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 31.08.2021. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Саве Кезића под насловом „Имплементација сигурне заједничке обраде података у облаку коришћењем сигурних процесорских енклава“. Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Сава Кезић је рођен 14.07.1997. године у Београду. Завршио је основну школу „Карађорђе" у Београду као вуковац. Уписао је Трећу београдску гимназију у Београду, коју је завршио као одличан ђак. Електротехнички факултет уписао је 2016. године. Дипломирао је у року као студент на Одсеку за софтверско инжењерство 2020. године са просечном оценом 9,15. Дипломски рад одбранио је 2020. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу Рачунарска техника и информатика уписао је у октобру 2020. године. Положио је све испите са просечном оценом 9,80. Запослен је у струци на позицији девопс инжењера.

2. Извештај о студијском истраживачком раду

Кандидат Сава Кезић је као припрему за израду мастер рада урадио истраживање релевантне литературе која се односи на начине реализације сигурне заједничке обраде података (енг. *secure multiparty computation*). Такође, анализиран је начин рада данас најпознатијих имплементација сигурних хардверских енклава (*AMD SEV* и *Intel SGX*) као и функционалностима услуга заснованих на овим решењима код највећих пружалаца услуга у облаку: MS Azure и Google cloud. Ова решења су упоређена са начином рада *Amazon Nitro* енклава који се разликује због различитих подржаних одлика на процесорима *Amazon AWS* облака, те је у складу са овим истраживањем пројектовано решење за сигурну заједничку обраду података које је приказано у раду.

3. Опис мастер рада

Мастер рад обухвата 42 стране, са укупно 14 слика, 1 табелом и 19 референци. Рад садржи увод, 2 поглавља и закључак (укупно 4 поглавља), списак коришћене литературе, списак скраћеница, списак слика, списак табела и додатак.

Прво поглавље представља увод у коме су описани предмет, мотивација и циљ рада. Уведен је појам *Trusted Execution Environment*-а, као најперспективније решење за заштиту података у току процесирања (енг. *data in use*). Објашњене су основне функционалности данас најпознатијих хардверских *TEE* имплементација, тј. *AMD SEV* и *Intel SGX*, као и дефинисана која *TEE* решења данас нуде највећи пружаоци услуга у облаку.

У другом поглављу детаљно је описан начин функционисања Амазон нитро енклава. Поред дефинисаних основних концепата функционисања нитро енклава, описана су њихова ограничења, начини комуникације као и напредна функционалност атестације енклаве.

У трећем поглављу је дефинисана целокупна имплементација сигурне заједничке обраде података у облаку коришћењем Амазон нитро енклава заједно са Амазоновим KMS помоћним сервисом за чување криптографских кључева. Реализован је сценарио заједничке обраде медицинских података између пет различитих ентитета од којих два представљају провајдере осетљивих података, један провајдера кôда алгоритма машинског учења, један софтверског инжењера одговорног за креирање главне апликације за обраду података и на

крају један који представља архитекту инфраструктуре у облаку одговорног за имплементирање заједничке обраде података у облаку коришћењем Амазон нитро енклава. Описан је ток података, његова имплементација, кôд главне апликације која се извршава унутар нитро енклаве, као и предности и мане ове конкретне имплементације.

Четврто поглавље је закључак у оквиру кога су сумиране све мане конкретне имплементације сигурне заједничке обраде података у облаку коришћењем Амазон нитро енклава заједно са Амазоновим KMS сервисом и начини превазилажења истих потенцијалном модификацијом представљене имплементације. Такође, препоручена су друга *TEE* решења осталих највећих пружаоца услуга у облаку у циљу поспешивања безбедности података сигурне заједничке обраде података у облаку, као што су *GCP*, *Azure* и *IBM*.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Саве Кезића се бави имплементацијом сигурне заједничке обраде података у облаку коришћењем Амазон нитро енклава заједно са помоћним Амазоновим сервисом за чување криптографских кључева. Успешно је реализован прототип апликације који показује како је могуће извршити заједничку обраду медицинских података у којој учествује пет различитих ентитета. У оквиру рада упоређене су данас најкоришћеније хардверске *TEE* имплементације, детаљно је описано функционисање *TEE* решења данас највећег пружаоца услуга у облаку Амазон и упоређено са *TEE* решењима осталих данас најпознатијих пружаоци услуга у облаку, као што су *GCP*, *Azure* и *IBM*.

Основни доприноси рада су: 1) имплементација сигурне заједничке обраде података у облаку коришћењем Амазон нитро енклава коришћењем помоћног Амазоновог сервиса за чување криптографских кључева; 2) испитивање нивоа безбедности податка сигурне заједничке обраде података у облаку коришћењем Амазон нитро енклава, као и могућности измене конкретне имплементације у циљу поспешивања безбедности података 3) испитивање примене *TEE* решења других пружаоца услуга у облаку за исти процес, такође у циљу поспешивања безбедности података

5. Закључак и предлог

Кандидат Сава Кезић је у свом мастер раду имплементирао сигурну заједничку обраду података у облаку коришћењем Амазон нитро енклава коришћењем помоћног Амазоновог сервиса за чување криптографских кључева, утврдио ниво безбедности података у оквиру овог процеса, предложио модификацију конкретне имплементације и коришћење других *TEE* решења осталих пружаоца услуга у облаку у циљу подизања нивоа информационе безбедности података. Кандидат је исказао самосталност и систематичност у свом поступку као и иновативне елементе у решавању проблематике овог рада..

На основу горе наведеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Саве Кезића под насловом „Имплементација сигурне заједничке обраде података у облаку коришћењем сигурних процесорских енклава“ прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 10.09.2021. године

Чланови комисије:

Др Павле Вулетић, ванредни професор

Др Жарко Станисављевић, ванредни професор