

VEĆU DEPARTMANA ZA POSLEDIPLOMSKE STUDIJE

Odlukom Veća Departmana za posleddiplomske studije broj 4-41/2023 od 2.3.2023. godine, određeni smo za članove Komisije za ocenu i odbranu doktorske disertacije kandidata Nikole Savanovića pod nazivom „Analiza bezbednosnih modela detekcije upada u distribuirane sisteme, optimizacijom hibridnih algoritama neuronskih mreža.“

o čemu podnosimo sledeći

IZVEŠTAJ

1. Osnovni podaci o kandidatu i doktorskoj disertaciji

Kandidat Nikola Savanović rođen je 7.2.1988. godine u Beogradu, gde je završio osnovnu i srednju školu. Politehnika - Škola za nove tehnologije završio je 2007. god. na smeru mašinski tehničar za kompjutersko konstruisanje. Osnovne akademske studije završio je 2013. god. na Fakultetu za informatiku i računarstvo, Univerziteta Singidunum. Master akademske studije upisuje školske 2013/2014 i završava 2015. god. na studijskom programu: “Savremene informacione tehnologije“ na Univerzitetu Singidunum, sa prosečnom ocenom 10. Doktorske akademske studije na studijskom programu Napredni sistemi zaštite na Univerzitetu Singidunum, upisao je školske 2015/2016 godine.

Od 2013. godine započinje angažman u *Saga Doo*, u sektoru telekomunikacija. Nakon toga, iste godine prelazi u *Naxi Digital Doo* na poziciji sistem administratora. Decembra 2014. godine zapošljava se na Univerzitetu Singidunum, gde postaje deo tima Računarskog Centra. Od 2015. godine angažovan je kao saradnik u nastavi, a po upisivanju doktorskih studija stiče izbornu zvanje asistent u nastavi. Angažovan je na predmetima na Fakultetu za informatiku i računarstvo i Tehničkom fakultetu iz oblasti računarstva i informacionih tehnologija. Kandidat je angažovan kao asistent na predmetima Računarske mreže, Zaštita u računarskih mrežama, Zaštita na vebu, Dizajn i programiranje korisničkih interfejsa, Klijetske-veb aplikacije, Interakcija čovek-računar, Veb dizajn, Veb programiranje i drugo.

Kandidat Nikola Savanović učestvuje u realizaciji mnogobrojnih stručnih kurseva u okviru Univerziteta Singidunum. Aktivno je držao obuke i seminare za direktore i nastavnike osnovnih i srednjih škola (Zavod za unapređivanje obrazovanja i vaspitanja). Imenovan je od strane

Univerziteta kao ocenjivač na maturskom ispitu u srednjoj školi *ETŠ Rade Končar*. Više puta je učestvovao u *ERAZMUS+* programu. Aktivno se bavi naučno-istraživačkim radom. Tokom master i doktorskih studija učestvovao je u pisanju četiri univerzitetska udžbenika kao koautor. Takođe, kandidat aktivno učestvuje na različitim domaćim i stranim naučnim i stručnim konferencijama.

Kandidat ima sledeće objavljene radove u odgovarajućim kategorijama, čime je ispunjen preduslov za odbranu doktorske disertacije.

U nastavku se može videti tabelarni prikaz broja objavljenih naučnih radova kandidata:

Broj objavljenih naučnih radova kandidata				
Kategorija	M20	M33	M13	Udžbenika
Ukupno	3	11	5	4

Kategorija M21a

1. Savanović, N.; Arandelović, I.D.; Mitrović, Z.D. The Results on Coincidence and Common Fixed Points for a New Type Multivalued Mappings in b-Metric Spaces. *Mathematics* 2022, 10, 856. <https://doi.org/10.3390/math10060856>

Kategorija M22

1. Savanović, N., Toskovic, A., Petrovic, A., Zivkovic, M., Damaševičius, R., Jovanovic, L., Bacanin, N., & Nikolic, B. (2022). Intrusion Detection in Healthcare 4.0 Internet of Things Systems via Metaheuristics Optimized Machine Learning. *Sustainability*, 15(16), 12563. <https://doi.org/10.3390/su151612563>

