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 16.05.2023. године именовало нас је у Комисију за преглед и оцену мастер рада дипл. инж. Данијела Чамџића под насловом „Сигурно дистрибуирано складиштење и опоравак лозинки на *MQTT* повезаним *IoT* чворовима“. Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Данијел Чамџић је рођен 03.08.1997. године у Котору у Црној Гори. Завршио је основну школу „Орјенски батаљон” у Бијелој као носилац дипломе "Луча". Уписао је Средњу Поморску школу у Котору и завршио са одличним успехом.

Електротехнички факултет у Београду уписао је 2016. године. Дипломирао је на модулу за Електронику 2020. године са просечном оценом 8.63. Дипломски рад одбранио је у септембру 2020. године са оценом 10.

Мастер академске студије на Електротехничком факултету у Београду, на Модулу за Електронику. уписао је у октобру 2021. године. Положио је све испите са просечном оценом 10.

2. Извештај о студијском истраживачком раду

Кандидат Данијел Чамџић је као припрему за израду мастер рада урадио истраживање релевантне литературе која се односи на област којој припада тема мастер рада. Конкретно, анализирана су постојећа решења и проблеми који постоје у тренутно доступним имплементацијама система за складиштење лозинки. Истраживањем области утврђено је да постоје решења која пружају флексибилне механизме за складиштење и опоравак лозинки. Међутим, такође је уочено да та решења у одређеној мери не поштују приватност корисника и да постоје могућности за додатна унапређења и реализације система, у виду интеграције флексибилнијих јединица за складиштење података као и употребу криптографских алгоритама у сврху локализоване и дистрибуиране заштите података, што је и искоришћено у изради мастер рада.

3. Опис мастер рада

Мастер рад обухвата 81 страну, са укупно 25 слика, 1 табелу и 18 референци. Рад садржи резиме, посвету, увод, 5 поглавља и закључак (укупно 7 поглавља), 4 додатка, списак слика, списак табела, списак скраћеница и списак коришћене литературе.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Представљен је систем за сигурно дистрибуирано складиштење и опоравак лозинки.

У другом поглављу анализирана су тренутно доступна решења за складиштење и опоравак лозинки, са фокусом на анализи улоге приватности у имплементацији тих решења. Изнети су аргументи за и против анализираних решења и представљене идеје које отклањају важне проблеме који су откривени.

У трећем поглављу представљен је теоријски увод у криптографске методе које се користе на слоју података у система. Анализирано је математичко извођење *RSA* алгоритма за енкрипцију као и Шамирове формуле тајног дељења. Представљене су предности и мане метода и дато објашњење у вези улоге представљених метода у систему.

У четвртом поглављу анализиран је *MQTT* протокол и његова улога на транспортном слоју система. Представљена је нова имплементација *MQTT* библиотеке за *MQTT 3.1.1* клијенте

који чине наменски уређаји система, написана у *C* програмском језику, користећи *FreeRTOS* библиотеку.

У петом поглављу описана је архитектура и дизајн система, са фокусом на интеграцију компонената који чине систем и њихову интеракцију са главним програмом.

У шестом поглављу представљени су најважнији резултати које систем реализује у реалним ситуацијама у којима се може наћи. Анализирано је понашање система у разним околностима и представљена је флексибилност која се огледа у способности система да правилно функционише и отклања проблеме. Такође су представљена потенцијална унапређења и значај система у другим областима.

Седмо поглавље је закључак у оквиру кога је описан значај истраживачког рада.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Данијела Чамџића се бави анализом и имплементацијом система за сигурно и дистрибуирано складиштење и опоравак лозинки уз употребу криптографских метода, *MQTT* протокола и софтверско/хардверских компоненти. У области *IoT* система и система за складиштење лозинки, овај истраживачки рад је од значаја јер представља ново решење које пружа додатне могућности за очување приватности корисника у виду очувања власништва над подацима који се складиште. Кроз интеграцију софтверско/хардверских компонената, њихову повезаност употребом *MQTT* протокола и криптографских метода, представљена је идеја и реализација система која пружа додатне предности у погледу отпорности на нападе, заштите поверљивих података и ефикасности у обнови тајних информација.

Основни доприноси рада су: 1) теоријска анализа и презентација новог система за складиштење и опоравак лозинки и других типова осетљивих информација; 2) разрада и демонстрација дистрибуиране методе чувања података са фокусом на сигурност и приватност корисника; 3) имплементација система заснованог на *master/slave* моделу у форми софтверско/хардверских чворова који користе *publish/subscribe* модел *MQTT* протокола; 4) употреба *RSA* методе енкрипције и Шамирове формуле тајног дијељења за осигурање података; 5) анализа и практична демонстрација робусности и сигурности система; 6) могућност наставка истраживања и даљег развоја система.

5. Закључак и предлог

Кандидат Данијел Чамџић је у свом мастер раду успешно решио проблем очувања приватности лозинки и других осетљивих информација присутан у многим централизованим решењима складиштења лозинки кроз имплементацију новог система за сигурно и дистрибуирано очување података. Представљени начин рада система пружа велике предности у погледу отпорности на нападе, заштите поверљивих података и ефикасности у обнови тајних информација. Предочене додатне модификације система у поглављу у ком су дискутовани резултати пружају увид у потенцијал приказаног система да се искористи као потпуно решење за складиштење информација чија је сржа да остану корисниково власништво.

Кандидат је исказао самосталност и систематичност у своме поступку као и иновативне елементе у решавању проблематике овог рада.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Данијела Чамџића прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 31. 08. 2023. године

Чланови комисије:

др Лазар Сарановац, редовни професор

др Иван Поповић, редовни професор