УНИВЕРЗИТЕТ У БАЊОЈ ЛУЦИ
ФАКУЛТЕТ: ЕЛЕКТРОТЕХНИЧКИ

Образац 2

ИЗВЈЕШТАЈ

о оцјени подобности студента, теме и ментора за израду докторске дисертације

1. ПОДАЦИ О КОМИСИЈИ

Орган који је именовао комисију:

НАУЧНО-НАСТАВНО ВИЈЕЋЕ ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА

(СЕНАТ УНИВЕРЗИТЕТА У БАЊОЈ ЛУЦИ)

Датум именовања комисије: **11.10.2024. године (24.10.2024. године)**

Број одлуке: **20/3.709-7/24 (02/04-3.2250-77/24)**

Чланови комисије:

	Презиме и име	Звање	Научно поље и ужа научна област
1.	**др ДРАЖЕН БРЂАНИН**	ванредни професор	Електротехника, електроника, информационо инжењерство, рачунарске и информационе науке / Рачунарске науке
	Установа у којој је запослен-а		Функција у комисији
	Електротехнички факултет Универзитет у Бањој Луци		предсједник
2.	**др БОШКО НИКОЛИЋ**	редовни професор	Електротехника и рачунарство / Рачунарска техника и информатика
	Установа у којој је запослен-а		Функција у комисији
	Електротехнички факултет Универзитет у Београду		члан
3.	**др МИЛОШ ЦВЕТАНОВИЋ**	ванредни професор	Електротехника и рачунарство / Рачунарска техника и информатика
	Установа у којој је запослен-а		Функција у комисији
	Електротехнички факултет Универзитет у Београду		члан

2. ПОДАЦИ О СТУДЕНТУ

Име, име једног родитеља, презиме: **ДИЈАНА, Рајко, ВУКОВИЋ ГРБИЋ**

Датум рођења: **8.10.1984.**

Мјесто и држава рођења: **Приједор, Босна и Херцеговина**

2.1. Студије првог циклуса или основне студије или интегрисане студије

Година уписа:	**2003.**	Година завршетка:	**2007.**	Просјечна оцјена током студија:	**8.55**

Универзитет: **УНИВЕРЗИТЕТ У БАЊОЈ ЛУЦИ**

Факултет/и: **ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ**

Студијски програм: **Рачунарство и информатика–Софтверско инжењерство**

Стечено звање: **Дипломирани инжењер електротехнике**

2.2. Студије другог циклуса или мастер студије

Година уписа:	**2009.**	Година завршетка:	**2011.**	Просјечна оцјена током студија:	**9.83**

Универзитет: **УНИВЕРЗИТЕТ У БАЊОЈ ЛУЦИ**

Факултет/и: **ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ**

Студијски програм: **Рачунарство и информатика–Информационо-комуникационе технологије**

Назив завршног рада другог циклуса или мастер тезе, датум одбране:

Нови алат за окривање сигурносних пропуста Web апликација статичком анализом изворног кода

Датум одбране: **17.5.2011.**

Ужа научна област завршног рада другог циклуса или мастер тезе: **Рачунарске науке**

Стечено звање: **Магистар рачунарства и информатике**

2.3. Студије трећег циклуса

Година уписа:	**2012.**	Број ECTS остварених до сада:	**60**	Просјечна оцјена током студија:	**10.00**

Факултет/и: **ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ УНИВЕРЗИТЕТА У БАЊОЈ ЛУЦИ**

Студијски програм: **Информационо-комуникационе технологије**

2.4. Приказ научних и стручних радова студента

РБ	Подаци о референци	Категорија[1]

[1] Категорија се односи на оне часописе и научне скупове који су категорисани у складу са Правилником о публиковању научних публикација („Службени гласник РС”, бр. 77/17) и Правилником о мјерилима за остваривање и финансирање Програма одржавања научних скупова („Службени гласник РС”, бр. 102/14) односно припадност рада часописима индексираним у свјетским цитатним базама.

1.	**D. Vukovic Grbic**, Z. Djuric, A. Kelec: Enhancing Security and Privacy in Modern Text-Based Instant Messaging Communications, *Advances in Electrical and Computer Engineering*, Vol. 24, No. 2, pp. 49-60, 2024, doi:10.4316/AECE.2024.02006	Истакнути научни часопис међународног значаја (JCR IF: 0.7)

Кратак опис садржаја (до 150 ријечи):

Модерно друштво све више користи апликације за размјену инстант порука (*IM*), али обезбјеђивање сигурности и приватности остаје кључно. Многи постојећи протоколи користе енкрипцију, али она је често мета масовног надзора. У овом раду предложен је *StegaCloak*, нови протокол који комбинује криптографију и стеганографију, побољшавајући сигурност и приватност у *IM* комуникацији. Преложени протокол скрива стварну комуникацију унутар обичних *chat* порука, чиме рјешава слабости других сличних протокола, као што је детектабилност. Протокол је описан дијаграмом тока порука и формалном нотацијом. Упоређен је са два постојећа *IM* протокола (*OTR* и *Signal*), а његова сигурност верификована је *AVISPA* алатом.

РБ	Подаци о референци	Категорија
2.	**D. Vuković Grbić**, I. Dujlović, Social engineering with ChatGPT, *22nd International Symposium INFOTEH-JAHORINA (INFOTEH)*, 2023, doi: 10.1109/INFOTEH57020.2023.10094141	Научни скуп међународног значаја

Кратак опис садржаја (до 150 ријечи):

Врло брзо након јавног представљања, *ChatGPT* је показао добре резултате у генерисању одговора на упите у различитим областима, у генерисању кода и припреми текстуалних шаблона, па чак и комплетних текстова на одређене теме. Комбинујући те могућности, уз добру припремљеност система, могуће је добити све што је потребно за креирање *phishing* или неког другог напада само у неколико кликова за свега неколико минута. У овом раду приказана је могућност коришћења *ChatGPT* за припрему окружења за извршавање *phishing* напада базираних на социјалном инжењерингу, као и могућности за њихову превенцију.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
3.	**D. Vuković**, A. Keleč: Problem privatnosti na Android mobilnim uređajima, *INFO M*, Vol. 15, No. 57, pp. 28-35, 2016.	Научни часопис националног значаја

Кратак опис садржаја (до 150 ријечи):

Људи користе апликације на паметним телефонима у свакодневном животу за различите сврхе, као што су: фотографисање и објављивање фотографија на мрежи, слање електронске поште, скенирање *QR* кодова, размјену инстант порука итд. Ово је само подскуп могућности које пружају данас доступне апликације. Инсталирање апликација обично подразумијева давање одређених привилегија апликацији, као што су приступ интернету, камери и сл. Привилегије могу довести до проблема који се односе на приватност корисника. У овом раду дискутована је сигурност *Android* оперативног система и дат примјер искоришћавања слабости система кроз камера-базирани напад којим се нарушава приватност корисника. Дат је преглед побољшања везаних за приватност корисника, које је донијела *Marshmallow* верзија *Android* оперативног система и предложено једно рјешење проблема приватности.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
4.	**D. Vuković**, I. Dujlović: Facebook Messenger Bots and Their Application for Business, *24th Telecommunications Forum (TELFOR)*, 2016, doi: 10.1109/TELFOR.2016.7818926	Научни скуп међународног значаја

Кратак опис садржаја (до 150 ријечи):

Након представљања ботова за *Facebook Messenger*, априла 2016. године, њихова примјена постала је много шира. Ботови се користе за једноставне задатке, као што су приказ временске прогнозе или забава, али се све више истражује њихова примјена у пословне сврхе. Иако није уобичајено, ботови могу бити веома корисни у пословању, као замјена за информативне шалтере, попут оних у банкама. Клијентима се може омогућити једноставно информисање о кредитима, отварању рачуна и другим банкарским услугама, чиме се смањује чекање у редовима и повећава задовољство клијената. У овом раду истражени су *Facebook Messenger* ботови, њихове примјене, развој и имплементација. Као пословни случај, имплементиран је банкарски бот под називом *PseudoBank*, уз приказ предности и недостатака таквих апликација у пословању.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
5.	A. Kelec, **D. Vukovic**: Privacy threats on Android devices – Big Brother is Watching you, *23rd Telecommunications forum (TELFOR)*, pp. 926-929, 2015, doi: 10.1109/TELFOR.2015.7377617	Научни скуп међународног значаја

