УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ ОРГАНИЗАЦИОНИХ НАУКА

30.04.2012. године
Београд,
04-03-11/49

УНИВЕРЗИТЕТ У БЕОГРАДУ
Веће научних области техничких наука
Београд
Студентски трг бр 1

У прилогу дописа достављамо извештај комисије о оцени завршене докторске дисертације кандидата мр Аце (Стојан) Алексића, са пратећом документацијом.

Докторска дисертација и извештај комисије о оцени завршене докторске дисертације кандидата мр Аце (Стојан) Алексића стављени су на увид јавности и у предвиђеном року није било примедби на изложену докторску дисертацију.

С поштовањем,

Секретар факултета

Гордана Алексић Славински, дипл. Правник

Образац 2.

Факултет организационих наука

УНИВЕРЗИТЕТ У БЕОГРАДУ

04-03-11/49
(Број индекса)

Веће научних области техничких наука
(назив стручног већа коме се захтев упућује, сходно чл 75. Статута Универзитета у Београду и чл.7. ст. 1. овог Правилника)

30.04.2012. године
(Датум)

Београд
Студентски трг бр.1

ЗАХТЕВ
за давање сагласности на извештај о урађеној докторској дисертацији

Молимо да, сходно члану 68. ст. 3. Закона о универзитету («Службени гласник РС» бр. 20/98), дате сагласности на Извештај о урађеној докторској дисертацији кандидата
мр Аце (Стојан) Алексића
(име, име једног родитеља и презиме)

Кандидат мр Аца (Стојан) Алексић пријавио је докторску дисертацију под називом:
(име, име једног родитеља и презиме)

Статистички модел аутоматизованог управљања дигиталним сертификатима

Универзитет је дана 10.04.2009. године својим актом под 612-25/63/09 дао сагласност на предлог теме докторске дисертације која је гласила

Статистички модел аутоматизованог управљања дигиталним сертификатима

Комисија за оцену и одбрану докторске дисертације кандидата мр Аце (Стојан) Алексића
(име, име једног родитеља и презиме)

образована је на седници одржаној 15.06.2011. године, одлуком Факултета под 3/56-4 у саставу:

	име и презиме члана комисије	звање	научна област
1.	др Зоран Радојичић	ванр. проф. ФОН-а	рачунарска статистика
2.	др Братислав Петровић	ред. проф. ФОН-а	управљање системима
3.	др Душан Старчевић	ред. проф. ФОН-а	информационе технологије
4.	др Драган Вукмировић	ред. проф. ФОН-а	електронско пословање
5.	др Вељко Милутиновић	ред. проф. ЕТФ-а	рачунарска техника и информатика

Наставно-научно веће Факултета прихватило је извештај Комисије за оцену и одбрану докторске дисертације на седници одржаној дана 28.03.2012. године.

ДЕКАН ФАКУЛТЕТА

_____

Проф. др Милан Мартић

Прилог:

1. Извештај Комисије са предлогом,
2. Акт Наставно-научног већа Факултета о усвајању Извештаја,
3. Примедбе дате у току стављања Извештаја на увид јавности, уколико је таквих примедби било.

05-01 бр 3/40-6

Поводом предлога Већа студијског програма докторских академских студија, а на основу члана 56. Статута Факултета, на седници Наставно-научног већа одржаној 28.3.2012. године, једногласно је донета следећа

О Д Л У К А

Прихвата се Извештај Комисије за оцену завршене докторске дисертације кандидата мр Аце Алексића, под насловом »СТАТИСТИЧКИ МОДЕЛ АУТОМАТИЗОВАНОГ УПРАВЉАЊА ДИГИТАЛНИМ СЕРТИФИКАТИМА« и даје се на увид јавности.

На Наставно-научном Већу 30.04.2009. године одобрена је израда докторске дисертације кандидата мр Аце Алексића под називом »СТАТИСТИЧКИ МОДЕЛ АУТОМАТИЗОВАНОГ УПРАВЉАЊА ДИГИТАЛНИМ СЕРТИФИКАТИМА« на основу добијене Одлуке Већа научних области техничких наука Универзитета у Београду, о давању сагласности на предлог теме докторске дисертације од 10.04.2009. године, број: 612-25/63/09.

Кандидат мр Аца Алексић је објавио следеће радове који га квалифику да може да одбрани докторску дисертацију:

1. Миленковић Д., Јовановић Миленковић М., Вујин В., Алексић А., Радојичић З., „Electronic health system and its introduction into the health system of the Republic of Serbia", Војносанитетски преглед, Београд, 2011, ISSN 0042-8450, http://www.vma.mod.gov.rs/vsp/ (прихваћен за објављивање) IF=0.199 Science Citation Index Expanded (SCIe) by Thomson Reuters http://science.thomsonreuters.com/cgi-bin/jrnlst/jlresults.cgi?PC=MASTER&ISSN=0042-8450

2. Јеремић В., Секе К., Радојичић З., Јеремић Д., Марковић А., Словић Д., Алексић А., „Measuring health of countriers;a novel approach", HealthMED, Vo. 5, No.6, Novembar 2011, ISSN 1840-2291, http://helthmedjournal.com IF=0.331 Science Citation Index Expanded (SCIe) by Thomson Reuters http://science.thomsonreuters.com/cgi-bin/jrnlst/jlresults.cgi?PC=MASTER&ISSN=1840-2291

Председник Наставно научног већа

Проф. др Милан Мартић

Доставити:
- Служби за ПДС
- Секретару органа управљања и стручних органа
- Архиви

УНИВЕРЗИТЕТ У БЕОГАДУ
ФАКУЛТЕТ ОРГАНИЗАЦИОНИХ НАКА

НАУЧНО-НАСТАВНОМ ВЕЋУ

ПРЕДМЕТ: ИЗВЕШТАЈ КОМИСИЈЕ ЗА ОЦЕНУ ЗАВРШЕНЕ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

Поштоване Колегинице и Колеге,

Одлуком Научно-наставног већа ФОН-а од 15.06.2011. године именовани смо у комисију за оцену завршене докторске дисертације мр Аце Алексића, под насловом:

„Статистички модел аутоматизованог управљања дигиталним сертификатима“

и на основу тога подносимо следећи:

И З В Е Ш Т А Ј

1. УВОД

1.1. Наслов и обим дисертације

Наслов дисертације је: „Статистички модел аутоматизованог управљања дигиталним сертификатима“. Дисертација је обима 183 страница, садржи 52 слике и 5 графичких приказа, 12 табела, и 126 литературних навода.

