4-157/122
27-10-2022.

UNIVERZITET SINGIDUNUM
Departman za poslediplomske studije
Danijelova 32, Beograd

VEĆU DEPARTMANA ZA POSLEDIPLOMSKE STUDIJE

Odlukom Veća Departmana za poslediplomske studije broj _4 - 169/2019_ od 12.07.2019. godine, određeni smo za članove Komisije za ocenu i odbranu doktorske disertacije kandidata Jelene Gavrilović pod nazivom „Jedna klasa sistema za generisanje i distribuciju kriptoloških ključeva zasnovana na više biometrijskih modaliteta"

o čemu podnosimo sledeći

IZVEŠTAJ

1. Osnovni podaci o kandidatu i doktorskoj disertaciji

Jelena Gavrilović rođena je 6. juna u Valjevu. Osnovnu školu završila u Valjevu. Srednju tehničku PTT školu u Beogradu, završila je 2002. godine na smeru Telekomunikacije. Osnovne studije je pohađala na Visokoj školi elektrotehnike i računarstva i na Fakultetu za informatiku i računarstvo Univerziteta Singidunum. Master studije na studijskom programu Savremene informacione tehnologije završava 2011. godine stiče zvanje master informatičar. Student doktorskih studija na studijskom programu Napredni sistemi zaštite.

Zaposlena je na Univerzitetu Singidunum kao asistent u nastavi, uža naučna oblast: Informatika i računarstvo, za predmete iz oblasti matematike i računarskih nauka.

Kandidat ima objavljene sledeće radove, čime je ispunjen preduslov za odbranu doktorske disertacije:

Radovi objavljeni u kategoriji M23:

1. N.Maček, B.Đorđević, J. Gavrilović, K.Lalović, An Approach to Robust Biometric Key Generation System Design, Acta Polytechnica Hungarica, Vol. 12, No. 8, pp. 43 - 60, Dec, 2015

Ostali objavljeni radovi u časopisima

1. J. Gavrilovic, M. Stanković, M. Tanasković. A Ćuk „Analysis of Available Data and Parameters in the Process of Forensics of Unmanned Aerial Vehicles" Journal of Mechatronics, Automation and Identification Technology, Vol. 7, No.1 , pp. 8-11 ,2022.
2. A. Savić, J. Gavrilović, I. Kostić-Kovačević, Free software for learning mathematics, International Journal of Science, Innovation and New Technology, Vol. 1, No. 3, pp. 1 - 7, Feb, 2012
3. M. Živić, J. Gavrilović, A. Njeguš, Informatička znanja i veštine kao resurs ekonomskog rasta i konkurentnosti, Singidunum revija, Vol. 8, No. 1, pp. 153 - 162, Mar, 2011
4. I. Kostić-Kovačević, J. Gavrilović, Visualization of Mathematics through incorporation of educational software into distance learning, Metalurgia International, Vol. 8, No. 9, pp. 178 - 181, Sep, 2013

Radovi na konferencijama:

1. A. Ćuk, J. Gavrilović, M. Tanasković, M. Stanković, "Mobile Robot Path Planning Optimization by Artificial Bee Colony," in Sinteza 2022 – International Scientific Conference on Information Technology and Data Related Research, Belgrade, Singidunum University, Serbia, pp. 399-403, 2022.
2. J. Gavrilović, M. Tanasković, M. Stanković, A. Ćuk, Forenzička analiza komercijalnih dronova, Zbornik konferencije, pp. 88 - 91, Mar, 2022
3. D. Đurović, J. Gavrilović, I. Kostić-Kovačević, B. Kovačević, A new adaptive robustified prediction algorithm with unknown noise statistics, Conference proceedings IcETRAN, Jun, 2014
4. D. Golijanin, M. Miljković, S. Alčaković, J. Gavrilović, M. Savković, D. Stamenković, Generacija Z, internet i obrazovanje, 1st International Scientific Conference of IT and Business-Related Research SYNTHESIS 2014, Belgrade, Serbia, pp. 506 - 509, Apr, 2014
5. Kostić-Kovačević, D. Lukač, J. Gavrilović, D. Đurović, Obrazovni alati u nastavi matematike, Zbornik radova Međunarodne naučne konferencije Univerziteta Singidunum, Uticaj interneta na poslovanje u Srbiji i svetu, Sinteza 2014, pp. 340 - 344, Apr, 2014
6. L. Barjaktarović, J. Stanković, J. Gavrilović, The Role of Internet Technologies in Lecturing and Learning, Zbornik radova Međunarodne naučne konferencije Univerziteta Singidunum, Uticaj interneta na poslovanje u Srbiji i svetu, Sinteza 2014, pp. 397 - 401, Apr, 2014
7. D. Đurović, I. Kostić-Kovačević, J. Gavrilović, S. Golubović, Dva metoda za pripremu oštećenih dokumenata u cilju optičkog prepoznavanja karaktera, Zbornik radova, Mar, 2014

