

UNIVERZITET U BEOGRADU FAKULTET ORGANIZACIONIH NAUKA

Nastavno-naučnom veću

Predmet: Podobnost teme i kandidata Nenada Badovinca za izradu doktorske disertacije.

Odlukom 05-01 бр. 3/150-13 od 11. 12. 2019. godine, imenovani smo za članove Komisije za ocenu podobnosti teme i kandidata Nenada Badovinca za izradu doktorske disertacije i naučne zasnovanosti teme „**MODEL AUTENTIFIKACIJE KORISNIKA PRIMENOM BIOMETRIJE U SISTEMIMA ELEKTRONSKOG PLAĆANJA**“

Na osnovu materijala priloženog uz Zahtev kandidata, Komisija podnosi sledeći

R E F E R A T

1. PODACI O KANDIDATU

1.1. Biografski podaci

Nenad Badovinac rođen je 12.10.1977. godine u Bjelovaru. Osnovnu i srednju školu je završio u Bjelovaru. Diplomirao je 2003. godine na „Fakultetu organizacije i informatike“, Univerziteta u Zagrebu, na smeru „Informacioni sistemi“ odbranivši diplomski rad na temu „Simulacija rada bankarskog sistema“. Postdiplomske studije, smer „Elektronsko poslovanje“ upisao je 2014. na Fakultetu organizacionih nauka, Univerziteta u Beogradu. Odbranio je master rad: „Komparativne metode mobilnih plaćanja“, u septembru 2015. Doktorske studije studijskih program „Informacione tehnologije“, upisao je na istom fakultetu, 2015. godine. Učestvovao je na više stručnih skupova o upotrebi informaciono-komunikacionih tehnologija. Nenad Badovinac je zaposlen u firmi „Azelijski doo“ na radnom mestu direktor preduzeća. Azelija je firma koja se bavi implementacijom ERP softvera PANTHEON. Nenad aktivno učestvuje u školovanju korisnika za rad u poslovnim softveru kao i u poslovima implementacije poslovnog softvera.

Obrazovanje:

- 1996–2003; Diplomirani informatičar (Dipl. Inf), Sveučilište u Zagrebu, Fakultet organizacije i informatike u Varaždinu
- 2015–2016: Master informatike (M.Sc.), Univerzitet u Beogradu, Fakultet organizacionih nauka
- 2016–do danas: Student doktorskih studija, Univerzitet u Beogradu, Fakultet organizacionih nauka

Autor je ili koautor više radova iz oblasti informacionih tehnologija koji su objavljeni u domaćim i međunarodnim časopisima i na konferencijama.

1.2. Stečeno naučnoistraživačko iskustvo

U nastavku će biti predstavljene naučnoistraživačke aktivnosti kandidata. One se odnose na prikaz položenih ispita i objavljene radove u časopisima i na konferencijama.

Sledi prikaz položenih predmeta na doktorskim studijama sa ocenama i ESPB bodovima:

Naziv predmeta	Ocena	ESPB
Internet inteligentnih uređaja – odabrana poglavlja	10 (deset)	10
Internet tehnologije – odabrana poglavlja	10 (deset)	10
Interakcija čoveka i računara – odabrana poglavlja	10 (deset)	10
Metode zaštite u elektronskom poslovanju – odabrana poglavlja	10 (deset)	10
Metodologija naučno-istraživačkog rada	10 (deset)	10
Mobilno poslovanje – odabrana poglavlja	10 (deset)	10
Multimedijalne komunikacije – odabrana poglavlja	10 (deset)	10
Multimediji – odabrana poglavlja	10 (deset)	10
Napredne biometrijske tehnologije	10 (deset)	10

Nenad Badovinac je 10. jula 2023. godine odbranio pristupni rad pod nazivom: „**MODEL AUTENTIFIKACIJE KORISNIKA PRIMENOM BIOMETRIJE U SISTEMIMA ELEKTRONSKOG PLAĆANJA**“.

1.3. Spisak radova

Nenad Badovinac je autor ili koautor u sledećim naučnim publikacijama:

1. Poglavlje u monografiji međunarodnog značaja (M13):

- **Badovinac N.**, Simic D. (2020): “E-Payment Systems Using Multi-card Smartcard”. In: Mladenović N., Sifaleras A., Kuzmanović M. (eds) *Advances in Operational Research in the Balkans*. Springer Proceedings in Business and Economics. Springer.
- **Nenad Badovinac**, Dejan Simić: “A Multimodal Biometric Authentication (MBA) in Card Payment Systems”. *Proceedings of 2019 International Conference on Artificial Intelligence: Applications and Innovations*, Los Alamitos, USA (ISBN-13: 978-1-7281-4326-2), pp. 23-27, DOI 10.1109 / IC-AIAI48757.2019.00011