1.2. Хронологија одобравања и израде дисертације

Кандидат је поднео пријаву за одобравање израде докторске дисертације “Статистички модел аутоматизованог управљања дигиталним сертификатима“ 19.02.2009. године. Наставно-научно веће ФОН-а је именовало комисију за оцену научне заснованости теме пријављене докторске дисертације 25.02.2009. године. Позитиван извештај комисије усвојен је на седници Наставно-научног већа одржаној 18.03.2009. године, одлука бр. 3/37-7. Стручно веће Универзитета у Београду је на седници одржаној 10.04.2009. године одобрило израду предложене докторске дисертације, одлука бр. 612-25/63/09.

Након добијене сагласности стручног већа Универзитета у Београду, на седници Наставно-научног већа ФОН-а одлуком бр. 3/51-8 од 30.04.2009. године одобрена је израда докторске дисертације кандидата мр Аце Алексића под насловом “Статистички

модел аутоматизованог управљања дигиталним сертификатима", и за ментора је именован др Зоран Радојичић, ванредни професор ФОН-а.

Ментор, др Зоран Радојичић ванр. проф. је констатовао да је докторска дисертација завршена и Наставно-научно веће ФОН-а је одлуком бр 3/56-4 од 15. јуна 2011. године формирало комисију за преглед и оцену завршене докторске дисертације у саставу:

- др Зоран Радојичић, ванр.проф. ФОН-а, ментор;
- др Братислав Петровић, ред.проф. ФОН-а;
- др Душан Старчевић, ред. проф. ФОН-а;
- др Драган Вукумировић, ред. проф.ФОН-а; и
- др Вељко Милутиновић, ред. проф. Електротехничког факултета у Београду.

1.3. Место дисертације у одговарајућој научној области

Докторска дисертација под називом "Статистички модел аутоматизованог управљања дигиталним сертификатима" по предмету истраживања и коришћеној методологији припада техничким наукама, прецизније области информациони системи. Поред тога, дисертација има мултидисциплинарни карактер, јер се обједињују појаве из домена рачунарске статистике, информационо-комуникационих технологија и електронског пословања. Предмет дисертације је заснован на анализи дигиталних сертификата и његовом специфичном појавном облику везаном за електронско окружење.

1.4. Биографски подаци о кандидату

Мр Аца Алексић је рођен 03.10.1957. године у Београду, где је уписао Електротехничку школу "Никола Тесла", усмерење ваздухопловна електроника и завршио са одличним успехом. Студије на Факултету организационих наука уписао је школске 1976/1977. године на кибернетском смеру, а дипломирао је у априлу 1981. године одбраном дипломског рада „Примена табела одлучивања у симулационим моделима" код професора др Бранислава Лазаревића, оцењеним оценом десет (10), са оствареном просечном оценом 8.60 током студија. Континуитет образовања наставио је на последипломским студијама и, након положених испита, пријавио је и одбранио магистарску тезу под насловом "Развој организације и савремене друштвене промене", маја 2005 године, под вођством ментора професора др Живка Дулановића.

Поред горе наведеног образовања похађао је низ курсева и семинара из области менаџмента, информационо – комуникационих технологија, ИСО стандарда, а поседује више сертификата за различите софтверске алате.

Након дипломирања започела је његова радна каријера и то на следећим пословима и задацима:

- Главни инжењер за информатику од 1981. до 1985. године, Техногас;
- Самостални саветник у државним органима од 1985. до 1988 .године, Државна управа Републике Србије;

- Самостални саветник од 1988. до 1994. године, Савезна управа царине СР Југославије;
- Начелник центра за информатику од 1994. до 1997. године, Савезна управа царине СР Југославије;
- Помоћник директора за информатику и наплату прихода од 1997. до 1998. године, Савезна управа царине СР Југославије;
- Начелник управе информатике и аналитике од 1998. до 2002. године, Ресор државне безбедности, Републичког министарства унтрашњих послова Републике Србије;
- Предавач информационих технологија од 2002. до 2003. године, Институт државне безбедности, Министарства унутрашњих послова Републике Србије;
- Саветник директора банке за информационе технологије од јануара до октобра 2003. године, Капитал Банка Београд;
- Саветник председника компаније за информационе технологије од октобра 2003. до 2005. године, Цитроен Србија;
- Директор центра за информатику и електронско пословање од априла 2005. године до октобра 2007. године, Привредне Коморе Србије;
- Секретар удружења информатичке делатности Привредне Коморе Србије од децембра 2005. до октобра 2007. године, Привредне Коморе Србије;
- Начелник службе за информационе и комуникационе технологије у Директорату цивилног ваздухопловства Републике Србије од октобара 2007 до јануара 2010. године;
- Директор сектора за откривање превара у осигурању, спречавање прања новца и финасирање тероризма, у Компанији Дунав Осигурање А.Д. од јануара 2010 године – до августа 2011 године;
- Помоћник генералног директора за информационе технологије, „Дунав РЕ“ од августа 2011 године.

Објавио је у сарадњи са другим ауторима, већи број стручних радова на домаћим и међународним симпозијумима. Био је укључен на изради, развоју, имплементацији и руковођењу следећих пројеката:

- Руководилац пројекта информационог система у Техногасу,
- Руководилац пројекта информационог система у државној управи Републике Србије,
- Руководилац пројекта информационог система Савезне управе царине СР Југославије,
- Руководилац пројекта информационог система, ресора државне безбедности, Министарства унутрашњих послова Републике Србије,
- Руководилац пројекта информационог система банкарског пословања у Капитал банци,
- Руководилац пројекта информационог система Цитроен Србија,

- Руководилац пројекта информационог система портала Привредне коморе Србије,
- Руковдилац пројекта сертификационог тела Привредне коморе Србије и
- Члан управног одбора пројекта, интегрисаног информационог система Дунав РЕ.