Kategorija M23

1. Zivkovic, M.; Bacanin, N.; Antonijevic, M.; Nikolic, B.; Kvascev, G.; Marjanovic, M.; Savanovic, N. Hybrid CNN and XGBoost Model Tuned by Modified Arithmetic Optimization Algorithm for COVID-19 Early Diagnostics from X-ray Images. *Electronics* 2022, 11, 3798. <https://doi.org/10.3390/electronics11223798>

Spisak objavljenih univerzitetskih udžbenika (koautorskih izdanja):

1. D. Cvetković N. Savanović, Veb dizajn i multimedijalni sistemi, Univerzitet Singidunum, Beograd, 2023.
2. M. Jovanović N. Savanović, Dizajn i programiranje korisničkog interfejsa, Univerzitet Singidunum, Beograd, 2023.
3. S. Alčaković, A. Đorđević, N. Savanović, Digitalni marketing, Univerzitet Singidunum, 2021

4. Dragan Cvetković, Dragan Marković, Nikola Savanović, *Multimedija*, ISBN: 978-86-7912-609-2, Univerzitet Singidunum, 2017 Beograd

Preostali objavljeni radovi:

Spisak rezultata M33

1. Petrovic, M. Antonijevic, I. Strumberger, L. Jovanovic, N. Savanovic, S. Janicijevic, The XGBoost Approach Tuned by TLB Metaheuristics for Fraud Detection, Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022), pp. 219 - 234, Jan, 2023
2. V. Toković, M. Živković, N. Savanović, Modern JavaScript 3D Visualization Frameworks: A Survey Study, IcETRAN 2020, Sep, 2020
3. V. Toković, L. Gajić, D. Cvetnić, M. Vidačić, N. Savanović, M. Živković, Meme App Generator, IcETRAN 2020, Sep,
4. V. Toković, L. Gajić, D. Cvetnić, M. Vidačić, N. Savanović, M. Živković, Android Application For Promoting The Cultural Institutions Through Wi-Fi Access, IcETRAN 2020, Sep, 2020
5. J. Knežević, J. Panović, N. Savanović, M. Živković, SEO in Serbian websites, IcETRAN 2020, Sep, 2020
6. Elsadaï, M. Tair, N. Savanović, The Evaluation of The Technical Quality of Web Sites with Contents in Arabic and Serbian Languages, Proceedings of the Sinteza 2019 International Scientific Conference on Information Technology and Data Related Research, ISBN: 978-86-7312-703-7, pp. 351-359, Apr, 2019
7. D. Marković, M. Tair, M. Šarac, D. Stamenković, N. Savanović, Content distribution in education support software, 4nd International Scientific Conference of IT and Business-Related Research SINTEZA 2017, Belgrade, Serbia, ISBN: 978-86-7912-657-3, pp. 248-253, Apr, 2017
8. N. Savanović, M. Sarac, D. Markovic, D. Radovanovic, A. Jevremovic, Computer network security on physical layer, 3rd International Conference on Electrical, Electronic and Computing Engineering IcETRAN 2016, Zlatibor, Serbia , Jun 2016, ISBN 978-86-7466-618-0, pp. 80-81, Jun, 2016
9. M. Tair, A. Mihajlović, N. Savanović, A Multi-Layered Image Format for the Web With an Adaptive Background Layer Selection Algorithm, Book of proceedings, Sinteza 2016, ISBN: 978-86-7912-628-3, pp. 24-30, Dec, 2016
10. N. Savanović, M. Šarac, D. Stamenković, S. Adamović, Unreal Engine platforma za razvoj edukativnih video igara, 16th International Scientific Conference SINERGIJA 2015, Bijeljina, Republika Srpska, pp. 118-121, Dec, 2015
11. N. Savanović, S. Adamović, A. Jevremović, M. Milosavljević, M. Veinović, M. Šarac, Konstruisanje generatora slučajnih brojeva preko fizičkog izvora informacija - TRNG, ISBN: 978-99955-26-32-0, pp. 248-252, Dec, 2013

