VEĆU DEPARTMANA ZA POSLEDIPLOMSKE STUDIJE
UNIVERZITETA SINGIDUNUM

Beograd
Danijelova 32

Odlukom Veća Departmana za poslediplomske studije i međunarodnu saradnju Univerziteta Singidunum, broj 4-239/2016 od02.07.2016.godine, određenismo za članove Komisije za pregled, ocenu i usmenu odbranu doktorske disertacije Dejana Savića, master pod nazivom: *"Jedna klasa sistema zaštite u računarskom oblaku zasnovana na homomorfnim šiframa"*.

Posle pregleda dostavljene Disertacije i drugih pratećih materijala, Komisija je sačinila sledeći

REFERAT

1. UVOD

1.1 Hronologija odobravanja i izrade disertacije

Dejan Savić je upisao doktorske studije na Singidunum univerzitetu školske 2009/2010. godine. Položio jesvih 12 ispita, sa srednjom ocenom 10. Zahtev za odobravanje teme za izradu doktorske disertacije podneo je 2016.godine. Odlukom VećaDepartmana za poslediplomske studije i međunarodnu saradnju Univerziteta Singidunum, broj 4-239/2016 od 02.07.2016. godine, formirana je Komisija u sastavu:

1. dr Mladen Veinović, redovni profesor, Univerzitet Singidunum, Beograd
2. dr Milan Milosavljević, redovni profesor, Univerzitet Singidunum, Beograd
3. dr Goran Šimić, vanredni profesor, Univerzitet odbrane, Beograd

zaocenu teme i podobnosti kandidata za izradu doktorske disertacije pod nazivom:"*Jedna klasa sistema zaštite u računarskom oblaku zasnovana na homomorfnim šiframa"*.Na osnovu pozitivnog izveštaja Komisije Senat Univerziteta Singidunum je 2016. godine odobrio rad na izradi doktorske disertacije.Za mentora je imenovan prof. dr Mladen Veinović.

1.2. Naučna oblast disertacije

Tema disertacije kandidata je u oblasti informatike i računarstva, za koju je Fakultet za informatiku i računarstvo Univerziteta Singidunum matičan.

1.3. Biografski podaci o kandidatu

Dejan Savić je rođen 22.06.1975. uZemunu, Republika Srbija. Srednju školu"Nikola Tesla" u Beograduzavršio je 1994. godine.

Školske 1994/1995. godine upisao je Vojnotehničku akademiju u Beogradu smer elektronski sistemi na kome je 1999. godine diplomirao.

Master studije upisao je školske 2007/2008.godine na Fakultetu za primenjenu informatiku (smer "Savremene informacione tehnologije") Univerziteta "Singidunum". Master

rad odbranio je kod mentora prof dr Mladena Veinovića 2009. godine i stekao akademski naziv mastera informacionih tehnologija.

Trenutno je zaposlen u Vojnobezbednosnoj agenciji Ministarstva odbrane Republike Srbije na radnom mestu operativca.

Recenzent je više radova za međunarodni Tajvanski časopis *Journal of Internet Technology* iz oblasti računarske bezbednosti koji se nalazi na SCI listi časopisa.

Trenutno učestvuje na istraživačkom projektuju *Upravljanje pristupom zaštićenim resursima računarskih mreža u MO i VS na osnovu multimodalne biometrijske identifikacije korisnika*, Univerziteta odbrane Ministarstva odbrane Republike Srbije.

Tokom konstantnog usavršavanja uspešno je završio više specijalističkih kurseva iz oblasti informacione bezbednosti i IT administracije kao što su:

- Tehnologija organizacije napada na WEB servise i monitoring socijalnih mreža, Moskva, Rusija
- Sertifikovani etički haker EC - Council, Oberammergau, Nemačka
- Cisco CCNA, Beograd, Srbija
- Linux IT Academy,Beograd, Srbija
- Microsoft Solution Expert Private Cloud,Beograd, Srbija
- VMware vSphere,Beograd, Srbija.