1.5. Предмет, циљеви и хипотезе истраживања

Миграција рачунарских окружења ка дистрибуираним, мрежним решењима радикално је променила начин на који компаније реализују пословање. Електронска трговина (*e-commerce*) и електронско пословање (*e-business*) постали су стварност и компаније могу сада пословати користећи електронску размену пословних докумената на глобалном нивоу без посебних тешкоћа. Многе корпорције су унапредиле своје рачунарске мреже и целу комуникациону инфраструктуру у циљу искоришћења свих предности нових система, остварујући бенефиције на основу ниске цене Интернета и његових карактеристика глобалности.

Поред предности, електронска трговина, као и свако решење базирано на отвореним рачунарским мрежама и електронским документима, доноси и нове опасности по интегритет пословног процеса. Овај елеменат има негативан утицај на ширење електронског пословања, јер сва корист која се оствари применом електронске размене може бити елиминисана уколико се не обезбеди адекватна заштита пословног процеса. Ова констатација се посебно односи на критичне апликације као што су финансије, процеси уговарања, пословне тајне, планирање и развој и сл. Стога је стални предмет научног истраживања, развој нових безбедносних система који су намењени да елиминишу наведене ризике и пруже квалитетнију заштиту од оне која је својствена пословању преко папира.

Безбедност корпорацијских података је од изузетног значаја за сваки пословни систем. Информације, интелектуална својина, документација, садржај, мреже, подаци о запосленима и корисницима се могу сматрати делом кључних добара дате корпорације. Сваки од ових елемената треба да буде брижљиво чуван у циљу обезбеђења да пословне тајне једне организације остану поверљиве, што пружа додатне компаративне предности на тржишту.

Криптографски механизми представљају најраспрострањенији начин за остваривање безбедности у отвореним системима и мрежама. У последње време је дефинисан широк дијапазон нових система за заштиту Интернет система, и у већини се користе криптографски механизми заштите. Ове технологије се примењују за различите системе електронске размене као што су заштићено слање порука, заштићени e-mail сервис, системи електронског плаћања, заштита софтверских апликација и мрежних комуникација.

Предмет истраживања дисертације представља истраживање унапређење развоја и увођења дигиталних сертификата, који су усмерени на изградњу одређене инфраструктуре јавних кључева - PKI (*PKI - Public Key Infrustructure*) система, који треба да буде дизајниран, тако да је ефикасан и флексибилан у циљу лаког решавања различитих PKI захтева.

Циљ и задаци који су постављени при изради ове дисертације су:

- Вишеструки системи за регистрацију и доставу сертификата и кључева – потребно је да дати PKI систем подржава различите механизме регистрације и доставе PKI параметара, укључујући: е-маил сервис, web комуникацију, личну доставу, VPN и друго;
- Подршка различитим безбедносним модулима: HSM (HSM - *Hardware Security Module*) као и малим хардверским модулима (токенима) и смарт картицама за ефикасно генерисање дигиталног потписа;
- Подршка примени различитих криптографских алгоритама, како јавних, тако и приватних алгоритама дефинисаних од стране специјализованих дизајнера или самих корисника система;
- Вишеструки системи публикације издатих и повучених сертификата који укључују различите екстерне сервисе (LDAP i X.500), као и публикацију на хард диск у циљу олакшавања интерне публикације;
- Подршка различитим методама провере валидности (повучености) дигиталних сертификата, као што су CRL (*CRL-Certificate Revocation List*), CRL дистрибуционе тачке и OCSP (*OCSP - Online Certificate Status Protocol*), DOSCP (*Distributed OCSP*);
- Подршка вишеструким кључевима и сертификатима по кориснику – политика рада PKI система, и самог Сертификационог тела CA (*CA- Certification Authority*), треба да предвиди коришћење вишеструких кључева и сертификата по кориснику, а да се коришћење ових кључева тако конфигурише да се одвојени кључеви користе за дигитално потписивање и за шифровање (у оквиру дигиталне envelope);
- Подршка комплексним PKI хијерархијама – PKI систем мора подржати хијерархију сертификационих тела (*Root CA* и структура *Intermediate CA* било које дубине), вишеструка регистрациона тела RA *(RA-Registration Authority),* вишеструке операторе RA, и мора подржати процедуру међу-сертификације са другим CA;
- Систем треба да подржи флексибилни ауторизациони процес – сваки захтев за издавањем сертификата може бити ауторизован од стране једне или више овлашћених особа, што треба дефинисати у политици рада CA. Додатно, систем треба да омогући да се захтеви за издавање сертификата процесирају и аутоматски, без потребе за применом специфичне процедуре ауторизације;
- Отвореност система у циљу евентуалних захтева за интероперабилношћу, PKI систем мора задовољавати особину да се базира на отвореним стандардима, од којих је најважнији X.509v3 стандард за формат дигиталног сертификата као и каснији стандарди за конкретну примену и Интернет пословном амбијенту; и
- Изградња модела који се базира на статистичкој анализи ефикасности примене PKI система и дигиталних сертификата. Анализа представља дефинисање потребе пословања PKI у складу са развојем електронских услуга, применом статичких савремених метода ради мерења постигнутих резултата.

Основна хипотеза овог истраживања је да, на основу статистичких метода и анализе доступних реалних података из процеса PKI система, је могуће препознати латентне параметре система, чија би адекватна идентификација и примена квалитативно допринела побољшању процеса управљања дигиталним сертификатима PKI система у електронском пословању.

Додатна хипотеза претпоставља да је могуће извршити аутоматизацију кључних процеса управљања дигиталним сертификатима одабраног PKI система, путем статистичких метода, са циљем да се обједине у одговарајући статистички модел.

У складу са изложеним предметом, циљем и постављеним хипотезама истраживања, садржај дисертације је укратко следећи.