Ostali radovi:

1. Aleksandar Jevremović, Mladen Veinović, Goran Shimić, Nikola Savanović, Dragan Randjelović, "Development of the Android - based secure communication device", Knowledge Discovery in the Cyberspace: Statistical Analysis and Predictive Modeling, New York, 2/2017, ISSN:978-1-53610-566-7
2. M. Zivkovic, L. Jovanovic, N. Bacanin, A. Petrovic, N. Savanovic, M. Dobrojevic, XGBoost Tuned by Hybridized SCA Metaheuristics for Intrusion Detection in Healthcare 4.0 IoT Systems, Chapter in AIS Algorithms for Intelligent Systems: ICEAI 2023: Evolutionary Artificial Intelligence, Springer, AIS Algorithms for Intelligent Systems: ICEAI 2023: Evolutionary Artificial Intelligence, pp. 1 - 16, Springer, Singapore, Malaysia, Mar, 2024
3. M. Milicevic, L. Jovanovic, N. Bacanin, M. Zivkovic, D. Jovanovic, M. Antonijevic, N. Savanovic, I. Strumberger, Optimizing Long Short-Term Memory by Improved Teacher Learning-Based Optimization for Ethereum Price Forecasting, Chapter in LNDECT Lecture Notes on Data Engineering and Communications Technologies: ICMCSI 2023: Mobile Computing and Sustainable Informatics, Springer, volume 166, LNDECT Lecture Notes on Data Engineering and Communications Technologies: ICMCSI 2023: Mobile Computing and Sustainable Informatics, volume 166, pp. 125 - 139, Springer, Singapore, Nepal, May, 2023
4. Petrovic, M. Antonijevic, I. Strumberger, L. Jovanovic, N. Savanovic, S. Janicijevic, The XGBoost Approach Tuned by TLB Metaheuristics for Fraud Detection, Chapter in Advances in Computer Science Research: ICIITB 2022: 1st International Conference on Innovation in Information Technology and Business, Springer, pp. 219 - 234, Atlantis Press, Springer Nature, Jan, 2023
5. Petrovic, M. Antonijevic, I. Stumberger, N. Savanovic, S. Janicijevic, N. Budimirovic, Intrusion Detection by XGBoost Model Tuned by Improved Multi-verse Optimizer, Chapter in Advances in Computer Science Research: ICIITB 2022: 1st International Conference on Innovation in Information Technology and Business, Springer, pp. 203 - 218, Atlantis Press, Springer Nature, Jan, 2023

Doktorska disertacija kandidata Nikole Savanovića sadrži 161 stranice, od čega 7 strana čine prilog i spisak literature. Spisak literature obuhvata 108 referenci koje čine naučni radovi, knjige, zbornici radova, zakonski propisi kao i elektronski izvori. Uz osnovni tekst disertacija sadrži i 53 slika i 15 tabela.

Doktorska disertacija kandidata Nikole Savanovića je bila podvrgnuta proveri softverom za ustanovljavanje preklapanja/plagijarizma (iThenticate Plagiarism Detection Software). *Ukupan procentualni iznos zapaženih preklapanja iznosi 1 % disertacije.*

2. Predmet i cilj istraživanja

Predmet istraživanja je analiza bezbednosnih mehanizama i modela distribuiranih sistema i uređaja internet stvari (IoT) putem globalne računarske mreže, tj. interneta. Optimizacijom algoritama mašinskog učenja vrši se modifikacija postojećeg algoritma, kojim se ujedno može značajno unaprediti mehanizam detekcije upada u distribuirane sisteme. Time se postižu veća efikasnost i tačnost prilikom detekcije. Analiza obuhvata različite klasifikacije podataka, mehanizme zaštite, uključujući napredne algoritme mašinskog učenja i neuronske mreže, koji se koriste za detekciju i prevenciju savremenih bezbednosnih pretnji u distribuiranim sistemima.