Кратак опис садржаја (до 150 ријечи):

Кориштење апликација за паметне телефоне у различитим аспектима људског живота постало је уобичајено за све кориснике мобилних телефона. Снимање фотографија и њихово објављивање на мрежи, слање електронске поште и скенирање *QR* кодова само су мали подскуп могућности за ове врсте апликација, које су доступне у одређеној продавници апликација на мрежи. Када неко жели да инсталира одређену апликацију на свој телефон, треба да додијели привилегије апликацији, као што су: приступ интернету, приступ камери итд. Додјељивање привилегија може довести до проблема приватности, који утиче на корисника, нпр. давањем привилегија приступа камери могуће је претворити телефон корисника у алат за видео надзор. У овом раду приказани су резултати истраживања о сигурности *Android* оперативног система и дат примјер искоришћавања његових слабости за нарушавање приватности корисника.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
6.	**D. Vukovic**, D. Gligoroski, Z. Djuric: CryptoCloak protocol and the prototype application, *IEEE Conference on Communications and Network Security (CNS)*, pp. 721-722, 2015, doi: 10.1109/CNS.2015	Научни скуп међународног значаја

Кратак опис садржаја (до 150 ријечи):

Број апликација за размјену *chat* порука расте из дана у дан, не само у свакодневној комуникацији обичних људи, него и у пословној кореспонденцији. Посљедично, сигурност и приватност оваквих апликација врло су важни и не би смјели бити нарушени. У овом раду описан је *CryptoCloak* протокол за сигурну и приватну *chat* комуникацију, заједно са прототипом апликације која је имплементирана у програмском језику *Java*.

РБ	Подаци о референци	Категорија
7.	**D. Vuković**: Security issues in Internet of Things (IoT) related to passive RFID tags, *Facta Universitatis – Series: Automatic control and robotics*, Vol. 13, No. 2, pp. 97-105, 2014.	Научни часопис националног значаја

Кратак опис садржаја (до 150 ријечи):

Интернет ствари (*IoT*) биће једна од водећих технологија у трансформацији данашњег интернета у интернет будућности. *IoT* укључује паметне објекте, комуникацију машина-машина, радио-фреквентне технологије итд. Један од главних захтјева за *IoT* јесте да објекти морају имати јединствени идентитет, који се користи за идентификацију уређаја при размјени информација. Да би се то постигло, могу се користити *RFID* тагови, који могу бити: активни, полупасивни и пасивни. С обзиром на њихове основне карактеристике, пасивни тагови су најпогоднији за коришћење у *IoT*-у. Коришћење пасивних *RFID* тагова носи одређене безбједносне ризике. У овом раду анализирани су потенцијални проблеми примјене пасивних *RFID* тагова и могућности за њихово елиминисање.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
8.	**D. Vuković**: CryptoCloak as a Protection Against Internet Surveillance, *INFOTEH 2014*, pp. 909-912, 2014.	Научни скуп са међународним учешћем

Кратак опис садржаја (до 150 ријечи):

CryptoCloak је пројекат отвореног кода који користи познате криптографске алгоритме за размјену кључева и криптовање саобраћаја, али се криптовање обавља на тајан начин. Полазећи од навода о нарушавању приватности на интернету, циљ пројекта је смањење могућности успјешног коришћења аутоматских алата за анализу саобраћаја свакоме ко има приступ серверима за *chat*. Под успјешним коришћењем сматра се детекција потенцијално сумњивог саобраћаја. Анализом комуникације, која се обавља кроз *CryptoCloak*, биће примијећен само обичан *chat*, док су праве криптоване информације уграђене у њега. Обичан *chat* је скривач (енг. *cloak*) за криптоване информације у комуникацији између два *CryptoCloak* клијента. У имплементацији *CryptoCloak* протокола користи се *Skype API* за *Java* програмски језик.

РБ	Подаци о референци	Категорија
9.	**D. Vuković**, D. Gligoroski, Z. Đurić: On Privacy Protection in the Internet Surveillance Era, *11th International Conference on Security and Cryptography (SECRYPT)*, pp. 261-266, 2014.	Научни скуп међународног значаја

Кратак опис садржаја (до 150 ријечи):

У овом раду представљен је протокол за заштиту приватности у *chat* комуникацији, под називом *CryptoCloak*. Криптована комуникација је маскирана динамички генерисаним обичним разговором. Оваква комуникација није од интереса алатима за масовни надзор. За имплементацију *CryptoCloak* протокола користи се *Facebook Messenger API*, а *Diffie-Hellman* размјена кључева се врши тајно – умјесто слања униформног низа бројева, шаљу се реченице. Приказана верзија пружа механизам криптовања/декриптовања *chat* комуникације коришћењем симетричног алгоритма *AES* у *CBC* моду.

РБ	Подаци о референци	Категорија
10.	**D. Vuković**, D. Gligoroski, Z. Đurić: Improvement proposal for the CryptoCloak application, *NordSec 2014. Lecture Notes in Computer Science*, Vol. 8788, pp. 283-284, 2014, doi: 10.1007/978-3-319-11599-3.	Научни скуп међународног значаја

Кратак опис садржаја (до 150 ријечи):

Бројне организације широм свијета улажу велике напоре у развој апликација отпорних на прислушкивање. *CryptoCloak* је апликација за *chat* комуникацију, са посебним фокусом на заштиту приватности крајњег корисника. Криптована комуникација је маскирана динамички генерисаним обичним разговором, при чему се размјена кључева *Diffie-Hellman* врши на тајан начин – умјесто слања униформног низа бројева, шаљу се реченице. У овом раду дат је један приједлог за унапређење *CryptoCloak* апликације.

РБ	Подаци о референци	Категорија
11.	O. Joldžić, Z. Đurić, **D. Vuković**: Experiences and Challenges in Implementing Adaptive Bitrate Multimedia Streaming for Live Multimedia Content, *22nd Telecommunications forum (TELFOR),* pp. 909-912, 2014, doi: 10.1109/TELFOR.2014.7034552	Научни скуп међународног значаја

Кратак опис садржаја (до 150 ријечи):

Процес мрежне конвергенције и повећана доступност мрежа велике брзине отворили су низ могућности у области дистрибуције мултимедијалних садржаја. Првенствено, популарност мобилних платформи и праћена мобилност корисника захтијева платформе које могу одговорити на промјену услова мреже и одржавати задовољавајући квалитет услуге без обзира на могућности клијентског уређаја. Овај рад разматра искуства и изазове у имплементацији *adaptive bitrate* (*ABR*) платформе за пренос мултимедије код емитовања садржаја уживо. У раду су описане уобичајене технике и протоколи који се користе за *live streaming*, заједно са основним принципима *adaptive bitrate* на основу доступних пропусних опсега. Као доказ концепта, имплементиран је дигитални мултимедијални дистрибутивни систем под називом *GSTV*.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
12.	**D. Vuković**, Z. Đurić, D. Gligoroski: CryptoCloak - improvement proposal implementation, *22nd Telecommunications forum (TELFOR)*, pp. 1067-1070, 2014, doi: 10.1109/TELFOR.2014.7034591.	Научни скуп међународног значаја

Кратак опис садржаја (до 150 ријечи):

У пост-Сноуденовом раздобљу улаже се велики напор у развој апликација које пружају заштиту приватности у интернет комуникацијама. Сигурне *chat* апликације, системи за анонимно прегледање, стеганографске апликације и слични производи постали су потреба и користе се у свакодневном животу. *CryptoCloak* је апликација за сигуран *chat*, развијена у програмском језику *Java*. У овом раду представљен је *CryptoCloak* и приказано његово побољшање у контексту смањења временског преоптерећења претходне верзије апликације.