2. ОПИС ДИСЕРТАЦИЈЕ

2.1. Структура и садржај дисертације

Докторска дисертација "Статистички модел аутоматизованог управљања дигиталним сертификатима " се састоји из 9 поглавља. Структура дисертације је следећа:

1. УВОД

1.1. Опис проблема

1.2. Осврт на релевантне библиографске изворе и остварене резултате који су вези с предметом истраживања

1.3. Циљ докторске дисертације

1.4. Полазне хипотезе

1.5. Научне методе истраживања

1.6. Резултати докторске дисертације

1.7. Структура рада

2. СИСТЕМИ СА ЈАВНИМ КЉУЧЕВИМА

2.1. Подршка различитим политикама рада PKI система

2.2. Безбедност

2.3. Скалабилност

2.4. Флексибилност

2.5. Једноставно коришћење

2.6. Отвореност система

3. КОМПОНЕНТЕ PKI СИСТЕМА

3.1. Модули PKI система

3.2. Сертификационо тело (CA)

3.3. Оператор сертификационог тела (CAO)

3.4. Регистрационо тело (RA)

3.5. Оператор регистрационог тела (RAO)

3.6. Сервер за архивирање кључева

2.2. Кратак приказ појединачних поглавља

У уводном поглављу најпре се описују предмет и циљ истраживања, и наводе се хипотезе, а затим се даје садржај и опис дисертације по поглављима.

Друго поглавље разматра општи аспект функционисања инфраструктуре јавних кључева - PKI (*PKI - Public Key Infrustructure*) који је комплексан систем, који се састоји од: Криптографских технологија, протокола, стандарда, политика, процедура, сервиса и апликација. PKI систем представља основу за примену решења заштите електронских података, којим се обезбеђује тајност података, аутентитификација, интегритет и непорицивост. Основни концепт на коме се заснива PKI систем је асиметрична криптографија или криптографија јавних криптографских кључева (*Public Key Cryptography*).

У трећем делу дисертације су најважније компоненте PKI система: сертификационо тело – CA (*CA- Certification Authority*), регистрационо тело - RA (*RA-Registration Authority*), јавни именик (*PublicDirectory*) и корисничке апликације. Сертификационо тело извршава следеће послове: Издавање, обнављање, суспендовање и опозивање дигиталних сертификата (*digital certificate*) конфигурисање различитих врста, животног циклуса и других параметра сертификата, објављивање опозваних сертификата –CRL (*Certificate Revocation List*), узајамна сертификација са другим сертификационим телима и друго. Регистрационо тело представља спону између корисника који постављају захтеве за издавањем сертификата и сертификационог тела. Послови регистрационог тела су: прихватање захтева корисника за издавањем сертификата, проверавање идентитета корисника и прикупљање потребних података и посредовање захтева корисника за издавањем сертификата ка сертификационом телу. Јавни именик је локација на којој се чувају дигитални сертификати,тј. јавни криптографски кључеви за шифровање и верификовање потписаних докумената. Посредством јавних именика PKI систем обезбеђује дистрибуцију сертификата корисницима. Корисничке апликације омогућавају корисницима да употребом дигиталних сертификата врше шифровање/дешифровање докумената и потписивање/версификовање потписаних докумената.

У четвртом делу дисертације описане су активности симетричне и асиметричне криптографије и образложено коришћење криптографских кључева приликом шифровања/дешифровања докумената и приликом потписивања/версификовања потписаних докумената. Осим тога, представљени су различити начини за размену јавних криптографских кључева по дигиталних сертификата. У оквиру сертификата се налазе јавни криптографски кључеви, тако да се разменом сертификата размењују јавни криптографски кључеви. Зато је најбољи начин за успешну реализацију PKI система, иницирање пилот – пројекта, који ће брзо, релативно јефтино и аргументовано, да покаже предности и евентуалне недостатке у постојећој пракси.

У петом делу приказане су статистичке методе у функцији изградње статистичког модела ради спровођења процеса аутоматизације управљања. На основу методе статистичког закључивања, индуктивног и дедуктивног, модел омогућава научну обраду статистичких података и доношење закључака на бази таквих резултата. Статистички модел омогућава да се дају одговори на деловање система, тј. да се на основу измерених резултата, донесе закључак и о ономе што није измерено, те спроведе понашање система у правцу заштите од неауторизованог приступа. Ради изналажења одговарајућих анализа, ради изградње модела, коришћене су методе експлораторне анализе, методе мултиваријационе анализе и data mininga.

Правилна примена модела је хеуристичко питање, као што су важан избор теорија, хипотеза, метода индикатора и других елемената научног истраживања. Стога се статистичка анализа третира као моделирање података тј. њихових латентних својстава и односа.

Добра теоријска основа изведена је из формалних аксиома, јер само у том случају представља потпун дедуктивни систем, а својства која предвиђа могу се израчунати. То је правило свих формалних система и оно не подразумева да је теоријски модел тачан. Тачност таквих модела проверава се било кроз анализу унутрашње усаглашености, било кроз анализу усаглашености са реалним светом. За анализу усаглашености са реалним светом постављене су емпиријске хипотезе које се проверавају помоћу података – где се статистика намеће као инструмент.

Статистичка контрола процеса представља методу за прикупљање и анализу података, која се примењује у циљу решавања практичних проблема контроле квалитета процеса. Статистичка контрола процеса своди се на приказивање узорака у облику контролних тачака на контролној карти, са границама које су претходно одређене.

Шест Сигма је организован и систематичан метод за стратешко унапређење пословних процеса (као и развој нових производа и услуга), који се конципира на статистичким методама и константно смањује број дефектних производа/услуга. Програми континуалног побољшавања као што је Шест Сигма (*Six Sigma*) се најчешће имплементирају на два нивоа – кроз пројекат и кроз организацију. Суштина Шест Сигма пројеката је смањивање варијансе процеса. Конкретно, Шест Сигма тежи редукцији и контроли варијансе процеса у тој мери да иако излаз варира до $\pm 6\sigma$, он је у потпуности повинован доњој и горњој граници спецификације. Шест Сигма програми успостављају иницијативу за континуално побољшање перформанси организационих система – раст ефикасности и модификовање процеса у складу за жељама наших клијената.