Kandidat je *ušestvovao*na više projekata u privredi kao što su:

- Informatička podrška međunarodnim turnirima u rvanju grčko-rimskim i slobodnim stilom za žene i muškarce u organizaciji Rvačkog saveza u zadnjih deset godina.
- Informatička podrška 2. međunarodnom atletskom mitingu "Memorijal Artur Takač.
- Razvoj i implementacija poslovne aplikacije za Beogradski "Alo taksi".
- Razvoj i implementacija poslovne aplikacije za Višu poslovnu školu Čačak.
- Razvoj i implementacija poslovne aplikaciju za firmu "Rastošnica" iz Beograda.
- Razvoj i implementacija poslovne aplikaciju za firmu "Komunalac Čukarički" iz Beograda.
- Razvoj i implementacija aplikacije za vođenje sportske kladionice za lanac kladionica Roma sa sedištem u Nikšiću.

Razvoj i implementacija aplikacije za vođenje sportske kladionice za lanac kladionica Bubamara sa sedištem u Podgorici.

2. OPIS DISERTACIJE

2.1. Sadržaj disertacije

Doktorska disertacijapod naslovom: "*Jedna klasa sistema zaštite u računarskom oblaku zasnovana na homomorfnim šiframa*" ima ukupno 102strane. Disertacija ima šest poglavlja i spisak literature. Poglavlja su:

1. Uvod, 9 strana
2. Računarstvo u oblaku, 19 strane
3. Homomorfni šifarski sistemi, 20 strana
4. Povećanje stepena bezbednosti ključeva primenom VFS, 13 strana
5. Primena jedne klase homomorfnog šifarskog sistema kod sistema sa ograničenim resursima, 14 strana
6. Zaključak, 4 strane.

U disertaciji ima ukupno 28 slika, 1 tabela i 44 izraza. Literatura sadrži 83 bibliografske jedinice.

2.2. Kratak prikaz pojedinačnih poglavlja

U uvodu su prikazane osnovne ideje koje su motivisale istraživački rad na temi disertacije. Korišćenjem pokazatelja istaknuta je aktuelnost teme i dat značaj teme u svakodnevnom životu. Definisane su hipoteze naučnog istraživanja, metode koje će biti korišćenje i naveden je sam tok naučnoistraživačkog rada te je dat očekivani naučni doprinos. Na kraju poglavlja dat je kratak pregled preostalih poglavlja.

Drugo poglavlje se bavi računarstvom u oblaku. Kroz više navoda literature prikazan je istorijski razvoj računarstva u oblaku idata jesama definicija računarstva u oblaku. Obzirom na postojanje više modela računarstva u oblaku autor je odabrao opšteprihvaćenu *NIST* metodologiju i prateći je prikazao modele računarstva u oblaku. Nadalje je se osvrnuo na mobilno računarstvo u oblaku gde ga je definisao, objasnio arhitekturne principe, naveo prednosti u primeni kao i aktuelne probleme koji postoje u mobilnom računarstvu u oblaku. Prikazani su aktuelni bezbedosni problemi i pretnje kod računarstva u oblaku i ponaosob kod mobilnog računarstva u oblaku.

U trećem poglavlju autor je se bavio homomorfnim šifarskim sistemima. U prvom delu objasnio je pojam i koristeći matematički alat definisao homomorfizam u šifarskim sistemima. Obzirom na činjenicu da postoje potpuno i delimično homomorfni šifarski sistemi autor je uveo oba pojma, definisao ih i oba rešenja prikazao kroz aktuelne implementacije.

U trećem poglavlju je takođe prikazana aktuelna primena homomorfnih šifarskih sistema u realnom životu. Kroz pet oblasti primene dati su aktuelni dometi homomorfnih šifarskih sistema i stvarni modeli korišćenja sa karakteristikama.

Četvrto poglavlje se bavi problemima povećanja stepena bezbednosti šifarskih ključeva primenom virtuelnog fajl sistema. Tokom praktične realizacije šifarskog sistema problem čuvanja i primene šifarskih ključeva je veoma bitan te se tokom istraživanja došlo na ideju da se šifarski ključevi čuvaju na *Smart Card* uređajima. Autor je implementirao ovo rešenja na

*Unix/Linux*operativnim sistemima i kroz poglavlje je opisao sam način implementacije dajući pri tome kroz poglavlje deo razvijenog koda.