РБ	Подаци о референци	Категорија
13.	**D. Vuković**: Security Issues of Passive RFID Tags Used in Internet of Things (IoT), *XII International SAUM Conference*, 2014.	Научни скуп међународног значаја

Кратак опис садржаја (до 150 ријечи):

Парадигма Интернета ствари (*IoT*) биће једна од водећих технологија у трансформацији од данашњег интернета ка будућем интернету. *IoT* укључује паметне објекте, комуникацију машина-машина, *RF* технологију итд. За омогућавање комуникације између уређаја у *IoT*-у, потребна је јединствена идентификација сваког објекта, што се постиже коришћењем *AutoID* технологије (нпр. *RFID* тагови). Пасивни *RFID* тагови су најприкладнији за *IoT*, али њихова употреба носи одређене сигурносне ризике. У овом раду, коришћењем *STRIDE threat* модела, описани су потенцијални проблеми пасивних RFID тагова и дате смјернице за њихову елиминацију.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
14.	O. Joldžić, Z. Đurić, **D. Vuković**: Building a transparent intrusion detection and prevention system on SDN, *NIK-2014*, 2014.	Међународни научни скуп

Кратак опис садржаја (до 150 ријечи):

Мрежна конвергенција, мобилност корисника и разне врсте апликација доприносе нехомогености савремених мрежа. Појава нових технологија повећава број могућих сигурносних пријетњи свим дијеловима мрежне инфраструктуре. Због тога, мрежни сигурносни протоколи и механизми морају бити у стању да одговоре на било коју сигурносну пријетњу, без утицаја на перформансе мреже или деградацију квалитета услуге. У овом раду представљен је концепт ране фазе транспарентне превенције упада у систем (*TIPS*), имплементиран комбиновањем различитих технологија, прије свега софтверски дефинисаног умрежавања (*SDN*) и *poll-mode* процесирања пакета, што омогућава дубоку инспекцију пакета у мрежама велике брзине.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
15.	**D. Vuković**, Z. Đurić, D. Gligoroski: CryptoCloak application - main idea, an overview and improvement proposal, *NIK-2014*, 2014.	Међународни научни скуп

Кратак опис садржаја (до 150 ријечи):

У пост-Сноуденовом раздобљу улаже се велики напор у развој апликација отпорних на прислушкивање. "Надзор" и "приватност" постали су термини који се све чешће користе, како у неформалним разговорима, тако и у истраживачкој заједници. Почела је трка у развоју апликација које нуде различите врсте заштите приватности за просјечне кориснике: анонимно претраживање интернета, тајни разговори, енкрипција електронске поште итд. *CryptoCloak* је апликација за *chat* са заштићеном приватношћу комуникације. Криптована комуникација је маскирана динамички генерисаним обичним разговором. У овом раду представљен је *CryptoCloak* алат и дат један приједлог за његово унапређење, јер се *Diffie-Hellman* размјена кључева врши на начин који производи огромне трошкове – умјесто слања униформних бројева, шаљу се реченице.

РБ	Подаци о референци	Категорија
16.	O. Joldžić, **D. Vuković**: The impact of cluster characteristics on HiveQL query optimization, *21st Telecommunications Forum (TELFOR)*, pp. 837-840, 2013, doi: 10.1109/TELFOR.2013.6716360.	Научни скуп међународног значаја

Кратак опис садржаја (до 150 ријечи):

Различите врсте апликација складиште огромну количину података које касније користе и анализирају на одређене начине. Релационе базе података су се деценијама користиле као складишта података, али у неким случајевима нису прикладне за обраду великих колекција података. За рјешавање овог проблема, развијене су нерелационе базе података. Као помоћ за пренос података из релационих база података у нерелационе, развијени су адекватни алати. У овом раду, представљен је алат под називом *Sqoop*. Оптимизацијом упита треба да се баве све апликације које раде са великим количинама података, без обзира на њихову област примјене и обим. У овом раду анализиран је утицај карактеристика кластера на *HiveQL* оптимизацију упита.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
17.	**D. Vuković**: Using polyglot persistence to keep sensitive data protected, *INFOFEST 2013*, pp. 130-134, 2013.	Научни скуп са међународним учешћем

Кратак опис садржаја (до 150 ријечи):

Релационе базе података користе се деценијама за складиштење различитих врста података. Како количина података расте (проблем *Big Data*), све их је теже обрадити извршавањем упита над релационим базама података. За рјешавање ових проблема развијене су *NoSQL* базе података. Обје врсте база имају своје предности и недостатке, а обично су прикладне за различите примјене. Један од најважнијих аспеката складиштења података јесте заштита осјетљивих података. Према *OWASP TOP 10* пројекту, многе апликације, које користе релационе базе података, рањиве су на *SQL Injection* нападе. Добро је позната чињеница да већини *NoSQL* база недостају сигурносни механизми. Са сигурносног аспекта, обје врсте база имају проблема. Комбинујући ове двије базе, постоји већа могућност да осјетљиви подаци буду заштићени. Овај концепт познат је као *polyglot persistence* и представљен је у овом раду.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
18.	**D. Vuković**, Z. Đurić, D. Gligoroski: Proposal for expansion of STASEC tool, *20th Telecommunications Forum (TELFOR)*, pp. 1705-1708, 2012, doi: 10.1109/TELFOR.2012.6419555.	Научни скуп међународног значаја

Кратак опис садржаја (до 150 ријечи):

Један од приоритета у развоју веб апликација јесте имплементација сигурносних механизама. Да би се детектовали потенцијални сигурносни пропусти и имплементирали одговарајући сигурносни механизми, потребно је извршити детаљну анализу сигурносних аспеката апликације. За детекцију потенцијалних пропуста користи се статичка анализа изворног кода, односно алати који аутоматизују овај процес. *STASEC* је алат за статичку анализу изворног кода веб апликација имплементираних у програмском језику *Java*. У раду је дат приједлог проширења алата модулом за аутоматску детекцију рањивости апликација изазваних манипулацијом улазних података са клијентске стране кроз *Java* сервлете и *JSP* (*Java Server Pages*).

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
19.	**D. Vuković**, O. Joldžić: Static and dynamic analysis – usage in web application vulnerability detection, *ICIST 2011*, pp. 83-87, 2011.	Научни скуп међународног значаја

Кратак опис садржаја (до 150 ријечи):

Овај рад даје преглед основних принципа статичке и динамичке анализе веб апликација у циљу откривања њихове рањивости. У раду је описана типична употреба сваке технике, заједно са посебним условима због којих би се одређена техника сматрала непримјенљивом. Коначно, како би се илустровао процес откривања пријетњи, дат је примјер у којем се примјењују обје методе описане у раду.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
20.	**D. Vuković**, Z. Đurić: STASEC – alat za otkrivanje sigurnosnih propusta web aplikacija statičkom analizom Java izvornog koda, *INFO M*, Vol. 10, No. 39, pp. 26-37, 2011.	Научни часопис националног значаја

Кратак опис садржаја (до 150 ријечи):

Сигурност представља један од најбитнијих аспеката у развоју веб апликација. Све више веб апликација манипулише осјетљивим подацима, због чега је неопходно обезбиједити њихову адекватну заштиту од напада. Откривање сигурносних пропуста могуће је кроз статичку и динамичку анализу. Статичка анализа подразумијева тестирање кода без покретања апликације. Чести узроци рањивости су неадекватна валидација података и комплексност кода. Статичком анализом могу се открити сигурносни пропусти и припремити услови за њихово отклањање. Алати за статичку анализу могу бити комерцијални или отвореног кода. У овом раду представљен је *STASEC*, алат за откривање сигурносних пропуста статичком анализом *Java* кода. Карактеристике овог алата укључују висок проценат детекције пропуста и могућност проширења модулом за друге програмске језике.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
21.	Z. Đurić, **D. Vuković**: STASEC – alat za otkrivanje sigurnosnih propusta statičkom analizom Java izvornog koda, *Infoteh-Jahorina*, Vol. 9, pp. 491-495, 2010.	Научни скуп са међународним учешћем

Кратак опис садржаја (до 150 ријечи):