Дискриминациона анализа је често коришћен алат у статистици. Заснива се на креирању модела који омогућује да се одреди модел који за вредности интервалних променљивих (задатих атрибута неке појаве) одређује припадност групи. Да би се добио добар модел, представљен дискриминационом функцијом, потребно је да улазни подаци садрже поред вредности атрибута и припадност групи. Са техничке стране основни циљ дискриминационе анализе је формирање линеарних комбинација независних променљивих којима ће се дискримнација између унапред дефинисаних група тако извршити да грешка погрешне класификације опсервација буде минимизирана, или другачије речено, да се максимизира релативан однос варијанси између и унутар група. Линарном комбинацијом независних променљивих за сваког испитаника или објекат одређује се број, дискриминациони скор, који се затим трансформише у апостериорну вероватноћу да испитаник или објекат потиче из једне од група.

У шестом делу дисертације представљено је и описано емпиријско истраживање о примени дигиталних сертификата. Основу истраживања чини апликативни модел, презентован програм, који омогућује упоредни преглед резултата добијених применом класичног и новог приступа дискриминационој анализи. Обе анализе обрађују исте улазне скупове података.

У седмом делу докторске дисертације, у студији примера, извршена је анализа, излазних резултата који су добијени применом технике *Soft Computing*–а, који пружају

бољи увид у посматрану појаву, јер су у анализи укључене и логичке комбинације атрибута, а не само атрибути, као што то чини класичан приступ.

На крају је дат закључак рада са одговором на питања у вези са постављеним циљем и хипотезама. Дата је систематизација и преглед научних доприноса који су проистекли из рада на докторској дисертацији, скуп отворених проблема и могућности за даљи рад у области докторске дисертације. Литература коришћена приликом израде докторске дисертације садржи релеватне радове других истрживача.

3. ОЦЕНА ДИСЕРТАЦИЈЕ

3.1. Савременост, оригиналност, значај

Предмет дисертације обухвата актуелне области истраживања дигиталних сертификата и PKI система. Велики број научних и стручних часописа, конференција, књига, Интернет ресурса и велика заинтересованост универзитета, школа и компанија, показују актуелност теме докторске дисертације.

Докторска дисертација детаљно приказује досадашња истраживања и сазнања из области дигиталних сертификата. Описани су елементи који чине компоненте PKI система. Реализовано је апликативно решење које представља апликативни модел презентован програм, који омогућује упоредни преглед резултата добијених применом класичног и новог приступа дискриминационој анализи.

На основу изложеног, може се закључити да докторска дисертација доноси новине у односу на постојеће стање и отвара простор за даља истраживања.

3.2. Осврт на референтну и коришћену литературу

Последњих година вршена су интензивна истраживања у вези примене квалификованих дигиталних сертификата у електронском пословању. Многобројни резултати публиковани су у часописима, презентовани на разним конференцијама и од стране водећих светских софтверских компанија.

Кандидат је у докторској дисертацији користио савремену и релевантну литературу. Укупно је навео 126 референци, које обухватају најзначајније ауторе из ове области, радове из научних часописа и конференција у којима су представљени резултати који су релевантни са темом дисертације. Литература обухвата радове од старијих до савремених како би се критички осврнуло на развој дигиталних сертификата, његове предности и ограничења и његова примена у електронском пословању.

3.3. Анализа примењених научних метода и њихова адекватност за спроведено истраживање

Ради тестирања постављених хипотеза у току израде дисертације примењен је већи број научних метода од систематског прегледа стања у области истраживања са адекватним класификацијама проблема, приступа, метода и техника и навођењем литературе, затим анализе постојећих резултата и закључивање са предикцијом будућих праваца развоја. У изради дисертације коришћене су следеће научне методе:

- У првом делу дисертације (поглавља 1, 2, 3) коришћене су методе прикупљања и анализе постојећих научних резултата и достигнућа.
- У четвртом и петом поглављу, коришћене су методе и технике унапређења дигиталних сертификата ради изградње апликативног модела електронског пословања.
- У шестом поглављу урађена је студија случаја, где су прикупљени резултати обрађени статистичким методама. Апликативно решење омогућава статистичко праћење података који представљају појединачну и збирну опсервацију клијената, праћену кроз време трајања посматрања и вредности параметра који се прати.

Резултати истраживања су презентовани текстуално, описивањем, и кроз више табела, слика и дијаграма са упоредним резултатима. Истраживање је интердисциплинарно, јер укључује научне дисциплине: рачунарску статистику, информатиционо-комуникационе технологије и електронско пословање.

На основу анализе докторске дисертације, може се закључити да примењене научне методе и технике одговарају, по свом значају и структури, теми дисертације и спроведеном истраживању.

3.4. Оцена применљивости и верификације научних резултата

Резултати докторске дисертације могу имати широку практичну примену у пословним системима. Дигитални сертификати треба да учине пословање ближе корисницима електронских сервиса, утичу на модернизацију и побољшање квалитета услуга, побољшање ефикасности, транспаретности и ефективности рада.

За равој дигиталних сертификата пресудне су информације, јер пружају податке на основу којих корисници електронских сервиса, доносе ефикасније и ефективније одлуке и самим тим повећавају степен задовољства живота.

Апликациони модел представља примену дигиталних сертификата, где су дефинисне активности које имају стратешку улогу у унапређењу електронског пословања, одређивању степена значаја активности и мерења ефекта његове примене. На оваквом апликативно модулу уз примену статистчких анализа дошло се до циљне архитектуре PKI система, који је дао најбоље резулате у практичној примени савременим пословним окружењима.

Тиме је остварена верификација теоријских поставки и добијених резултата који су изнесени у дисертацији.

3.5. Оцена способности кандидата за самостални научни рад

У току израде докторске дисертације, мр Аца Алексић је показо способност да сагледа проблем истраживања са више аспеката и да креативно приступи његовом решавању. Уочио је главне недостатке и проблеме постојећих решења из области дигиталних сертификата и конципирао и спровео истраживања са циљем да се превазиђу.

Свеобухватни и систематизовани преглед стања у области потврђује способност кандидата за откривање и сагледавање отворених проблема истраживања као и критичку анализу постојећих сазнања у области.