Peto poglavlje je centralno poglavlje u kome se prikazuje najvažniji naučni doprinos disertacije. Detaljno se opisuje problem koji se posmatra prilikom čega se vrši njegovo modelovanje i predlaže testni problem i njegov jednostavniji model.

Potom se opisuje implementacija predloženog rešenja koja je u ovom slučaju realizovana na dve različite platforme uređaja sa ograničenim resursima, industrijskog računara *Raspberyy Pi* i *Android* mobilnih telefona. Nadalje se opisuje proces implementacije samog eksperimenta sa dobijenim mernim rezultatima kojima se pokazuje da je moguća implementacija delimično homomorfnih šifarskih sistema na obe pomenute platforme. Na osnovu dobijenih rezultata da se videti koja su ograničenja u smislu dužine primenjenih ključeva, broja nadgledanih senzora i dužine rezutata korektivne funkcije. Tokom poglavlja dati su pojedini delovi razvijenog koda kako za *Unix/Linux* operativni sistem tako i za *Android* operativni sistem.

U zaključku teze su navedeni osnovni doprinosi disertacije i date su smernice za moguća dalja istraživanja u ovoj oblasti.

3. OCENA DISERTACIJE

3.1. Savremenost i originalnost

Opšte je poznato da je jedan od bezbednih načina čuvanja podataka koji se nalaze u računarskom oblaku i primena šifarskih metoda. Nažalost, skladištenje podataka u obliku šifrata na računarskom oblaku ima nedostatak koji se ogleda u nemogućnosti obrade tih podataka unutar računarskog oblaka bez njihovog prethodnog dešifrovanja. Ova osobina onemogućava primenu bitne mogućnosti računarskog oblaka, obradu uskladištenog sadržaja po zahtevu korisnika uz korišćenje znatnih resursa koje poseduje sam računarski oblak.

Akademska zajednica u zadnje vreme ulaže velike napore u istraživanju i unapređenju šifarskih metoda kojima se omogućava obrada šifrata u računarskom oblaku. Prateći ove trendove uočili smo da je veza između šifarskih metoda primenjenih na računarskom oblaku i sistemima sa ograničenim računarskim resursima malo istražena a da postoje znatni potencijali njene primene u svakodnevnom životu.

Shodno tome došli smo do predloga predmeta istraživanja ovoga rada koji bi bio istraživanje mogućnosti sprovođenja izvršavanja homomorfnog šifarskog sistema na računarskom sistemu sa ograničenim resursom i određenje karakteristika te primene i mogućnosti svakodnevne primene.

Prateći ovo kandidat je primenjujući jedan delimično homomorfni šifarski sistem kroz praktičan primer došao do zaključaka da se on može implementirati na sisteme sa ograničenim računarskim resursima i eksperimentalnim putem došao do ograničenja koji ovakav sistem ima.

U ovom kontekstu, kandidat je svoju originalnost potvrdio na korektan i uverljiv način-objavljivanjem radova u međunarodnim naučnim časopisima (1 rad u časopisu sa impakt faktorom) i u zbornicima sa međunarodnih (1 rad) i domaćih (3 rada) naučnih konferencija.

3.2. Osvrt na referentnu i korišćenu literaturu

U izradi disertacije korišćena je obimna literatura iz oblasti šifarskih sistema, bezbednosti računarskih sistema, računarskog oblaka polazeći od fundamentalnih referenci, pa sve do najnovijih radova u vrhunskim međunarodnim naučnim časopisima uključujući i

sopstvene reference. Na osnovu tih referenci, originalni naučni rezultati do kojih je kandidat došao u disertaciji su stavljeni u korektan kontekst.