У овом раду анализиран је проблем сигурности веб апликација и указано на различите врсте напада на веб апликације. Као најзначајније врсте напада на веб апликације, детаљно су анализирани *SQL Injection* и *XSS* (*Cross-site scripting*). Описана је и техника детекције рањивости веб апликације статичком анализом њеног изворног кода. У раду је представљен *STASEC* алат, који омогућава откривање сигурносних пропуста статичком анализом *Java* изворног кода.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
22.	**D. Vuković**, Z. Đurić: Statička analiza izvornog koda i njena primjena u ocjeni kompleksnosti koda, *INFOFEST 2010*, pp. 249-256, 2010.	Научни скуп са међународним учешћем

Кратак опис садржаја (до 150 ријечи):

Веома важан аспект развоја софтвера, посебно пословних информационих система, јесте сигурност. Комплексност изворног кода директно утиче на поузданост и сигурност софтвера. Комплексност се може мјерити различитим метрикама, као што су број линија кода и цикломатска комплексност. Ове метрике развијене су за оцјењивање сложености процедуралних програма, али се користе и за објектно-оријентисане програме. Да би се метрике ефикасно примјењивале, потребна је аутоматизација. Оцјена комплексности може се вршити у било којем дијелу животног циклуса софтвера, а најбоље је прије пуштања у рад. Статичка анализа изворног кода, која се врши прије покретања софтвера, представља добар приступ за аутоматско оцјењивање комплексности. У овом раду предложен је алат за статичку анализу изворног кода који врши оцјењивање његове комплексности.

Рад није у директној вези са предложеном темом докторске дисертације.

РБ	Подаци о референци	Категорија
23.	Z. Đurić, **D. Vuković**: Implementacija SSO na bazi open source rješenja, *17. Telekomunikacioni forum TELFOR 2009*, pp. 1233-1236, 2009.	Научни скуп са међународним учешћем

Кратак опис садржаја (до 150 ријечи):

У овом раду дат је примјер централизованог система за аутентикацију који обезбјеђује *SSO* (*Single Sign-On*) функционалност. Систем је базиран на *open source CAS* (*Central Authentication Service*) серверу. Указано је на неке добре и лоше особине *SSO* рјешења и дат је опис рада *CAS* сервера на конкретном примјеру. У раду је описана имплементација *CAS* сервера у тестном окружењу са више веб апликација. Разматрани су и начини имплементације модула за аутентикацију и дати су примјери имплементације у тестном окружењу. Посебно су разматрани проблеми који се јављају при прилагођавању постојећих апликација за коришћење *CAS* сервера, али и других *SSO* рјешења.

Рад није у директној вези са предложеном темом докторске дисертације.

Оцјена релевантности научне и стручне активности кандидата за предложену тему дисертације:

Студент је (ко)аутор 23 научна рада, од којих је: један рад објављен у истакнутом научном часопису међународног значаја, два рада објављена у научним часописима националног значаја и 20 радова објављених у зборницима радова научних скупова међународног значаја или научних скупова са међународним учешћем.

Сви објављени радови баве се различитим сигурносним аспектима софтверских система, а седам радова је у директној вези са предложеном темом докторске дисертације, међу којима је и један рад објављен у истакнутом научном часопису међународног значаја.

Да ли студент испуњава прописане услове?	**ДА**	НЕ

3. ПОДАЦИ О МЕНТОРУ

Име и презиме: **др ЗОРАН ЂУРИЋ**

Академско звање: **Редовни професор**

Научно поље и ужа научна област:

Електротехника, електроника, информационо инжењерство, рачунарске и информационе науке / Рачунарске науке

Матична институција стицања избора у звање: **УНИВЕРЗИТЕТ У БАЊОЈ ЛУЦИ**

Биографија (до 300 ријечи):

Др Зоран Ђурић је редовни професор на Електротехничком факултету Универзитета у Бањој Луци. Декан је Електротехничког факултета, руководилац Катедре за рачунарство и информатику, те члан Сената Универзитета у Бањој Луци.

Основне студије завршио је 2001. године, магистрирао је 2004. године, а докторску дисертацију одбранио је 2008. године. Његова главна подручја интересовања су сигурност рачунарских система, PKI системи, криптографија, платни системи и протоколи, развој софтвера, машинско учење, *big data* и вјештачка интелигенција.

Проф. Ђурић учествовао је у више од 200 међународних и националних пројеката (TEMPUS, HERD, пројекти подржани од стране WUS Austria, USAID, SIDA и пројекти Свјетске банке). Учествовао је у пројектовању и развоју већег броја софтверских рјешења и рјешења у области сигурности рачунарских система за потребе различитих домаћих и страних компанија и институција. Објавио је 70 научних радова у часописима и конференцијама. Аутор је три књиге. Рецензент је за неколико међународних часописа и конференција, укључујући *IEEE Internet Computing*, *The Computer Journal* и *Information Technology and Control*. Проф. Ђурић је члан IEEE.

Радови из области којој припада приједлог теме докторске дисертације:

РБ	Навести појединачно радове, књиге, поглавља. Додати потребан број редова. Користити исти стил за навођење свих референци.	Категорија
1.	D. Vukovic Grbic, **Z. Djuric**, A. Kelec: Enhancing Security and Privacy in Modern Text-Based Instant Messaging Communications, *Advances in Electrical and Computer Engineering*, vol. 24, no. 2, pp. 49-60, 2024, doi:10.4316/AECE.2024.02006.	Истакнути научни часопис међународног значаја (IF 2024: 0.700)
2.	B. Malčić, **Z. Đurić**, S. Šajić: Implementacija steganografije i kriptografskih algoritama u MATLAB-u, *Info M*, no. 77, pp. 4-17, 2023.	Научни часопис националног значаја
3.	A. Bojanić, **Z. Đurić**: Uporedna analiza metoda za kategorizaciju teksta, *Info M*, no. 73, pp. 4-11, 2021.	Научни часопис националног значаја
4.	J. Jokić, **Z. Đurić**: Detekcija malicioznih URL-ova korištenjem metoda mašinskog učenja, *Info M*, no. 71, pp. 28-37, 2020.	Научни часопис националног значаја
5.	A. Kelec, **Z. Djuric**: A Proposal for Addressing Security Issues Related to Dynamic Code Loading on Android Platform, *Computer Systems Science and Engineering*, vol. 35, no. 4, pp. 271-282, 2020, doi: 10.32604/csse.2020.35.271.	Научни часопис међународног значаја

6.	D. Šušak, **Z. Đurić**: Analiza Apache Hadoop-a i mogućnosti upotrebe, *Info M*, no. 70, pp. 11-19, 2020.	Научни часопис националног значаја
7.	L. Antonijević, **Z. Đurić**: Razvoj sistema za automatsko uspostavljanje okruženja za izvršavanje web aplikacija, *Info M*, no. 70, pp. 46-53, 2019.	Научни часопис националног значаја
8.	**З. Ђурић**: *Мрежно и дистрибуирано програмирање*, Универзитет у Бањој Луци, Електротехнички факултет, ISBN 978-99955-46-38-0, 2019.	Универзитетски уџбеник
9.	**З. Ђурић**: *Програмски језик Јава*, Универзитет у Бањој Луци, Електротехнички факултет, ISBN 978-99955-46-36-6, 2019.	Универзитетски уџбеник
10.	М. Шербић, **З. Ђурић**: Имплементација интерних DSL-ова на JVM платформи, *Info M*, број. 68, стр. 17-28, 2018.	Научни часопис националног значаја
11.	O. Joldzic, **Z. Djuric**, P. Vuletic: A transparent and scalable anomaly-based DoS detection method, *Computer Networks*, vol. 104, pp. 27-42, 2016, doi: 10.1016/j.comnet.2016.05.004.	Истакнути научни часопис међународног значаја (IF 2016: 2.516)
12.	D. Vukovic, D. Gligoroski, **Z. Djuric**: CryptoCloak protocol and the prototype application, *IEEE Conference on Communications and Network Security (CNS)*, pp. 721-722, 2015, doi: 10.1109/CNS.2015.	Научни скуп међународног значаја
13.	**Z. Đurić**, D. Gašević: FEIPS - a Secure Fair-Exchange Payment System for Internet Transactions, *The Computer Journal*, vol. 58, no. 10, pp. 2537-2556, 2015, doi: 10.1093/comjnl/bxu120.	Истакнути научни часопис међународног значаја (IF 2015: 1.000)
14.	O. Joldžić, **Z. Đurić**, D. Vuković: Building a transparent intrusion detection and prevention system on SDN, *NIK-2014*, 2014.	Научни скуп међународног значаја
15.	D. Vuković, **Z. Đurić**, D. Gligoroski: CryptoCloak application - main idea, an overview and improvement proposal, *NIK-2014*, 2014.	Научни скуп међународног значаја
16.	D. Vuković, **Z. Đurić**, D. Gligoroski: CryptoCloak - improvement proposal implementation, *22nd Telecommunications forum (TELFOR)*, pp. 1067-1070, 2014, doi: 10.1109/TELFOR.2014.7034591.	Научни скуп међународног значаја
17.	D. Vuković, D. Gligoroski, **Z. Đurić**: Improvement proposal for the CryptoCloak application, *NordSec 2014. Lecture Notes in Computer Science*, Vol. 8788, pp. 283-284, 2014, doi: 10.1007/978-3-319-11599-3.	Научни скуп међународног значаја
18.	D. Vuković, D. Gligoroski, **Z. Đurić**: On Privacy Protection in the Internet Surveillance Era, *11th International Conference on Security and Cryptography (SECRYPT)*, pp. 261-266, 2014.	Научни скуп међународног значаја

