КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА
ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 07.10.2025 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Никола Новаковић под насловом „Примена библиотеке за креирање и одбрану од обмањујућих захтева у детекцији DNS ексфилтрације". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Никола Новаковић је рођен 18.04.1996. године у Београду. Завршио је основну школу „Старина Новак" и Пету београдску гимназију у Београду. Електротехнички факултет уписао је 2015. године. Дипломирао је на одсеку за Рачунарску технику и информатику 2021. године са просечном оценом 7,78. Дипломски рад одбранио је у септембру 2021. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за Рачунарску технику и информатику уписао је у октобру 2021. године. Положио је све испите са просечном оценом 8,20. Запослен је у струци на позицији инжењера дигиталне верификације у компанији Elsys Eastern Europe.

2. Извештај о студијском истраживачком раду

Кандидат Никола Новаковић је као припрему за израду мастер рада проучио релевантну литературу из области машинског учења, напада на моделе машинског учења, посебно технике креирања обмањујућих напада, безбедности модела и детекције DNS ексфилтрације. У оквиру студијског истраживачког рада анализирани су различити типови обмањујућих напада (енг. Adversarial attack), њихова примена у тзв. black-box поставци, као и могућности одбране модела. Посебно је истражена примена Adversarial Robustness Toolbox (ART) библиотеке, за креирање и одбрану од обмањујућих напада на моделе машинског учења, анализа напада избегавања, напада закључивања о тренинг скупу и напада екстракције модела у контексту табеларних DNS података.

3. Опис мастер рада

Мастер рад обухвата 36 страна без насловне стране, са укупно 10 слика и 8 референци. Рад садржи увод, 3 поглавља и закључак (укупно 5 поглавља), списак коришћене литературе, списак скраћеница, списак слика и прилог које показује начин коришћења ART библиотеке.

Прво поглавље представља увод у коме су описани предмет, мотивација и циљ рада. Такође су уведени основни појмови обмањујућих напада на моделе машинског учења и објашњен значај анализе рањивости модела у контексту безбедности система машинског учења.

У другом поглављу су представљени најважнији концепти напада DNS ексфилтрације који је коришћен за анализу обмањујућих напада. Показани су приступи њеној детекцији, описан је коришћени скуп података и припрема одлика. Посебна пажња посвећена је одликама појединачних DNS захтева, које су у раду коришћене као основа за експериментални део рада.

У трећем поглављу су описани обмањујући напади релевантни за овај рад, интеграција XGBoost класификатора са ART библиотеком, експериментална поставка, као и напади и одбране који су коришћени у раду. Обрађени су напад избегавања типа HSJA, напад закључивања о тренинг скупу и напад екстракције модела, као и одбране засноване на тренингу уз коришћење обмањујућих примера, ограничењу буџета упита и санитизацији излаза модела.

У четвртом поглављу су приказани резултати експеримената и дата је дискусија о успешности разматраних напада и одбрана. Анализирани су резултати HSJA напада избегавања, са посебним осврtом на промене одлика у успешним обмањујућим примерима, резултати напада закључивања припадности и ефекти различитих врста одбрана од обмањујућих напада, као и резултати напада екстракције и степен слагања заменског модела са моделом метом.

У петом поглављу дат је закључак рада, у оквиру кога су сумирани главни налази и истакнут значај анализе осетљивости на обмањујуће нападе у процени робусности, приватности и корисности модела за детекцију DNS ексфилтрације. Такође су наведени могући правци даљег рада.

4. Анализа са кључним резултатима

Мастер рад дипл. инж. Николе Новаковића бави се анализом рањивости модела машинског учења за детекцију DNS ексфилтрације у присуству обмањујућих напада. У раду је успешно примењена ART библиотека и анализирани су напади избегавања, напади закључивања о тренинг скупу и напади екстракције модела.

Основни доприноси рада су: 1) анализа примене ART библиотеке у проблему детекције DNS ексфилтрације над табеларним подацима; 2) експериментална анализа HSJA напада избегавања и одбрана као што су тренинг са обмањујућим примерима и ограничење буџета упита; 3) анализа напада закључивања припадности и напада екстракције модела у истом безбедносном домену; 4) разматрање компромиса између робусности, приватности и корисности модела.

5. Закључак и предлог

Кандидат Никола Новаковић је у свом мастер раду успешно анализирао примену метода креирања обмањујућих напада у проблему детекције DNS ексфилтрације. Кандидат је исказао самосталност и систематичност у раду, као и способност да релевантне резултате експериментално прикаже и протумачи. На основу горе наведеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Николе Новаковића под насловом „Примена библиотеке за креирање и одбрану од обмањујућих захтева у детекцији DNS ексфилтрације" прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 28.04.2026. године

Чланови комисије:

др Павле Вулетић Редовни професор
сагласан, 27.04.2026.

др Жарко Станисављевић Ванредни професор
сагласан, 28.04.2026.

Кристијан Жижа Асистент
сагласан, 27.04.2026.