3.3. Opis i adekvatnost primenjenih naučnih metoda

Kandidat je u svom istraživačkom radu koristio više različitih postupaka. Najpre je uvidom u literaturu, zajedno sa mentorom došao do zaključka o potrebi za istraživanjem efikasosti homomorfnog šifrovanja na sistemima sa ograničenim resursima potpomognutim računarskim oblakom. Detaljnom analizom raspoloživih pristupa uočene su oblasti primene, nedostatk primene dosadašnjih šifarskih sistema i formulisan je cilj istraživanja:koliko je realizacija povećanja bezbednosti podataka primenom homomorfnog šifrovanja na posmatranom sistemu prihvatljiva za neku realnu, svakodnevnu upotrebu, potreba da se postave granice i ograničenja kako u načinu upotrebe homomorfnih šifarskih sistema tako i u resursima neophodnim za istu, koji problemi bi mogli biti rešeni takvom primenom homomorfnog šifrovanja i sa kojim ograničenjima.

U postupku razvoja i implementacije predložene šifarske šeme, kandidat je pokazao samostalnost i inventivnost u izboru modela, odabiru optimalnih alata za realizacuju, njihovim ovladavanjem i naposletku samim implementiranjem. Očekivani rezultati su u potpunosti verifikovani iscrpnim merenjima koja su izvršena na testnom modelu.

Prednosti i nedostaci predloženog pristupa na bazi primene homomorfnih šifarskih sistema su kritički sagledani i na kraju disertacije su date smernice za moguća dalja istraživanja.

3.4. Primenljivost ostvarenih rezultata

Rezultati do kojih je kandidat došao u svojoj disertaciji mogu imati neposrednu primenu u oblasti napredne zaštite računarskih sistema koji koriste usluge računarskog oblaka. Naime, testni model veoma verno oslikava realne sisteme i za očekivati je da su rezultati simulacije veoma bliski mogućem ponašanju implementacije na realnim sistemima. Stoga se predloženi pristup može uspešno primeniti.

3.5. Ocena dostignutih sposobnosti kandidata za samostalni naučni rad

Kandidat je u svom dosadašnjem radu pokazao kvalitete presudne za uspešan istraživački rad: sposobnost uočavanja problema i postavljanje korektnog cilja istraživanja, shvatanje i proširivanje teorijskih koncepata, originalnost, sposobnost da teorijske metode pretoči u algoritme, strukture podataka i računarske programe, kao i da kritički analizira dobijene rezultate.

4. OSTVARENI NAUČNI DOPRINOS

4.1. Prikaz ostvarenih naučnih doprinosa

Originalni naučni doprinosi disertacije se mogu formulisati na sledeći način:

- Sistematizacija i klasifikacija postojećih rešenja homomorfih šifarskih sistema i područija njihove upotrebe gde autor predlaže novi koncept upotrebe u oblasti automatizovane detekcije organizovanog kriminala,
- Novi pristup povećanju stepena bezbednosti ključeva primenom virtuelnog fajl Sistema gde se sam fajl u kome se nalazi privatni ključ praktično uvezuje na postojeći fajl sistem kroz poseban API, takozvani FUSE fajl sistem koji je jedna vrsta spone između samog korisničkog memorisjkog prostora u kome se izvršava aplikacija koja koristi privatni ključ i fizičkog skladišta privatnog ključa, u našem slučaju Java smart kartice,
- Izvršenim istraživanjem je pokazano da je moguće vršiti homomorfno šifrovanje u računarskom oblaku kao i da su računarski sistemi sa ograničenim resursima u mogućnosti da budu krajnji korisnici takvog rešenja. Obavljenim eksperimentima došlo se do stvarnih pokazatelja u kojoj meri je moguće koristiti ovakav scenario u realnim uslovima, koja su realna ograničenja, kolike su očekivane vrednosti parametara i za koje realne sisteme je moguće primeniti ovo rešenje.
- Sa dva nezavisna seta eksperimenata na dve nezavisne platforme, industrijski računar i set mobilnih telefona različitih generacija pokazano je ponašanje sistema u uslovima računarskog oblaka i mobilnog računarskog oblaka.

Predložena rešenja ukazuju na moguće nove načine korišćenja homomorfnih šifarskih sistema i daju merljive vrednosti o njihovom ponašanju na računarskom oblaku i na klijentima sa ograničenim hardverskim resursima. Obzirom na nadolazeće doba Interneta stvari i scenarija gde se računarski oblak kao veliki i snažni brat tankih klijenata pojavljuje da rešava njihove potrebe za skladištenjem i obradom podataka kao očigledna kombinacija, istraživanje za ultimatimnom potrebom za bezbednošću je veom savremeno i neophodno što pokazuje akademska zajednica sa sve većom zastupljenošću istraživanja o bezbednosti računarskog oblaka.