На крају, резултати студије случаја, који су приказани у дисертацији и објављени у зборницима радова научних скупова и у научним часописима, указује на свест кандидата о неопходној строгој верификацији резултата научног истраживања.

На основу наведеног, сматрамо да кандидат мр Аца Алексић поседује потребно знање и искуство за самосталан научни рад.

4. ОСТВАРЕН НАУЧНИ ДОПРИНОС

4.1. Приказ остварених научних доприноса

Најважнији резултат истраживања у оквиру ове докторске дисертације је развој статистичког модела за управљање дигиталним сертификатима. Развијени модел је прилагођен за примену у условима информационо комуникационих технологија у Србији и зато има велику употребну вредност и представља значајан научни резултат.

Истраживањем, које је спроведено за израду докторске дисертације, даје се научни и стручни допринос.

Научни допринос се огледа у систематизацији сазнања до којих се дошло симулацијом кроз имплементирани сегмент дигиталних сертификата. Потреба за применом квалификованих дигиталних сертификата у Републици Србији се огледа у његовом све већем афирмисању, као и у интензивном развоју елктронских сервиса у електронском пословању. У домаћој литератури ова област није заступљена у довољној мери, па обрада ове теме са теоријског аспекта представља још један допринос ове дисертације.

Као што је већ речено, PKI системи, представљају комбинацију хардверских и софтверских елемената за реализацију функција система са применом јавних кључева, као и правила, процедуре и институције надлежне за њихову примену. Основна функција PKI система је поуздано успостављање дигиталног идентитета свих овлашћених корисника датог информационог система, специфицираног у облику дигиталног сертификата.

Функционалне целине PKI система треба да обезбеде:

- Поверење у једнозначну везу између идентитета овлашћеног субјекта CA и јавног кључа који му је додељен – што се постиже механизмом дигиталног сертификата кога ће потписати CA,
- Највиши криптолошки квалитет јавних и тајних кључева за асиметричне криптографске алгоритме, као и кључева за симетричне криптографске алгоритме,
- Највишу безбедност CA које издаје дигиталне сертификате и опционо.

Задатак ове дисертације био је да представи предности једне од техника *Soft Computing*–а, [0,1]-вредносне логике у односу на класичну {0,1}-вредносну логику, кроз употребу статистичког алата за дискриминациону анализу.

Идеја да се проширењем класичног приступа {0,1}-вредносне логике на [0,1]-вредносну логику и применом истог статистичког апарата могу добити доста бољи резултати представљала је суштину овог рада. Показало се да неки проблеми нису били решиви класичним приступом, док су решења добијена новим приступом бивала не само квалитетнија, већ и са малим процентом грешке.

Стручни допринос у докторској дисертацији се огледа у апликативном решењу. Програм је написан применом алата "*The MathWorks MATLAB*®" и омогућује упоредни преглед резултата добијених применом класичног {0,1} вредносног приступа и новог [0,1] вредносног приступа дискриминационој анализи.

Развијени програм омогућује упоредни преглед резултата добијених применом класичног и новог приступа дискриминационој анализи. Обе анализе обрађивале су исте улазне скупове података. Излазни резултати добијени применом технике *Soft Computing*–а пружају бољи увид у посматрану појаву, јер у анализу укључују и логичке комбинације атрибута, а не само атрибуте, као што то чини класичан приступ.

4.2. Критичка анализа резултата истраживања

Дигитални сертификати постављају темеље новом приступу организовања пословних процеса, где су, детаљно су описане основне карактеристике система за примену јавних кључева (PKI систем) и функције CA, као и начин њихове реализације. Истакнути су концептуални ставови, описани су међународни стандарди који се користе и приказане су основне карактеристике архитектуре једног сопствено реализованог софтверско-хардверског система за генерисање криптографских кључева, производњу дигиталних сертификата и персонализацију меморијских медијума или *smart* картица, тј. система за потпуну подршку рада PKI система као једног могућег предлога за реализацију CA .

Сертификационо тело (CA – *Certification Authority*) представља највишу тачку поверења у читавом PKI систему. Основни задатак CA је да процедуром дигиталног потписа на бази асиметричног криптографског алгоритма и свог тајног кључа, који мора бити најстроже чувана тајна, гарантује везу између јавног кључа и идентитета одређеног субјекта за потребе електронске размене података у оквиру информациног система. Сваки субјекат има могућност да верификује дигитални потпис CA, на бази јавног кључа асиметричног криптографског алгоритма CA, који је познат свим корисницима.

CA издаје дигиталне сертификате на основу захтева за учешће у електронској размени података у информационом систему, које субјекти подносе у регистрационим телима (RA) или директно преко *web* портала CA, путем *http* комуникације. Дигитални сертификати су у форми, прописаној стандардом ITU-T X.509 v3. RA је одговорно за управљање базом података свих издатих сертификата и те информације су доступне свим субјектима. Читав садржај дигиталног сертификата се потписује асиметричним криптографским алгоритмом са тајним кључем CA и добијени дигитални потпис се прикључује садржају сертификата. Полазна претпоставка која се заснива на дефинисању и развијању активности дигиталних сертификата и његовог специфичног облика везаног за електронско окружење, ради његовог развоја и примене. Тиме је приказан нови приступ у начину пружања електронских услуга.

Овом докторском дисертацијом није завршено истраживање утицаја квалификованог електронског сертификата, већ се проширују видици којима се ствара основа за изградњу статистичког модела у он-лајн окружењу. Овој проблематици се мора приступати са нарочитом пажњом око сигурности и аутентичности података који се размењују електронским путем. На ова питања национална тела покушавају да нађу оптималне одговоре, кроз доношење правних аката, у складу са Директивом Европске уније о електронским потписима и Законом о електронском пословању и електронском потпису, и треба да буде акредитовано од стране надлежног органа задуженог за послове акредитације сертификационих тела.

4.3. Очекивана примена резултата у пракси

С обзиром на актуелност теме и чињеницу да светски трендови у развоју и примени техника заштите информационих система и савремених криптографских протокола су у све већој примени PKI система и безбедносних механизама базираних на смарт картицама, чине елементе система електронског пословања, или планира да се уведе, може се закључити да су могућности примене резултата истраживања из дисертације велике.