Cilj ovog naučnog istraživanja jeste unapređenje postojećih okvira za zaštitu od upada u distribuirane sisteme kroz primenu i optimizaciju hibridnih algoritama, rezultujući u tačnosti predviđanja. Istraživanje teži da optimizuje postojeće metode i algoritme za poboljšanje detekcije upada i prevenciju bezbednosnih incidenata, sa fokusom na precizniju klasifikaciju podataka i zaštitu osetljivih informacija u *IoT* uređajima koji se koriste u okviru distribuiranih sistema. Metaheurističke metode značajno doprinose obradi posmatranih skupova podataka. Stoga se uključuje i implementacija dubokih neuronskih mreža, kako bi celokupan proces bio potpomognut postizanju visoke tačnosti prilikom detekcije upada. Obavljaju se komparativne analize performansi poredbenih algoritama, čime se prikazuju ostvareni rezultati sa svojim prednostima. Takođe, fokus i akcenat se stavljaju na identifikaciju i analizu metrika performansi kao što su Koenov koeficijent kape, *PR* krive i *ROC* krive, čime se može utvrditi efikasnost optimizovanog algoritma u realnim scenarijima, a sa konačnim ishodom poboljšanja sveukupne bezbednosti sistema. Naučno istraživanje pokazuje kako se optimizacijom hibridnih algoritama mašinskim učenjem mogu značajno poboljšati integritet podataka poboljšanjem prevencije upada u distribuirani sistem, usled savremenih brojnih bezbednosnih pretnji.

Doktorska disertacija fokusirana je na naučno istraživanje predstavljeno u radu:

Savanović, N., Toskovic, A., Petrovic, A., Zivkovic, M., Damaševičius, R., Jovanovic, L., Bacanin, N., & Nikolic, B. (2022). Intrusion Detection in Healthcare 4.0 Internet of Things Systems via Metaheuristics Optimized Machine Learning. Sustainability, 15(16), 12563. <https://doi.org/10.3390/su151612563>.

Doktorska disertacija se bavi i fokusira na koncept *Healthcare* 4.0, koji integriše i implementira sofisticirane tehnologije internet stvari (IoT) u zdravstveni sistem. Osnovni cilj naučnog istraživanja jeste optimizacija postojećih algoritama mašinskog učenja pomoću hibridnim metaheurističkim algoritmima, sa ciljem poboljšanja detekcije upada u distribuirani sistem. Zbirno, cilj povezivanja ovih disciplina i oblasti jeste poboljšanje i sveukupno unapređenje bezbednosti i integriteta ličnih podataka u zdravstvu. U doktorskoj disertaciji poseban osvrt stavlja se na detekciju upada u distribuirane sisteme zdravstva 4.0, gde se analiziraju i primenjuju napredne tehnike za identifikaciju i prevenciju bezbednosnih pretnji. Doktorska disertacija se primarno oslanja na rezultate i doprinose navedenog rada, ali uključuje i druga naučna istraživanja, kao i sveobuhvatnu analizu relevantnih istraživanja i naučne literature iz oblasti.

Istraživanje obuhvata evaluaciju postojećih metoda i savremenih sofisticiranih algoritama mašinskog učenja, pri čemu su predložena unapređenja postignuta sa ciljem i poboljšanjem njihovih performansi, tačnosti i efikasnosti, zatim, balansom sistema i konzistentnosti u radu između servisa. Dobijeni rezultati pokazuju visoke rezultate u pogledu tačnosti, preciznosti i odzivu algoritama za detekciju upada u distribuiran sistem.

Navedeno naučno istraživanje doprinosi poboljšanju bezbednosnih rešenja u zdravstvenom sektoru koncepta 4.0, što u budućnosti može biti od ključne važnosti za zaštitu osetljivih podataka i pružanja veće pouzdanosti zdravstvenim servisima na nivou globalne mreže. Disertacija je rezultat multidisciplinarnog pristupa koji uključuje mašinsko učenje, metaheuristike, integraciju hibridnih algoritama i bezbednost informacionih sistema.