19.	O. Joldzic, **Z. Djuric**: Video Streaming Protocol Extension for Session Control and Authorization, *IEEE International Conference on Systems, Signals and Image Processing - IWSSIP*, pp. 135-138, 2014.	Научни скуп међународног значаја
20.	**Z. Djuric**, O. Joldzic: GSTV: An Integrated, Adaptive and Scalable Digital Multimedia Content Distribution System, *Journal of Automation and Control Engineering*, vol. 2, no. 4, pp. 381-387, 2014, doi: 10.12720/joace.2.4.381-387.	Научни часопис међународног значаја
21.	**Z. Djuric**: WAPTT - Web Application Penetration Testing Tool, *Advances in Electrical and Computer Engineering,* vol. 14, no. 1, pp. 93-102, 2014, doi: 10.4316/AECE.2014.01015.	Истакнути научни часопис међународног значаја (IF 2014: 0.529)
22.	**Z. Djuric**: A black-box testing tool for detecting SQL injection vulnerabilities, *2nd International Conference on Informatics & Applications*, pp. 216-221, 2013, doi: 10.1109/ICoIA.2013.6650259.	Научни скуп међународног значаја
23.	O. Joldžić, **Z. Đurić**: Security Issues of Restful Web Services and the Possibilities of Automatic Security Vulnerability Detection, *INFOFEST 2013*, pp. 145-153, 2013.	Научни скуп са међународним учешћем
24.	D. Zoran, **Z. Đurić**: Mrežna komunikacija na Android platformi i mehanizmi njene zaštite, *INFOFEST 2013*, pp. 171-180, 2013.	Научни скуп са међународним учешћем
25.	D. Zoran, **Z. Đurić**: Metode sigurnog prenosa podataka između mobilne aplikacije i udaljenog servera, *Info M*, no. 47, pp. 16-24, 2013.	Научни часопис националног значаја
26.	**Z. Đurić**, D. Gašević: A Source Code Similarity System for Plagiarism Detection, *The Computer Journal*, vol. 56, no. 1, pp. 70-86, 2013, doi: 10.1093/comjnl/bxs018.	Истакнути научни часопис међународног значаја (IF 2013: 0.888)
27.	D. Vuković, **Z. Đurić**, D. Gligoroski: Proposal for expansion of STASEC tool, *20th Telecommunications Forum (TELFOR)*, pp. 1705-1708, 2012, doi: 10.1109/TELFOR.2012.6419555.	Научни скуп међународног значаја
28.	D. Vuković, **Z. Đurić**: STASEC – alat za otkrivanje sigurnosnih propusta web aplikacija statičkom analizom Java izvornog koda, *Info M*, no. 39, pp. 26-37, 2011.	Научни часопис националног значаја
29.	**Z. Đurić**, O. Joldžić: Pregled specifikacija i tehnika zaštite servisno-orijentisanih aplikacija, *Info M*, no. 37, pp. 16-24, 2011.	Научни часопис националног значаја
30.	S. Marić, **Z. Đurić**: Sigurnosni aspekti servisno orijentisanih arhitektura i najvažnije tehnike za kreiranje sigurnih servisno orijentisanih aplikacija, *INFOTEH-JAHORINA*, pp. 606-610, 2011.	Научни скуп са међународним учешћем
31.	O. Joldžić, **Z. Đurić**: Metrika za vrednovanje i klasifikaciju sigurnosnih propusta web aplikacija, *INFOFEST 2010*, pp. 163-171, 2010**.**	Научни скуп са међународним учешћем

32.	O. Joldžić, Z. Đurić: Prijedlog rješenja za detekciju i klasifikaciju sigurnosnih propusta web aplikacija, *Info M*, no. 34, pp. 42-52, 2010.	Научни часопис националног значаја
33.	**Z. Đurić**, D. Vuković: STASEC - alat za otkrivanje sigurnosnih propusta statičkom analizom Java izvornog koda, *INFOTEH-JAHORINA*, pp. 491-495, 2010.	Научни скуп са међународним учешћем
34.	O. Joldžić, **Z. Đurić**: Tipovi napada na web servise, *INFOTEH-JAHORINA*, pp. 482-486, 2010.	Научни скуп са међународним учешћем
35.	**Z. Đurić**, O. Joldžić: Sigurnost web aplikacija, *INFOFEST 2009*, pp. 204-212, 2009.	Научни скуп са међународним учешћем
36.	O. Joldžić, **Z. Đurić**: Mogućnosti testiranja sigurnosnih propusta u web aplikacijama sa prijedlogom rješenja sistema za testiranje, *INFOFEST 2009*, pp. 213-220, 2009.	Научни скуп са међународним учешћем
37.	**Z. Đurić**, O. Marić, D. Gašević: Internet Payment System: A New Payment System for Internet Transactions, *Journal of Universal Computer Science*, vol. 13, no. 4, pp. 479-503, 2007.	Истакнути научни часопис међународног значаја (IF 2007: 0.813)
38.	**Z. Djuric**: IPS – Secure Internet Payment System, *Int. Conf. on Information Technology: Coding and Computing – ITCC'05*, vol. I, pp. 425-430, 2005, doi: 10.1109/ITCC.2005.181.	Научни скуп међународног значаја
39.	**Z. Đurić**, S. Marić: Sigurnost web servisa, *INFOTEH-JAHORINA*, pp. 254-257, 2005.	Научни скуп са међународним учешћем

Да ли ментор испуњава прописане услове?	**ДА**	НЕ

4. ОЦЈЕНА ПОДОБНОСТИ ТЕМЕ

4.1. Формулација назива дисертације (наслова)

Развој протокола за сигурну и приватну комуникацију инстант порукама

Да ли је наслов тезе подобан?	**ДА**	НЕ

4.2. Научно поље и ужа научна област

Електротехника, електроника, информационо инжењерство, рачунарске и информационе науке / Рачунарске науке

Да ли су научно поље и ужа научна област исти као код ментора?	**ДА**	НЕ

4.3. Предмет истраживања

Савремено друштво значајно је промијенило начин комуникације, прелазећи са директне комуникације (*лице-у-лице*) на комуникацију инстант порукама (енг. *instant messaging – IM*), која је постала дио свакодневног живота у различитим областима и за различите сврхе. Развој *IM* протокола и апликација данас обликују сљедећи кључни правци: приватност и сигурност, интероперабилност, вјештачка интелигенција и аутоматизација, мултимедијална и проширена стварност, напредне функције за дијељење садржаја те фокус на колаборацију и продуктивност.