Приказани резултати имати практичну примену тако што ће бити коришћени као теоријска основа за даља истраживања.

4.4. Списак објављених радова

Аутор дисертације има објављених укупно 9 радова. Списак радова дат је у Прилогу 1, а овде издвајамо следеће, који су значајни непосредни резултати рада на докторској дисертацији:

1. Миленковић Д., Јовановић Миленковић М., Вујин В., Алексић А., Радојичић З., „Electronic health system and its introduction into the health system of the Republic of Serbia“, Војносанитетски преглед, Београд, 2011, ISSN 0042-8450, ИФ=0.199
2. Јеремић В., Секе К., Радојичић З., Јеремић Д., Марковић А., Словић Д., Алексић А., „Measuring health of countriers;a novel approach“, HealthMED, Vo.5, No.6, Novembar 2011, ISSN 1840-2291, ИФ=0.331
3. Атанасијевић С., Алексић А., Живановић В., Атанасијевић Т., „Мобилне технологије у функцији сервиса привреде: WAP сервиси за регистрацију привредних субјеката у информационом систему привредне коморе, IV форум регионалних привредних комора SEFICT, Дубровник, 2006.
4. Атанасијевић С., Алексић А., Мирчић Н., Атанасијевић Т., „Архитектура информационих подсистема за анектирање и анализу привредних субјеката“, Десети конгрес JISA, 2006, Херцег Нови, 2006.

5. ЗАКЉУЧАК И ПРЕДЛОГ

Докторска дисертација "Статистички модел аутоматизованог управљања дигиталних сертификата" представља савремен и оригиналан допринос научном сазнању из области информационих система, рачунарске статистике и електронског пословања.

Главне карактеристике новог приступа су најквалитетнија криптографска решења која се примењују у савременим рачунарским мрежама базирају се на примени симетричних криптографских система за заштиту тајности, технологије дигиталних потписа на бази асиметричних криптографских сертификата и хардверских модула уз коришћење савремених статистичких метода.

Применом резултата из ове дисертације, корпорације могу побољшати услове рада, реализовати пословне активности на ефикаснији и квалитетнији начин, омогућити бољу сарадњу и комуникацију учесника у електронском пословању.

С обзиром на постигнуте резултате, актуелност и мултидисциплинарност обрађене теме, ова дисертација задовољава највише критеријуме и показује способност мр Аце Алексића за научно-истраживачки рад.

На основу наведеног, Комисија предлаже Наставно-научном већу да донесе одлуку о прихватању овог извештаја и заказивању јавне одбране докторске дисертације.

Комисија за преглед и оцену рада

_____

др Зоран Радојичић, ванр. проф.
Факултет организационих наука, Београд

_____

др Братислав Петровић, ред. проф.
Факултет организационих наука, Београд

_____

др Драган Вукумировић, ред. проф.
Факултет организационих наука, Београд

_____

др Душан Старчевић, ред. проф.
Факултет организационих наука, Београд

_____

др Вељко Милутиновић, ред. проф.
Електротехнички факултет, Београд

Прилог 1.

Списак објављених радова Аце Алексића

Радови објављени у научним часописима

1. Миленковић Д., Јовановић Миленковић М., Вујин В., Алексић А., Радојичић З., „Electronic health system and its introduction into the health system of the Republic of Serbia“, Војносанитетски преглед, Београд, 2011, ISSN 0042-8450, ИФ=0.199
2. Јеремић В., Секе К., Радојичић З., Јеремић Д., Марковић А., Словић Д., Алексић А., „Measuring health of countriers;a novel approach“, HealthMED, Vo.5, No.6, Novembar 2011, ISSN 1840-2291, ИФ=0.331

Списак објављених радова од националног значаја штампаних у целини

1. Атанасијевић С., Алексић А., Живановић В., Атанасијевић Т., „Мобилне технологије у функцији сервиса привреде: WAP сервиси за регистрацију привредних субјеката у информационом систему привредне коморе, ИВ форум регионалних привредних комора SEFICT, Дубровник, 2006.
2. Атанасијевић С., Алексић А., Мирчић Н., Атанасијевић Т., „Архитектура информационих подсистема за анектирање и анализу привредних субјеката“, Десети конгрес ЈИСА, 2006, Херцег Нови, 2006.
3. Атанасијевић С., Алексић А., Живановић В.,Мирчић Н.,Атанасијевић Т., „WEB сервис за анкетирање и анализу потреба привредних субјеката – архитектура новог информационог система привредне коморе“, Једанести фестивал информатичких достигнућа, INFOFEST, Будва, 2006.
4. Бердић Д., Миленковић М.,Алексић А., „Реализација VPN мреже јединственог коморског система Србије“, Једанести фестивал информатичких достигнућа, INFOFEST 2006, Будва 2006.
5. Атанасијевић С., Алексић А., Војиновић Ђ., Атанасијевић В., „Савремени интернет сервиси за подршку у грађевинарст ву на порталу привредне коморе Србије“, Симпозијум о операционим истраживањима SYMOPIS 2006, Бања Ковиљача, 2006.
6. Атанасијевић С., Алексић А., Војиновић Ђ., Атанасијевић В., „Портал Српске привреде“, Систем научних, технолошких и пословних информација SNTPI 2006, Фрушка Гора, 2006.
7. Јовановић В., Алексић А., „Примена табела одлучивања у симулационим моделима“, Симпозијум о операционим истраживањима, SYMOPIS 1981, ФОН, Херцег Нови, 1981.