8. Kostić-Kovačević, J. Gavrilović, A. Savić, Jedno rešenje edukativnog modela nastave matematike realizovanog upotrebom obrazovnih alata, Zbornik radova Simpozijuma Infoteh Jahorina, Mar, 2014
9. Savić, J. Gavrilović, I. Kostić-Kovačević, Interactivity In Teaching Shown Through The Use Of Information Technology, Oct, 2013
10. J. Gavrilović, A. Savić, I. Kostić-Kovačević, Teaching of mathematics through different mediums of knowledge transfer, Sep, 2013
11. J. Gavrilović, I. Kostić-Kovačević, Komparativna analiza primenjenih edukativnih metoda u nastavi matematika, Zbornik 57. konferencije ETRAN, Zlatibor 3-6. juna 2013., pp. RT 2.1. 1 - 4, Jun, 2013
12. J. Stanković, J. Gavrilović, Jedno rešenje modela za učenje na daljinu prilagođeno studentima ekonomskog profila, mar, 2013
13. I Kostić-Kovačević, J. Gavrilović, A. Savić, Osavremenjavanje nastave matematike kroz interaktivnost, INFOTEH-JAHORINA Vol. 12, March 2013., pp. 776 - 779, Mar, 2013
14. A. Savić, J. Gavrilović, I. Kostić-Kovačević, Methods of teaching mathematics, Aug, 2012
15. Kostić-Kovačević, J. Gavrilović, Inkorporiranje obrazovnih softvera za dinamičku matematiku u sistem za učenje na daljinu, Zbornik radova, pp. 780 - 783, Mar, 2012
16. Kostić-Kovačević, J. Gavrilović, Primena matematičkih obrazovnih alata u nastavnom procesu, Zbornik radova, Mar, 2012
17. M. Savković, J. Gavrilović, Elektronski servisi kao podrška radu univerzitetskog karijernog centra, Zbornik radova Infotech Jahorina 2012, pp. 571 - 574, Feb, 2012
18. J. Gavrilović, I. Kostić-Kovačević, Use of non-commercial software in mathematics, Conference processing, pp. 2-36 - 2-42, Sep, 2011
19. J. Gavrilović, I. Kostić-Kovačević, A. Savić, Mathematical education materials development approach for distance learning systems, Conference Processing, pp. 111 - 116, Aug, 2011
20. J. Gavrilović, M. Šarac, B. Čavić, I. Kostić-Kovačević, Realizacija učenja na daljinu na Univerzitetu Singidunum, Zbornik radova, Jun, 2011
21. N. Stanić, J. Gavrilović, Komparativna analiza različitih sistema za učenje na daljinu, Zbornik radova, Mar, 2011

Doktorska disertacija kandidata Jelene Gavrilović je urađena na ukupno 144 strana, od čega 7 strana čini spisak literature. Spisak literature obuhvata 80 referenci koje čine naučni radovi, knjige, zbornici radova, zakonski propisi kao i elektronski izvori. Uz osnovni tekst disertacija sadrži i 31 sliku i grafikona i 4 tabele.

Doktorska disertacija kandidata Jelene Gavrilović je bila podvrgnuta proveri softverom za ustanovljavanje preklapanja/plagijarizma (iThenticate Plagiarism Detection Software). *Ukupan procentualni iznos zapaženih preklapanja iznosi 4% disertacije.*

2. Predmet i cilj istraživanja

Disertacija sadrži pregled i analizu različitih naučnih istraživanja u oblasti generisanja kriptoloških ključeva, biometrije i biometrijskih sistema. Na osnovu postojećih naučnih saznanja objavljenim u prestižnim naučnim časopisima dat je predlog radnog okvira zasnovanog na novoj metodi primene više biometrijskih modaliteta.

Naučni cilj ove disertacije i istraživanja obrađenog u okviru iste ogleda se u novoj metodi primene postojećih modaliteta čime je autor dao doprinos u procesu razvoja kriptološke bezbednosti i biometrijske kriptografije.

Praktični cilj predloženog sistema je generisanje i distribucija kvalitetnih kriptoloških ključeva dovoljnih dužina za primenu u standardizovanim mehanizmima 21. veka na osnovu više biometrijskih modaliteta

Društveni cilj ovog istraživanja je pomoć organizacijama različitih delatnosti (vlade zemalja, vojska, bezbednosne službe, veliki privredni subjekti) koje imaju neizostavnu potrebu za zaštitom važnih informacija.