Највећи изазов у развоју *IM* апликација представља осигурање високог нивоа сигурности и приватности корисника. Постојећи протоколи потенцијално су сумњиви због употребе енкрипције и постају мета алата за надзор. Из тог разлога, фокус овог истраживања јесте изучавање протокола за *IM* комуникацију и техника за пројектовање и имплементацију, како би се идентификовали њихови недостаци и развио нови протокол који би отклонио недостатке и помогао унапређењу сигурне и приватне *IM* комуникације. Сигурност се односи на заштиту од различитих облика напада, злоупотребе или неовлаштеног приступа, што подразумијева обезбјеђивање тајности, интегритета, аутентикације и доступности података, као и заштиту од пресретања, измјена и других врста злонамјерних активности. Приватност се односи на заштиту података и идентитета учесника у комуникацији, како би се осигурало да само овлаштене стране имају приступ осјетљивим подацима и да треће стране не могу пратити или открити ко комуницира нити шта се комуницира. Приватност подразумијева заштиту не само података, већ и метаподатака, као што су *IP* адресе и обрасци комуникације. Приватност је повезана са механизмима као што су анонимност, котролисан приступ информацијама те заштита од надзора и масовног праћења.

Постоји већи број протокола који се користе у *IM* комуникацији, међу којима су најзначајнији *OTR* и *Signal*. *OTRv3*, чије су основне карактеристике: аутентикација, тајност, *Perfect Forward Secrecy* (*PFS*) и непорецивост, пружа снажну енкрипцију за *IM*. Аутентикација је процес провјере идентитета корисника или система како би се утврдило да ли су они заиста оно за шта се представљају и обично се спроводи кориштењем неког облика идентификације (нпр. сертификати у случају *TLS* протокола). Тајност се односи на заштиту података од неовлашћеног приступа, тако да само овлаштене стране могу читати или приступити осјетљивим подацима, што се постиже енкрипцијом података, чиме се осигурава да само власници исправних кључева могу декриптовати и разумјети податке. *PFS* је својство које осигурава да компромитовање дугорочних тајних кључева не угрожава сигурност претходно успостављених сесија, јер свака сесија користи привремене кључеве који нису везани за дугорочни кључ. Непорецивост је својство које омогућава да учесници не могу негирати своје учешће у одређеној комуникацији, односно способност да се докаже да је одређени ентитет заиста одговоран за одређену акцију, комуникацију или податак. Главни проблем са *OTRv3* јесте недостатак могућности непорецивости за учеснике у алгоритму потписивања, јер је потпис видљив објема странама током *handshake* фазе. Као одговор на овај проблем развијен је *OTRv4* који обезбјеђује *end-to-end* енкрипцију, различите типове непорецивости и јаче концепте *forward* и *post-compromise* тајности. *End-to-end* енкрипција осигурава да само крајњи учесници комуникације могу читати садржај размијењених порука или података. У овом моделу, подаци се енкриптују на страни пошиљаоца и декриптују тек на страни примаоца, чиме се онемогућава било којој трећој страни (провајдери услуга, посреднички сервери или потенцијални нападачи) да приступи садржају порука док су у преносу. *Signal* је *Ratcheting Forward Secrecy (RFS)* протокол који функционише и у синхроним и асинхроним окружењима. *RFS* техника се користи да би се обезбиједила додатна заштита комуникација. Ова техника проширује *PFS* концепт и комбинује га са *ratcheting* механизмом (често ажурирање кључева у току комуникације). Да би се осигурао висок ниво сигурности, *Signal* користи *forward secrecy* – сваки сесијски кључ је јединствен и не може се реконструисати на основу дугорочних кључева. Иако *Signal* пружа висок ниво сигурности садржаја порука, метаподаци нису довољно заштићени, што може бити искоришћено за праћење корисника чак и кад је садржај порука енкриптован. Поред чињенице да је *Signal* сигуран од појединачних напада, његов недостатак јесте то што није оптимизован за избјегавање масовног надзора па корисници могу и даље бити мета система за праћење великих размјера који се фокусирају на метаподатке и обрасце комуникације. Анализа показује да постоје недостаци у актуелним протоколима и потреба за развојем новог протокола у којем ће бити отклоњени ти недостаци и унапријеђена сигурност и приватност у *IM* комуникацији.

Ово истраживање даће одговоре на кључне проблеме у области сигурности и приватности у *IM* комуникацији елиинацијом недостака постојећих протокола иновативном интеграцијом криптографије и стеганографије, јер је додатну сигурност и приватност у комуникацији могуће обезбиједити комбинацијом криптографије и стеганографије. Криптографија се користи за енкриптовање порука како би се осигурало да само ауторизовани корисници могу читати њихов садржај. Ово осигурава да чак и ако неко пресретне поруку, неће бити у могућности да је разумије без кључа за декрипцију. Стеганографија је техника скривања података унутар носиоца поруке, гдје носиоци могу бити различите врсте докумената (нпр. слике, текстуални документи, аудио и видео записи), на начин који не привлачи пажњу потенцијалног малициозног корисника. Ово омогућава да се порука скрива унутар већ постојеће комуникације. На тај начин, чак и ако неко надгледа комуникацију, неће бити свјестан присуства скривених података. Комбинација ових техника омогућава слање приватних порука на начин који је сигуран и тешко уочљив за било кога ко није ауторизован за приступ тим подацима. На примјер, могуће је користити криптографију за енкриптовање поруке, а затим користити стеганографију да се та порука сакрије унутар слике или аудио записа. Само особа која зна кључ за декрипцију моћи ће да извуче поруку из скривене комуникације, што је посебно корисно кад је важно очувати приватност.

Да ли је предмет истраживања релевантан и у складу са предложеним насловом?	**ДА**	НЕ

4.4. Релевантност и савременост коришћених референци и литературе са списком литературе

Списак коришћене литературе садржи 42 библиографске јединице које су релевантне и савремене за предметно истраживање:

1. J. M. Hudson, P. L. Witt: Internet Relay Chat (IRC), in: *Handbook of Computer Networks*, H. Bidgoli, Ed., Wiley, pp. 889–897, 2007, doi: 10.1002/9781118256107.ch57.
2. C. Fuchs, D. Trottier: Internet surveillance after Snowden: A critical empirical study of computer experts' attitudes on commercial and state surveillance of the Internet and social media post-Edward Snowden, *JICES*, vol. 15, no. 4, pp. 412–444, 2017, doi: 10.1108/JICES-01-2016-0004.
3. B. Schneier: *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W.W. Norton & Company, 2016.
4. D. Vukovic, D. Gligoroski, Z. Djuric: CryptoCloak protocol and the prototype application, *IEEE Conference on Communications and Network Security (CNS)*, pp. 721–722, 2015, doi: 10.1109/CNS.2015.7346903.
5. R. Stedman, K. Yoshida, I. Goldberg: A user study of off-the-record messaging, *4th Symposium on Usable privacy and security*, pp. 95–104, 2008, doi: 10.1145/1408664.1408678.
6. O. Bini, S. Celi: No evidence of communication and implementing a protocol: Off-the-Record protocol version 4, *PoPETS-2018*, 2018.
7. OTRv4, [Online], Available at: https://otr.im/
8. K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, D. Stebila: A Formal Security Analysis of the Signal Messaging Protocol, *J. Cryptol*, vol. 33, no. 4, pp. 1914–1983, 2020, doi: 10.1007/s00145-020-09360-1.
9. M. S. Taha, M. S. Mohd Rahim, S. A. Lafta, M. M. Hashim, H. M. Alzuabidi: Combination of Steganography and Cryptography: A Short Survey, *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 518, no. 5, p. 052003, 2019, doi: 10.1088/1757-899X/518/5/052003.
10. S. Saraireh: A secure data communication system using cryptography and steganography, *Int. Journal of Computer Networks & Communications (IJCNC),* vol. 5, no. 3, 2013.
11. P. P. Aung, T. M. Naing: A Novel Secure Combination Technique of Steganography and Cryptography, *IJITMC*, vol. 2, no. 1, pp. 55–62, 2014, doi: 10.5121/ijitmc.2014.2105.
12. A. Jan, S. Parah, M. Hussan, B. Malik: Double layer security using crypto-stego techniques: a comprehensive review, *Health Tech*., vol. 12, no. 1, pp. 9–31, 2022, doi: 10.1007/s12553-021-00602-1.

