактивни и неинтерактивни приступ), као и начине на које се може одабрати параметар епсилон који дефинише ниво приватности обезбеђен помоћу механизама диференцијалне приватности.

У петом поглављу дефинишемо алгоритам стабло одлучивања. Поглавље се састоји из три дела. У првом делу дајемо кратку мотивацију и опис стабла одучивања, у другом делу описујемо како се креира стабло одлучивања, док у трећем делу говоримо о томе како се бира атрибут и вредност атрибута по коме ће стабло креирати нове гране.

Шесто поглавље се бави применом диференцијале приватности у стаблима одлучивања. Поглавље се састоји из шест делова. Први део нам открива у којим деловима алгоритма се имплементира диференцијална приватност. Други део говори о подели параметра епсилон (тј. буџета диференцијалне приватности) кроз слојеве стабла одлучивања. Трећи део описује како се креира диференцијално приватно стабло одлучивања, док четврти део уводи функције које се користе за одабир атрибута за креирање нових грана. Пети део дефинише услове конвергенције алгоритма, док шести део презентује имплементацију два алгоритма у програмском језику „Python“.

Следеће поглавље бави се извршеним експериментима. Поглавље је подељено у више делова. Прво се упознајемо са поставкама рачунара на којем су тестирања вршена, затим пролазимо кроз сетове података над којима вршимо тестирања. У трећем делу упознајемо се са различитим метрикама које се користе за мерење перформанси ових алгоритама. Након тога, за сваки алгоритам приказујемо обављена тестирања у виду графика уз одговарајуће коментаре.

Последње поглавље износи закључке на основу остварених резултата, као и

	предлоге и могућности за будући рад.
VI	**ЗАКЉУЧЦИ ОДНОСНО РЕЗУЛТАТИ ИСТРАЖИВАЊА**
	У овом раду описујемо два алгоритма диференцијалне приватности у стаблима одлучивања. За оба алгоритма презентујемо теоријску основу, имплементацију у програмском језику „Python“, као и резултате добијене тестирањем алгоритама на пар јавно доступних сетова података. Показујемо да је могуће постићи добре резултате алгоритама и у окружењу које гарантује очување приватности. Такође, закључујемо да диференцијална приватност понекад захтева модификацију постојећих алгоритама машинског учења и да алгортими који дају најбоље резултате на стварним подацима, не морају увек давати најбоље резултате над зашумљеним подацима.
VII	**КОНАЧНА ОЦЕНА МАСТЕР РАДА**
	Мастер рад је у потпуности урађен у складу са одобреном темом. Сви проблеми, наведени у пријави теме, су детаљно анализирани и приказани. Рад је прегледно и добро написан, а главни резултати су илустровани кроз примене на реалним подацима.
VIII	**ПРЕДЛОГ**
	На основу укупне оцене, Комисија предлаже да се мастер рад прихвати, а кандидату Јелени Новаковић одобри одбрана.

Нови Сад, 11.09.2019.

ПОТПИСИ ЧЛАНОВА КОМИСИЈЕ

др Срђан Шкрбић
редовни професор ПМФ-а, председник

_____

др Драгана Бајовић
доцент ФТН-а, ментор

_____

др Душан Јаковетић
доцент ПМФ-а, члан

_____