УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
Булевар краља Александра 73, 11000 Београд, Србија
Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 23.03.2021. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Јоване Матић под насловом „Примена машинског учења у анализи и детекцији напада на ИоТ уређаје“. Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Јована Матић је рођена 14.09.1996. године у Београду. Завршила је основну школу „20. Октобар" у Београду као вуковац. Уписала је Девету гимназију „Михаило Петровић Алас“ у Београду, коју је завршила као одличан ђак. Електротехнички факултет уписала је 2015. године. Дипломирала је у року као студент на Одсеку за рачунарску технику и информатику 2019. године са просечном оценом 8,93. Дипломски рад одбранила је 2019. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу Сигнали и системи уписала је у октобру 2019. године. Положила је све испите са просечном оценом 9,60. Запослена је у струци на позицији софтвер инжењера.

2. Опис мастер рада

Мастер рад обухвата 56 страна, са укупно 31 сликом, 14 табела и 68 референци. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља), списак коришћене литературе, списак скраћеница, списак слика и списак табела.

Прво поглавље представља увод у коме су описани предмет, мотивација и циљ рада. Уведен је појам ботнета, као најчешће врсте компромитације ИоТ уређаја, где је као највећи проблем наведено константно усавршавање малициозних понашања.

У другом поглављу описане су основне карактеристике ИоТ уређаја и њиховог мрежног саобраћаја, као и рањивости које из њих произилазе. Наведени су и основни механизми заштите који се могу употребити код ИоТ уређаја.

У трећем поглављу су анализирани различити модели машинског учења који се могу користити у сврху детекције напада на ИоТ уређаје и истакнуте су њихове предности и мане. Такође, разматрани су различити јавно доступни скупови података, њихов садржај и начин прикупљања као и погодност примене.

У четвртом поглављу детаљно су објашњени скупови података који су коришћени у овом раду за тренирање и тестирање модела, алгоритми за препроцесирање података и модел машинског учења који је примењен. Наведене су све коришћене библиотеке и алати, као и параметри са којима су коришћени.

У петом поглављу су изложени резултати свих одрађених експеримената на тренинг и тест скуповима. Објашњен је процес сваког експеримента, као и разлози за његово извршавање. Резултати су анализирани и на основу њих су изведени закључци. Прво су одабрани скупови података обрађени и на основу њих добијени тренинг и два тест скупа који су даље коришћени. Други тест скуп представља податке сакупљене пар година касније, на којима се може видети усавршавање малициозних мрежних токова са временом. Коришћен је за испитивање деградације перформанси модела после неког времена и добрих пракси у овом случају. Одабрани модел, описан у четвртом поглављу, трениран је на тренинг скупу и тестиран на оба тест скупа. Како је примећена велика деградација перформанси на другом тест скупу, рађена су два додатна експеримента. Један је испитивао утицај избора алгоритма

за издвајање битних одлика на деградацију перформанси и стабилност модела, док је други испитивао накнадно дообучавање модела новим малициозним примерима као добру праксу.

Шесто поглавље је закључак у оквиру кога су сумирани најизраженији сигурносни проблеми ИоТ уређаја, као и резултати примењених експеримената. Изведен је закључак да је анализа комуникације бота са командно-контролним центром могућа и да може дати јако добре резултате. Такође, предложене су неке добре праксе за суочавање са проблемом дерадације перформасни услед промена малициозног понашања са временом.

3. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Јоване Матић се бави утврђивањем могућности детекције ИоТ бота на основу његове комуникације са командно-контролним центром, уз примену модела машинског учења, као и испитивањем деградације перформанси таквог модела након одређеног времена услед усавршавања малициозних мрежних токова. У оквиру рада су одабрана два јавно доступна скупа података из којих су издвојени тренинг и два тест скупа. Одабран је и један модел машинског учења који је обучен на тренинг скупу и тестирањем на првом тест скупу показан је потенцијал за детекцију бота на основу комуникације са командно-контролним центром, док је тестирање на другом тест скупу служило за испитивање деградације перформанси модела.

Основни доприноси рада су: 1) имплементација модела машинског учења који са високом осетљивошћу може да детектује ИоТ бот уређај само на основу његове комуникације са командно-контролним центром; 2) испробавање модела, који је дао добре резултате при детекцији напада на неколико јавно доступних скупова података, на новим скуповима и са другачијом сврхом (уместо конкретних напада, детектује се комуникација са командно-контролним центром); 3) практичан приказ нивоа деградације перформанси модела, услед промена малициозних понашања са временом, уз испитивање добрих пракси у овом случају.

4. Закључак и предлог

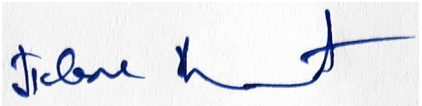
Кандидат Јована Матић је у свом мастер раду имплементирала модел машинског учења који са високом осетљивошћу може да детектује комуникацију бота са командно-контролним центром, утврдила је ниво деградације перформанси модела услед константног усавршавања малициозних понашања и предложила неке добре праксе за суочавање са овим проблемом.

Кандидат је исказао самосталност и систематичност у свом поступку.

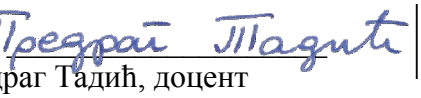
На основу горе наведеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Јоване Матић под насловом „Примена машинског учења у анализи и детекцији напада на ИоТ уређаје“ прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 30.08.2021. године

Чланови комисије:



Др Павле Вулетић, ванредни професор



Др Предраг Тадић, доцент