4.2. Kritička analiza rezultata istraživanja

U prvoj fazi kandidat je razmatrajući raspoloživu literaturu u oblasti teme disertacijeizvršio kritičku analizu dostupnih informacija i korektno definisao cilj istraživanja.

Tokomistraživačkog rada koristio je mogućnost kritičkog preispitivanja i pogodne načine unapređenja postojećih rešenja dodajući svoj doprinos kroz nove ideje.

Predloženi model rešenja postavljenog problema je praktično implementiran i eksperimentalno su dobijeni rezultata modelovanja sa odgovarajućim referentnim vrednostima (eksperimentalnim ili rezultatima računarskih simulacija).

Uočene su i prikazane prednosti i nedostaci predloženog pristupa i ukazano na smernice mogućih daljih istraživanja.

4.3.Verifikacija naučnih doprinosa

Naučni doprinosi disertacije verifikovani su sledećim radovima kandidata:

Kategorija M23

1. **D. Savić**, M. Trikoš, M. Veinović, D. Simić, *An application of partial homomorphic encryption in computer system with limited resources*, Technical Gazette, Vol. 25/No. 3, 2018.

Kategorija M33

1. M. Trikoš, **D. Savić**, *Upravljanje identitetima u računarskoj mreži kampusa primenom open source rešenja*, 58. konferencija za elektroniku, telekomunikacije, računarstvo, automatiku i nuklearnu tehniku, ETRAN 2014. ISBN 978-86-805095-70-9, jun 2014, Vrnjačka Banja.

Kategorija M63

1. M. Trikoš, **D. Savić**, *Posmatranje žrtve - prvi korak u napadu na informaciono-komunikacione sisteme*, XX konferencija i računarskim naukama i informacionim tehnologijama, YU INFO 2014. ISBN 978-86-85525-13-1, mart 2014, Kopaonik
2. **D. Savić**, M. Veinović, M. Trikoš, *Primena SMART kartica za ostvarivanje VPN konekcije*, ISBN 978-86-85525-08-7, mart 2011, Kopaonik
3. M. Veinović, **D. Savić**, Povećanje stepena bezbednosti VPN, 8. naučni skup sa međunarodnim učešćem Sinergija 2011, Bijeljina

5.MIŠLJENJE KOMISIJE I PREDLOG

Na osnovu izloženog, komisija konstatuje da doktorska disertacija Dejana Savića,master informacionih tehnologija, pod naslovom "*Jedna klasa sistema zaštite u računarskom oblaku zasnovana na homomorfnim šiframa*" ispunjava sve formalne i suštinske uslove predviđene Zakonom o visokom obrazovanju, kao i propisima univerziteta Singidunum u Beogradu. Doktorska disertacija Dejana Savića sadrži naučne doprinose koji se sastojeu analizi iprimeni koncepta homomorfnih šifarskih sistema radi povećanja stepena bezbednosti podataka koje računari sa ograničenim hardverskim resursima veoma bezbedno čuvaju i obrađuju na računarskom oblaku.

Tokom celokupne izrade doktorske disertacije, kandidat je pokazao nesumnjivu sposobnost za samostalni nauučnoistraživački rad. Stoga članovi Komisije sa zadovoljstvom predlažu Veću departmana za poslediplomske studije i međunarodnu saradnju da se doktorska disertacija pod naslovom "*Jedna klasa sistema zaštite u računarskom oblaku zasnovana na homomorfnim šiframa*" kandidata Dejana Savića, mastera u oblasti informacionih tehnologija prihvati, izloži na uvid javnosti i uputi na konačno usvajanje Senatu univerziteta Singidunuma u Beogradu.

Beograd, 07. 09. 2017. godine

Članovi komisije:

dr Mladen Veinović, redovni profesor,
Univerzitet Singidunum, Beograd

dr Milan Milosavljević, redovni profesor,
Univerzitet Singidunum, Beograd

drGoran Šimić, vanredni profesor,
Univerzitet odbrane, Beograd