3. Hipotetički okvir istraživanja

Opšta hipoteza izvodi se kao: primena i optimizacija hibridnih algoritama mašinskog učenja i neuronskih mreža može značajno poboljšati detekciju i prevenciju upada u distribuirane sisteme, posebno u kontekstu interneta stvari (IoT).

Posebne hipoteze

- Predloženi optimizovani algoritam *XG-MFA* postići će bolje performanse prilikom detekcije upada u distribuiranim sistemima u poređenju sa tradicionalnim algoritmima za klasifikaciju podataka.
- Optimizovani hibridni algoritmi će pokazati veću preciznost (precision) i odziv (recall) pri detekciji bezbednosnih pretnji nego standardni algoritmi.
- Implementacija hibridnih algoritama u IoT uređajima će smanjiti broj lažno pozitivnih (false positive) i lažno negativnih (false negative) rezultata u procesu detekcije upada.
- Primena Koenovog koeficijenta kape kao metrike performansi će omogućiti precizniju evaluaciju efikasnosti algoritama za detekciju upada.
- Upotreba *PR* i *ROC* krivih će pružiti bolji uvid u performanse algoritama u scenarijima sa neujednačenim klasama.
- Algoritmi zasnovani na mašinskom učenju mogu efikasnije prepoznati i neutralisati *probe* napade (PA) i *distributed denial of service* (DDoS) napade u distribuiranim sistemima.
- Integracija naprednih kriptografskih algoritama sa hibridnim algoritmima za detekciju upada poboljšaće ukupnu bezbednost IoT uređaja u relevantnom sektoru u koji se može integrisati.
- Analiza važnosti karakteristika (feature importance) putem *SHAP* vrednosti može unaprediti transparentnost i interpretaciju odluka modela za detekciju upada.
- Algoritmi mašinskog učenja optimizovani modifikovanim algoritmom svetlosnih mušica (MFA) će pokazati konzistentne performanse u različitim distribuiranim sistemima.
- Implementacija predloženih algoritama u realnim zdravstvenim okruženjima će smanjiti broj bezbednosnih incidenata i povećati otpornost sistema na buduće napade.

4. Metodologija istraživanja

Metodologija istraživanja u ovoj doktorskoj disertaciji ima za cilj da pruži detaljan pregled metoda i pristupa koji su korišćeni prilikom testiranja postavljenih hipoteza i ostvarivanja ciljeva istraživanja. Fokus je na analizi performansi različitih algoritama za detekciju upada u distribuiranim sistemima, posebno u kontekstu interneta stvari (IoT). Složenost predmeta istraživanja zahteva primenu

- Prikupljanje podataka,
- Odabir algoritma,
- Eksperimentalni postupak,
- Implementacija algoritama,
- Analiza rezultata.

Na osnovu dobijenih rezultata, u ovoj doktorskoj disertaciji formulisani su zaključci i preporuke za dalju primenu i unapređenje predloženih algoritama u realnim okruženjima distribuiranih sistema. Posebna pažnja je posvećena bezbednosti podataka i otpornosti sistema na savremene pretnje.

5. Kratak prikaz sadržaja doktorske disertacije

Rad se sastoji iz 13 poglavlja, sadržajno struktuiranih na sledeći način:

Prvo poglavlje – Uvod; pruža pregled ciljeva i značaja istraživanja, ističući važnost unapređenja bezbednosti distribuiranih sistema putem naprednih algoritama mašinskog učenja. U ovom poglavlju naglašava se potreba za efikasnim metodama detekcije i prevencije upada u kontekstu distribuiranih sistema. Takođe, uvod razmatra trenutne izazove u zaštiti osetljivih podataka od savremenih pretnji.