13. A. M. Ahmed, A. S. Nori: Improve Security Using Steganography and Cryptography Based on Smartphone Users Locations, *2nd Int. Conf. on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, pp. 1–7, 2022, doi: 10.1109/ICAECT54875.2022.9808046.
14. M. Junaid, K. Farhan: Enhanced Audio LSB Steganography for Secure Communication, *IJACSA*, vol. 7, no. 1, 2016, doi: 10.14569/IJACSA.2016.070146.
15. E. W. Abood et al.: Audio steganography with enhanced LSB method for securing encrypted text with bit cycling, *Bulletin EEI*, vol. 11, no. 1, pp. 185–194, 2022, doi: 10.11591/eei.v11i1.3279.
16. J. Peng, S. Tang: Covert Communication Over VoIP Streaming Media With Dynamic Key Distribution and Authentication, *IEEE Trans. Ind. Electron.*, vol. 68, no. 4, pp. 3619–3628, 2021, doi: 10.1109/TIE.2020.2979567.
17. A. Chandragiri, P. A. Cooper, L. Yanxin, L. Qingzhong: Implementing secure communication on short text messaging, *2nd Int. Symp. on Digital Forensics and Security*, pp. 77-80, 2014.
18. M. T. Ahvanooey, Q. Li, J. Hou, H. D. Mazraeh, J. Zhang: AITSteg: An Innovative Text Steganography Technique for Hidden Transmission of Text Message via Social Media, *IEEE Access*, vol. 6, pp. 65981–65995, 2018, doi: 10.1109/ACCESS.2018.2866063.
19. S. Kingslin, N. Kavitha: Evaluative Approach towards Text Steganographic Techniques, *Indian Journal of Science and Technology*, vol. 8, no. 29, 2015, doi: 10.17485/ijst/2015/v8i1/84415.
20. A. Yahya: Steganography Techniques, in: *Steganography Techniques for Digital Images*, pp. 9–42, 2019, doi: 10.1007/978-3-319-78597-4_2.
21. A. Armando et al.: The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications, in: *Computer Aided Verification*, K. Etessami and S. K. Rajamani, Eds., *Lecture Notes in Computer Science*, vol. 3576, pp. 281–285. 2005, doi: 10.1007/11513988_27.
22. A. H. Shinde, A. Umbarkar, N.R. Pillai: Cryptographic Protocols Specification and Verification Tools - A Survey, *IJCT*, vol. 08, no. 02, pp. 1533–1539, 2017, doi: 10.21917/ijct.2017.0226.
23. P. R. Yogesh, R. D. Satish: Formal Verification of Secure Evidence Collection Protocol using BAN Logic and AVISPA, *Procedia Computer Science*, vol. 167, pp. 1334–1344, 2020, doi: 10.1016/j.procs.2020.03.449.
24. M. Singh, M. Ranganathan: Formal Verification of Bootstrapping Remote Secure Key Infrastructures (BRSKI) Protocol Using AVISPA, *NIST Technical Note 2123*, 2020, doi: 10.6028/NIST.TN.2123.
25. A. D. Azzahra, Y. Farida, A. A. Lestari: Formal Analysis of SMAP Fog/Edge Protocol Using AVISPA, *1st Int. Conf. on Smart Technology, Applied Informatics, and Engineering (APICS)*, pp. 31–35, 2022, doi: 10.1109/APICS56469.2022.9918818.
26. M. M. Modiri, J. Mohajeri, M. Salmasizadeh: A Novel Group-based Secure Lightweight Authentication and Key Agreement Protocol for Machine-Type Communication, *Scientia Iranica*, 2021, doi: 10.24200/sci.2021.54832.3936.
27. H. Dalkilic, M. H. Ozcanhan: A Strong Mutual Authentication Protocol for Securing Wearable Smart Textile Applications, *Adv. Electr. Comp. Eng.*, vol. 22, no. 1, pp. 31–38, 2022, doi: 10.4316/AECE.2022.01004.
28. T. Genet: A Short SPAN+AVISPA Tutorial, [Research Report] IRISA, 2015, Available at: https://inria.hal.science/hal-01213074v3
29. A. Gotsman, F. Massacci, M. Pistore: Towards an Independent Semantics and Verification Technology for the HLPSL Specification Language, *Electronic Notes in Theoretical Computer Science*, vol. 135, no. 1, pp. 59–77, 2005, doi: 10.1016/j.entcs.2005.06.004.
30. D. Dolev, A. Yao: On the security of public key protocols, *IEEE Trans. Inform. Theory*, vol. 29, no. 2, pp. 198–208, 1983, doi: 10.1109/TIT.1983.1056650.
31. D. Adrian et al.: Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice, *22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 5–17, 2015, doi: 10.1145/2810103.2813707.
32. C. Johansen, A. Mujaj, H. Arshad, J. Noll: The Snowden Phone: A Comparative Survey of Secure Instant Messaging Mobile Applications, *Security and Communication Networks*, vol. 2021, pp. 1–30, 2021, doi: 10.1155/2021/9965573.

33. J. Alwen, S. Coretti, Y. Dodis: The Double Ratchet: Security Notions, Proofs, and Modularization for the Signal Protocol, in: *Advances in Cryptology – EUROCRYPT 2019*, Y. Ishai and V. Rijmen, Eds., *LNCS*, vol. 11476, pp. 129–158, 2019, doi: 10.1007/978-3-030-17653-2_5.
34. N. Kobeissi: Formal verification for real-world cryptographic protocols and implementations, Cryptography and Security [cs.CR]. Université Paris sciences et lettres, 2018. Available at: https://theses.hal.science/tel-03245433/document
35. A. Jurcut, T. Coffey, R. Dojen, R. Gyorodi: Security Protocol Design: A Case Study Using Key Distribution Protocols, *Journal of Computer Science & Control Systems*, vol. 2, no. 2, 2009.
36. B. Schneier: *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, 2015.
37. R. Sharp: *Principles of protocol design*, Springer, 2008.
38. N. Ferguson, B. Schneier, T. Kohno: *Cryptography engineering: design principles and practical applications*, John Wiley & Sons, 2011
39. P. Syverson: Limitations on design principles for public key protocols, *IEEE Symposium on Security and Privacy*, pp. 62-72, 1996.
40. M. Abadi, R. Needham: Prudent Engineering Practice for Cryptographic Protocols, *IEEE Trans. Softw. Eng.*, vol. 22, no. 1, pp. 6–15, 1996.
41. L. Dong, K. Chen, M. Wen, Y. Zheng: Protocol Engineering Principles for Cryptographic Protocols Design, *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, pp. 641-646, 2007, doi: 10.1109/SNPD.2007.441.
42. L. Dong, K. Chen: Engineering Principles for Security Design of Protocols, in: *Cryptographic Protocol*. Springer, https://doi.org/10.1007/978-3-642-24073-7_3.

Да ли су коришћена литература и референце релевантне у погледу обима, садржаја и савремености.	**ДА**	НЕ

4.5. Циљеви истраживања

Главни циљеви истраживања су:

- Развој новог протокола за текстуалну комуникацију у оквиру *IM* апликација, који интегрише криптографске и стеганографске технике, у сврху смањења детектабилности криптоване комуникације.
- Повећање нивоа приватности корисника у комуникацији предложеним протоколом, уз задовољавање фундаменталних сигурносних захтјева, при чему предложени протокол треба да користи стандардне *IM* протоколе као транспортне протоколе.
- Предложени протокол треба да има перформансе које омогућавају његову примјену у пракси.

Да ли су циљеви истраживања јасно дефинисани и усклађени са предметом истраживања?	**ДА**	НЕ

4.6. Хипотеза истраживања: главна и помоћне хипотезе

У складу са циљевима истраживања, постављене су сљедеће хипотезе:

H_1: Комбинација криптографских и стеганографских техника у новом протоколу за текстуалну комуникацију значајно смањује детектабилност криптоване комуникације, истовремено повећавајући ниво приватности корисника и задовољавајући фундаменталне сигурносне захтјеве.

H_2: Предложени протокол може користити стандардне IM протоколе као транспортне протоколе.