3. Hipotetički okvir istraživanja

U okviru disertacije postavljene su : Opšta hipoteza, Posebna hipoteza kao i pojedinačne hipoteze.

Opšta hipoteza od koje je i sam proces istraživanja u disertaciji počeo je: „Biometrijski izvori informacija su dovoljno kvalitetni za sintezu sistema iz domena biometrijske kriptografije a u svrhu generisanja i distribucije kriptoloških ključeva"

Posebna hipoteza proistekla iz opšte je sledeća: „Kombinovanjem više biometrijskih modaliteta moguće je poboljšati performanse navedenog sistema i učiniti njegov rad pouzdanijim i bezbednijim".

Pojedinačne hipoteze koje su korišćene i testirane u samoj disertaciji su:

- kvalitet kriptoloških ključeva je značajno bolji u informaciono-teorijskom smislu (Šenonova entropija, skup NIST statističkih testova za kontrolu slučajnosti generisanih nizova, na osnovu pseudoslučajnih generatora);
- izborom dobre strategije fuzije moguće je razviti sistem visokih performansi;
- već poznate odnosno postojeće metode napada na biometrijske sisteme se upotrebom predloženog rešenja, mogu sprečiti. Ukoliko se napad ne može sprečiti predloženo rešenje treba da smanji mogućnosti izvođenja odnosno da umanji efekte samih napada;
- koriste se poznate procene ostvarenog nivoa sigurnosti;

- na robusnost sistema ne utiče broj korisnika koji će koristiti sistem;
- vrste biometrijskih osobina koje je potrebno steći su već poznate i teorijski dokazive da predstavljaju reprezentativni biometrijski uzorak;
- upotreba poznatih i naučno dokazanih metoda u procesu integracije i obrade korišćenih informacija i
- dato rešenje predstavlja kompromis između troškova razvoja i performansi sistema.

4. Metodologija istraživanja

Istraživanje je sprovedeno upotrebom dostupnih saznanja iz ove oblasti, bilo da se radilo o prikupljanju informacija putem literature dostupne putem štampanih i relevantnih online izvora, poput radova objavljenih u časopisima i zbornicima relevantnih naučnih konferencija, sa željom da se analizom postojećeg stanja u ovoj oblasti postave smernice za dalji razvoj u domenu biometrije, kriptografije i kripto biometrijskih sistema .

Od naučnih metoda koristila se:

- analitičko-deduktivna metoda,
- hipotetičko-deduktivna,
- uporedna i komparativna metoda i
- eksperimentalna metoda ispitivanja.

Prikupljanje i analiza podataka izvršena je:

- postavljanjem kriterijuma za poređenje i klasifikaciju,
- poređenjem prikupljenih podataka,
- utvrđivanjem relevantnih činjenica i veza među podacima,
- preispitivanjem hipoteza,
- testiranjem i proverom zaključaka do kojih smo došli i
- postavljanjem budućih ciljeva.

5. Kratak prikaz sadržaja doktorske disertacije

Proces naučnog istraživanja je podeljen u nekoliko koraka

1) Uvod;

2) Pregled u oblasti istraživanja;

3) Generisanje i distribucija kriptoloških ključeva;

4) Pojam i definicije biometrije;

5) Predlog sistema za generisanje kriptoloških ključeva na osnovu više biometrijskih modaliteta;

6) Zaključak i predlozi za budući rad

U uvodnom delu navedeni su osnovni motivi i opšta razmatranja za razvoj nove klase sistema koja će značajno unaprediti performanse postojećih sistema za jednim biometrijskim modalitetom. Detaljno će biti obrazložen predmet istraživanja, očekivani doprinosi i struktura disertacije.

U drugom delu razmatramo opšte stanje u oblasti istraživanja, na osnovu najnovijih naučnih saznanja vezanih za ove dve klase biometrijskih sistema. Uočavamo nedostatke postojećih višemodalnih biometrijskih sistema, kako bi preciznije istakli doprinose ovog rada.

U trećem delu rada obrazložene su teorijske osnove istraživanja. Primena teorije informacije u proceni kvaliteta biometrijskog izvora informacije.

U četvrtom delu definisani su osnovi pojmovi biometrije i biometrijskih sistema. Opisana je primena različitih strategija fuzije za kombinovanje više biometrijskih izvora. Principi donošenja odluke u slučaju primene u servisima autentifikacije ili provere regenerisanih ključeva u kriptografskim svrhama. Bezbednosni aspekti sistema za generisanje i distribuciju ključeva iz domena biometrijske kriptografije.