Drugo poglavlje - Teorijske osnove; poglavlje obrađuje osnovne koncepte i teorije koje čine osnovu za razumevanje metoda i tehnika korišćenih u istraživanju. Obuhvaćeni su pojmovi distribuiranih sistema, mašinskog učenja i dubokog učenja. Takođe se razmatraju principi optimizacije algoritama i metaheuristike, koji su ključni za optimizaciju metoda detekcije upada.

Treće poglavlje - Nauka i pregled literature; daje se detaljan pregled postojeće literature i naučnih radova koji se odnose na analizu i primenu algoritama mašinskog učenja u bezbednosnim sistemima. Prikazuju se najnovija dostignuća i trendovi u oblasti zaštite distribuiranih sistema. Takođe, ističu se ključni radovi koji su postavili temelje za dalje istraživanje u ovoj oblasti.

Četvrto poglavlje - Distribuirani sistemi i mašinsko učenje; opisuje se kako su distribuirani sistemi integrisani sa algoritmima mašinskog učenja za poboljšanje detekcije upada i zaštite podataka. Analizira se uloga distribuiranih sistema u savremenim bezbednosnim okvirima. Takođe, prikazuju se prednosti korišćenja mašinskog učenja prilikom detekcije i prevencije upada.

Peto poglavlje - Mašinsko učenje i algoritmi neuronskih mreža; poglavlje se fokusira na različite algoritme mašinskog učenja i neuronskih mreža koji se koriste u istraživanju, kao i njihove prednosti i ograničenja. Razmatraju se specifikacije i performanse različitih modela. Posebna pažnja posvećena je algoritmu *XG-MFA*, njegovoj strukturi i primeni.

Šesto poglavlje - Problemi optimizacije algoritama mašinskog učenja; analizira probleme i izazove u optimizaciji algoritama mašinskog učenja, uključujući potrebu za poboljšanjem tačnosti. Analiziraju se različite tehnike optimizacije i njihovim efektima na performanse algoritama. Takođe, razmatraju se specifični problemi u kontekstu zaštite distribuiranih sistema.

Sedmo poglavlje - Duboko učenje; poglavlje objašnjava koncepte dubokog učenja, uključujući strukturu i primenu dubokih neuronskih mreža u detekciji upada u distribuirane sisteme. Prikazuju se različiti modeli dubokog učenja i njihova efikasnost. Takođe, utvrđuju se sve prednosti i izazovi prilikom primene dubokog učenja u distribuiranim sistemima.

Osmo poglavlje – Metaheuristike postupci visokog nivoa; pregled različitih metaheurističkih metoda i njihova primena u optimizaciji algoritama za detekciju upada. U doktorskoj disertaciji istražuju se i analiziraju najefikasnije metaheuristike, kao i njihova primena u oblasti istraživanja. Poseban osvrt i fokus su na metodima, kao što su optimizacija rojevi čestica i evolutivni algoritmi.

Deveto poglavlje - Predloženi eksperimentalni algoritam; daje se detaljan opis predloženog algoritma *XG-MFA*, uključujući metode, tehnike i korake korišćene u njegovoj implementaciji. Opisuju se specifične karakteristike koje čine ovaj algoritam efikasnim. Takođe, razmatraju se rezultati eksperimentalnih testova koji potvrđuju njegovu superiornost.

Deseto poglavlje - Eksperimentalni skup podataka; opis skupa podataka korišćenih u eksperimentima, uključujući izvore, vrste podataka i metode za njihovo prikupljanje i obradu. Detaljno se razmatraju karakteristike i struktura analiziranih podataka. Takođe, prikazuju se metode preprocesiranja i pripreme podataka za dalju analizu.

Jedanaesto poglavlje - Rezultati evaluacije eksperimenta i komparativna analiza rezultata; u poglavlju se prikazuju i prezentuje analiza rezultata eksperimenata, uključujući poređenje performansi različitih algoritama. Vrš se opservacija implikacija dobijenih rezultata za sveukupno unapređenje bezbednosti distribuiranih sistema.