H_3: Предложени протокол је примјењљив у пракси јер вријеме размјене порука између учесника у комникацији не одступа знанчајније од времена размјене порука код постојећих рјешења.

Да ли је хипотеза истраживања јасно дефинисана?	**ДА**	НЕ

4.7. Очекивани резултати

У поређењу са постојећим познатим протоколима, предложени протокол ће отклонити један од основних недостатака *IM* комуникације – детектабилност. Надаље, комбинацијом криптографских и стеганографских техника у дизајну новог протокола очекује се значајно унапређење приватности корисника у текстуалној *IM* комуникацији, при истовременом задовољавању фундаменталних сигурносних захтјева. Фундаментални сигурносни захтјеви биће предмет формалне верификације уз примјену специјализованих алата за анализу сигурносних аспеката протокола.

Предложени протокол биће имплементиран у оквиру прототипа рјешења за *IM* комуникацију, при чему ће имплементација користити један од постојећих *IM* протокола као транспортни слој, а вријеме размјене порука између учесника у комуникацији неће значајно одступати од времена размјене у постојећим рјешењима.

Да ли је образложен научни значај и/или потенцијална примјена очекиваних резултата?	**ДА**	НЕ

4.8. План рада и временска динамика

Фаза 1: Преглед литературе и анализа постојећих протокола

- Прикупљање релевантне литературе о *IM* протоколима и техникама стеганографије и криптографије.
- Детаљна анализа постојећих протокола за *IM* комуникацију и идентификација њихових снага и слабости.
- Документовање налаза из анализе литературе и постојеће технологије.

Фаза 2: Дизајн протокола

- Дефинисање основних принципа и алгоритама за комбиновање криптографије и стеганографије.
- Детаљни дизајн протокола.
- Преглед и ревизија дизајна како би се осигурала тачност и практичност имплементације.

Фаза 3: Формална верификација

- Припрема спецификација за формалну верификацију протокола *AVISPA* алатом.
- Спровођење формалне верификације.
- Анализа резултата добијених формалном верификацијом протокола.

Фаза 4: Компаративна студија

- Поређење карактеристика имплементираног протокола са постојећим протоколима.
- Статистичка анализа и интерпретација резултата компаративне студије.
- Документовање резултата компаративне студије.

Фаза 5: Имплементација апликативног прототипа

- Развој прототипа.
- Тестирање прототипа и исправљање грешака.

Фаза 6: Документација и презентација истраживања

- Детаљно документовање свих фаза истраживања, дизајна, имплементације и евалуације.
- Валидација хипотеза.
- Припрема рукописа за академске публикације и презентације за конференције.
- Израда завршног извјештаја истраживања.

Временска динамика није екплицитно наведена у пријави, али резултати истраживања, који су недавно објављени у истакнутом научном часопису међународног значаја, указују на чињеницу да је планирано истраживање већ у значајној мјери и спроведено.

Да ли су предложени одговарајући план рада и временска динамика израде дисертације?	**ДА**	НЕ

4.9. Материјал и методологија рада

Анализа постојећих протокола:

- Преглед постојећих протокола за *IM* комуникацију како би се идентификовале њихове снаге и слабости.
- Компаративна анализа сигурносних карактеристика постојећих протокола.

Дизајн и имплементација:

- Дизајн новог протокола коришћењем комбинације криптографских и стеганографских техника.
- Опис протокола кроз дијаграм тока порука и формалне нотације протокола.
- Дизајн и имплементација апликативног прототипа.

Формална верификација:

- Коришћење алата за формалну верификацију сигурносних карактеристика имплементираног протокола.
- Анализа резултата верификације како би се утврдила поузданост и сигурност протокола.

Компаративна студија:

- Поређење карактеристика протокола са постојећим *IM* протоколима на основу различитих параметара као што су сигурност, приватност, детектабилност и перформансе.
- Статистичка анализа резултата како би се утврдила значајност унапређења које доноси имплементирани протокол.

Документација и презентација истраживања:

- Детаљно документовање свих фаза истраживања, дизајна, имплементације и евалуације протокола.
- Припрема публикација за академске конференције и часописе како би се резултати истраживања подијелили са широм научном заједницом.

Да ли су предвиђени материјал и методологија рада одговарајући?	**ДА**	НЕ

4.10. Мјесто, лабораторија и опрема за експериментални рад

Истраживање ће бити реализовано на Електротехничком факултету Универзитета у Бањој Луци, у рачунарским лабораторија Катедре за рачунарство.

Планирана је употреба сљедеће опреме:

- персонални рачунари са оперативним системима *Windows 10/11* и *Linux Mint 22 Wilma*,
- *AVISPA* алат за формалну верификацију сигурносних протокола,
- *XMPP* сервер и *XMPP* клијенти,
- *MySQL* систем за управљање базама података,
- остала хардверска помоћна опрема и софтверски алати.

Да ли су предвиђени одговарајуће мјесто, лабораторија и опрема за експериментални рад?	**ДА**	НЕ
Да ли је планирана сарадња са другим институцијама у земљи и иностранству?	ДА	**НЕ**
Да ли је тема подобна?	**ДА**	НЕ

5. ЗАКЉУЧАК		
Да ли студент испуњава прописане услове?	**ДА**	НЕ
Да ли је тема подобна?	**ДА**	НЕ
Да ли ментор испуњава прописане услове?	**ДА**	НЕ

Образложење (до 300 ријечи):

Предложена тема докторске дисертације кандидаткиње Дијане Вуковић Грбић, под називом „Развој протокола за сигурну и приватну комуникацију инстант порукама“, јасно дефинише проблем и кључне аспекте истраживања. Тема је релевантна, односи се на актуелне изазове и проблеме обезбјеђивања сигурне и приватне комуникације инстант порукама, те има потенцијално значајан теоријски и практични допринос. Формулација наслова је прецизна, кохерентна и у складу са научним стандардима. План рада, методологија истраживања и предвиђени ресурси јасно су дефинисани и омогућавају валидно тестирање постављених хипотеза.

Кандидаткиња Дијана Вуковић Грбић испуњава све академске и стручне услове за реализацију предложене докторске дисертације. Њено претходно образовање на првом, другом и трећем циклусу студија, уз досадашњи научноистраживачки рад који се огледа у више од 20 научних радова, од којих је један објављен у истакнутом научном часопису међународног значаја, потврђују њену компетентност за извођење комплексног истраживања у области којој припада предложена тема докторске дисертације.

Ментор дисертације, проф. др Зоран Ђурић, редовни професор у области рачунарских наука, посједује значајно научно и стручно искуство које се огледа у великом броју радова објављених у истакнутим научним часописима међународног и националног значаја те учешћу у изузетно великом броју стручних пројеката у области сигурности рачунарских система, што га чини изузетно компетентним за менторство на овој докторској дисертацији.

На основу наведеног, предложену тему, кандидаткињу и ментора оцјењујемо као подобне за реализацију докторске дисертације.

Бања Лука, Београд, 11.12.2024.

Др Дражен Брђанин, ванредни професор
Предсједник комисије, с.р.

Др Бошко Николић, редовни професор
Члан, с.р.

Др Милош Цветановић, ванредни професор
Члан, с.р.

ИЗДВОЈЕНО МИШЉЕЊЕ: Члан комисије који не жели да потпише извјештај јер се не слаже са мишљењем већине чланова комисије дужан је да у извјештај унесе образложење, односно разлоге због којих не жели да потпише извјештај.

У прилогу Извјештаја доставити:

1. Одлуку о прихватању пријаве теме докторске дисертације;
2. Одлуку о именовању Комисије за оцјену подобности студента, теме и ментора за израду докторске дисертације;
3. Доказе о подобности чланова комисије (радови и пратећи докази из члана 12. Правила студирања на III циклусу студија за студије започете закључно са академском годином 2021/2022, односно докази из члана 31. Правила студирања на трећем циклусу студија за студије започете од академске 2022/2023. године); и
4. Доказе о подобности првог ментора/другог ментора (радови и пратећи докази из члана 11. Правила студирања на III циклусу студија за студије започете закључно са академском годином 2021/2022, односно докази из члана 30. Правила студирања на трећем циклусу студија за студије започете од академске 2022/2023. године).