Прилог 2

Подаци о радовима се могу видети на адреси

ВОЈНОСАНИТЕТСКИ ПРЕГЛЕД
ВОЈНОМЕДИЦИНСКА АКАДЕМИЈА
Црнотравска 17, 11000 **Београд, Србија**
Тел/факс: +381 11 2669689
vsp@vma.mod.gov.rs
vmavsp@hotmail.com

ПОТВРДА

Овим се потврђује да је рад под насловом:

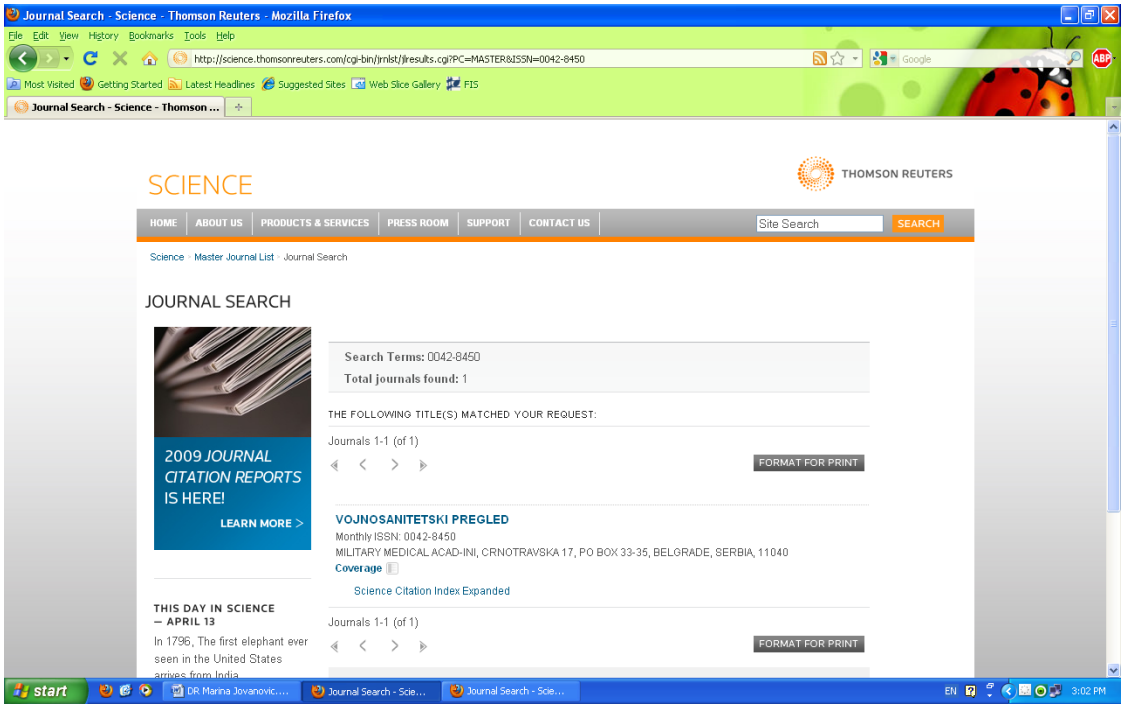
Electronic health system and its introduction into the health system of the Republic of Serbia

А у т о р а : Dejan Milenković, Marina Jovanović Milenković, Vladimir Vujin, Aca Aleksić, Zoran Radojičić

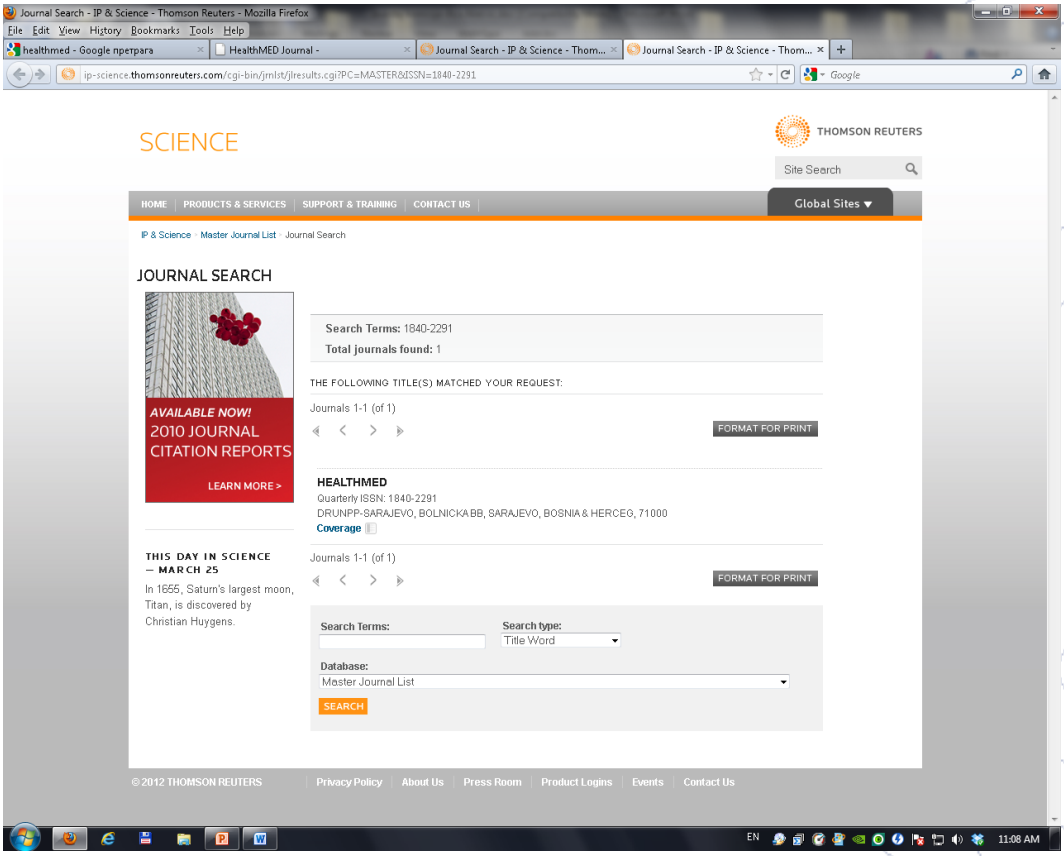
прихваћен за штампу у *Војносанитетском прегледу* и биће објављен у једном од наредних бројева.

05.04 .2011.

Главни и одговорни уредник
Проф. dr sc. pharm.
Силва Добрић



http://science.thomsonreuters.com/cgi-bin/jrnlst/jlresults.cgi?PC=MASTER&ISSN=0042-8450



http://ip-science.thomsonreuters.com/cgi-bin/jrnlst/jlresults.cgi?PC=MASTER&ISSN=1840-2291