Dvanaesto poglavlje - Zaključci obavljenih eksperimenata; sažetak ključnih nalaza istraživanja i preporuke za buduće istraživanje i primenu predloženih metoda. Analizira se u vezi sa poboljšanim potencijalnim unapređenjima i budućim koracima. Takođe, razmatraju se praktične implikacije rezultata istraživanja.

Trinaesto poglavlje – Literatura; prikazuje se spisak svih korišćenih izvora i referenci koje su korišćene u istraživanju, obezbeđujući potpunu dokumentaciju i verodostojnost rada. Prikazuju se izvori na kojima se zasniva ovo naučno istraživanje. Takođe, daju se preporuke za dodatnu literaturu za dalje čitanje i istraživanje.

Potvrđeni doprinosi ovog rada su sledeći:

- Poboljšanje algoritama za detekciju upada: Istraživanje je unapredilo postojeće algoritme za detekciju upada u distribuiranim sistemima, poboljšavajući njihovu tačnost i efikasnost.
- Implementacija *XG-MFA* algoritma: Analiziran je i testiran optimizovani algoritam *XG-MFA* koji pokazuje superiorne performanse u klasifikaciji podataka.
- Optimizacija algoritama mašinskog učenja: proučeni su i optimizovani algoritmi mašinskog učenja, povećavajući tačnost predviđanja.
- Unapređenje bezbednosti podataka: Istraživanje je doprinelo unapređenju bezbednosti osetljivih posmatranih skupova podataka kroz efikasnije tehnike detekcije i prevencije upada u distribuirani sistem u okviru kog se oni koriste.
- Primena metaheurističkih metoda: Korišćenje naprednih metaheurističkih metoda za optimizaciju algoritama mašinskog učenja omogućilo je bolju obradu i klasifikaciju podataka.
- Dubinsko učenje za detekciju upada: Implementacija dubokih neuronskih mreža za detekciju upada pokazala je značajna poboljšanja u tačnosti i brzini detekcije.
- Evaluacija i komparativna analiza: Obavljena je detaljna evaluacija i komparativna analiza performansi različitih algoritama, pružajući detaljniji uvid u njihove prednosti i mane.
- Analiza eksperimentalnih skupova podataka: Analizirani su različiti skupovi podataka za eksperimente, omogućavajući testiranje i validaciju optimizovanih metoda.
- Poboljšanje zaštite distribuiranih sistema: Istraživanje je pokazalo kako optimizovane metode mogu efikasno poboljšati zaštitu distribuiranih sistema od savremenih bezbednosnih pretnji i izazova.

6. Mišljenje i predlog Komisije o doktorskoj disertaciji

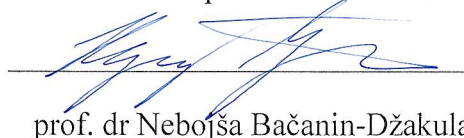
Na osnovu svega izloženog Komisija je mišljenja da doktorska disertacija kandidata Nikole Savanovića po svojoj temi, pristupu, strukturi i sadržaju rada, kvalitetu i načinu izlaganja, metodologiji istraživanja, načinu korišćenja literature, relevantnosti i kvalitetu sprovedenog istraživanja i donetim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

Sagledavajući ukupnu ocenu doktorske disertacije kandidata Nikole Savanovića pod nazivom „Analiza bezbednosnih modela detekcije upada u distribuirane sisteme, optimizacijom hibridnih algoritama neuronskih mreža“ predlažemo Veću departmana za posleddiplomske studije i Senatu Univerziteta Singidunum da prihvati napred navedenu doktorsku disertaciju i odobri njenu javnu odbranu.

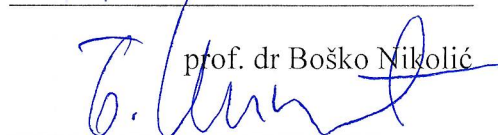
Beograd, 8.7.2024.

Članovi komisije:

prof. dr Marko Šarac



prof. dr Nebojša Bačanin-Džakula



prof. dr Boško Nikolić