U petom delu rada predstavljena je predloženu šemu biometrijskog sistema koji koristi više biometrijskih modaliteta u svrhu generisanja kvalitetnih kriptoloških ključeva dovoljnih dužina za primenu u kriptografskim šiframa u 21 veku. Analizu pojedinačnih komponenti sistema za merenjem performansi koji će učiniti ovaj sistem prihvatljivim za upotrebu. eksperimentalni rezultati. Urađena je bezbednosna analiza sistema.

U poslednjem, šestom delu rada dat je zaključak. Sumirani su svi ciljevi koji su postavljeni na početku istraživanja. Dati su svi ostvareni rezultati i doprinosi u radu. Razmatrane su moguće oblasti u kojima se rešenje može primeniti. Kao osnovne oblasti primene identifikovani su skoro

svi kripto sistemi, prvenstveno oni sistemi koji su od izuzetne važnosti za informacionu bezbednost jedne države u skladu sa postojećim softverskim i hardverskim rešenjima.

Šesto poglavlje predstavlja zaključak. Prikazan je rezultat i doprinos disertacije. U istom poglavlju predstavljen je i predlog daljeg rada.

6. Postignuti rezultati i naučni doprinos doktorske disertacije

Eksperimentalnim rezultatima je potvrđeno da je optimalan broj ćelija koje se koriste kao argument u neinvertibilnoj transformaciji (4x4), te se zaključuje da je za navedenu transformaciju parametar EER približno 2% ili u proseku jedno odbijanje u 50 pokušaja.

Kombinovanjem više biometrijskih modaliteta pokazalo se da je moguće poboljšati performanse navedenog sistema i učiniti da rad sistema bude pouzdan i bezbedan. Ova posebna hipoteza je dokazana putem empirijskih istraživanja gde je potvrđeno da višemodalni sistem za generisanje tajnih ključeva ne dozvoljava lažno prihvatanje, to znači da je parametar FAR u svim radnim režimima sistema jednak nuli, što čini ovaj sistem društveno prihvatljivim iz ugla korišćenja i u pogledu bezbednosti.

Rešenje prikazano u ovoj doktorskoj disertaciji kroz eksperimentalni rad koji je izložen u petom poglavlju ukazuje da je kvalitet kriptoloških ključeva značajno bolji u informaciono-teorijskom smislu. Sistem je u stanju da ekstraktuje ključeve dužine od 128 do 256 bitova. Treba napomenuti da se ključ od 256 bitova smatra izuzetno jakim ključem i da po NIST-ovim standardu ovaj ključ može biti predmet eksploatacije narednih 30 do 50 godina.

Zatim, primenom dobre strategije fuzije razvija se sistem visokih performansi. Sa aspekta sigurnosti, predloženo rešenje u ovoj tezi sprečava sve poznate metode napada na biometrijske sisteme, što je elaborirano u petom poglavlju koje se odnosi na evaluaciju bezbednosti predloženog rešenja. Ukoliko se napad ne može sprečiti, predloženo rešenje će smanjiti mogućnosti izvođenja, odnosno umanjiće efekte samih napada.

U predloženom rešenju, na robusnost ne utiče broj korisnika koji će koristiti sistem kao i da su vrste biometrijskih osobina koje je potrebno steći već poznate i teorijski dokazive te da kao takve predstavljaju reprezentativni biometrijski uzorak.

Za realizaciju datog rešenja u skladu sa kontinuiranim razvojem informacionih tehnologija i dostupnošću uređaja za izdvajanje biometrijskih karakteristika ovaj sistem predstavlja kompromis između troškova razvoja i njegovih performansi i omogućava primenu na standardnim hardverskim platformama za akviziciju biometrijskih uzoraka koji su danas u upotrebi.

7. Mišljenje i predlog Komisije o doktorskoj disertaciji

Na osnovu svega izloženog Komisija je mišljenja da doktorska disertacija kandidata Jelene Gavrilović po svojoj temi, pristupu, strukturi i sadržaju rada, kvalitetu i načinu izlaganja, metodologiji istraživanja, načinu korišćenja literature, relevantnosti i kvalitetu sprovedenog istraživanja i donetim zaključcima zadovoljava kriterijume zahtevane za doktorsku disertaciju, te se može prihvatiti kao podobna za javnu odbranu.

Sagledavajući ukupnu ocenu doktorske disertacije kandidata Jelene Gavrilović pod nazivom „Jedna klasa sistema za generisanje i distribuciju kriptoloških ključeva zasnovana na više biometrijskih modaliteta" predlažemo Veću departmana za poslediplomske studije i Senatu Univerziteta Singidunum da prihvati napred navedenu doktorsku disertaciju i odobri njenu javnu odbranu.

Beograd, 26/10/2022.

Članovi komisije:

prof. dr Saša Adamović

prof. dr Mladen Veinović

prof. dr Branko Kovačević