2. Poglavlje u monografiji međunarodnog značaja (M14):

- **Badovinac, N.**, Simić, D. (2023). Biometric Creation of Digital Signatures and Their Application in Blockchain. In: Mihić, M., Jednak, S., Savić, G. (eds) *Sustainable Business Management and Digital Transformation: Challenges and Opportunities in the Post-COVID Era*. SymOrg 2022. vol 562. Springer, Cham. https://doi.org/10.1007/978-3-031-18645-5_1

3. Zbornici međunarodnih naučnih skupova – saopštenja štampana u celini (M33):

- **Nenad Badovinac:** "Model adaptivne biometrijske autentifikacije", Konferencija sa međunarodnim učešćem "Napredne tehnologije u obrazovanju i privredi" (2023; Novi Sad) ISBN 978-86-6211-145-6, COBISS.SR-ID 116724745
- **Nenad Badovinac:** "Klasifikacija web stranica bazirana na Support Vector Machine ", XIII međunarodni naučno-stručni skup Informacione tehnologije za e-obrazovanje, Izdavač: Panevropski univerzitet "APEIRON", Banja Luka, godina 2021. ISBN 978-99976-34-80-1
- **Badovinac N, Simic, D.:** "Model biometrijske autentifikacije u sistemu mobilnog bankarstva", The 5-th international Conference on knowledge management and informatics. Book of Proceedings, 8 - 9. January 2019. Kopaonik-Srbija. ISBN 978-86-6211-115-9. COBISS.SR-ID 327620103 Str.115-120.
- **Nenad Badovinac,** "Android application for recording signed consents from GDPR regulation", XVI International symposium: "Doing Business in the Digital Age: challenges, approaches and solutions" (pp. 683-691), SymOrg 2018, Zlatibor-Serbia, June 7-10, 2018; Organised by Faculty of organizational sciences. ISBN 978-86-7680-361-3. Str.1084-1088.
- **Badovinac, N.:** „Organizacioni model sistema za evidenciju korisnika pametnih bolnica“, Međunarodno savetovanje na temu: „Upravljanje znanjem i informatika“ Kopaonik, 12.-13. januar, 2018., IV. Međunarodna konferencija Upravljanje znanjem i informatika. ISBN 978-86-6211-113-5, COBISS.SR-ID 320281095. Str.30-36.
- **Badovinac, N.:**"Automatsko generisanje programske sheme onlajn radija bazirane na kategorijama emisija", XVI međunarodni naučno-stručni simpozijum Infoteh-Jahorina 2017. Jahorina, 22.03.-24.03.2017. ISBN: 978-99976-710-0-4 Str.613-616.
- **Badovinac, N.:**"Elektronsko poslovanje u auto kućama - upravljanje mrtvim zalihama - Electronic business in auto-house companies management of dead stock" XLIII Simpozijum o operacionim istraživanjima. SYM-OP-IS 2016, Tapa-Srbija, 20–23. септембар 2016. ISBN 978-86-335-0535-2. COBISS.SR-ID 225714444 Str.85.
- **Badovinac Nenad, Đorđević Katarina:**"CRM model in e-business for non-commercial online radio", International symposium SymOrg 2016 Symposium proceedings / XV International symposium. Reshaping the Future Through Sustainable Business Development and Entrepreneurship - SymOrg 2016, june 10-13, Zlatibor; Organised by Faculty of organizational sciences, Serbia. ISBN 978-86-7680-326-2, COBISS.SR-ID 223988236. Str.318-324.

4. Zbornici međunarodnih naučnih skupova, saopštenja u izvodu (M34)

- **Nenad Badovinac, Dejan Simić:** Biometric Authentication model in electronic Payment System Based on Blockchain Transaction, INTERNATIONAL Symposium Sustainable Business Management and Digital Transformation: Challenges and Opportunities in the Post-COVID Era (18 ; 2022 ; Beograd) Book of abstracts / XVIII International Symposium Sustainable Business Management and Digital Transformation: Challenges and Opportunities in the Post-COVID Era, SYMORG 2022, Belgrade, June 11-14, 2022; ISBN 978-86-7680-411-5

5. Radovi objavljeni u naučnim časopisima nacionalnog značaja (M52)

- **Badovinac N.** "Osvrt na GDPR uredbu i sugestije za razvoj aplikativne podrške - Review of the GDPR regulation and suggestions for the development of support application.", Časopis InfoM, br 65/2018, str 11-16. UDC: 343.45:340.134

2. OCENA PODOBNOSTI KANDIDATA ZA RAD NA PREDLOŽENOJ TEMI

Na osnovu pokazanih rezultata dosadašnjeg obrazovanja, naučno-istraživačkog rada i profesionalnog iskustva, zaključujemo da je kandidat Nenad Badovinac kvalifikovan da samostalno radi na predloženoj temi doktorske disertacije i načini doprinose u toj oblasti.

Predložena tema disertacije je izmenjena radi jasnije formulacije teme u pristupnom radu koji je uspešno odbranjen. Modifikovani naziv je „**MODEL AUTENTIFIKACIJE KORISNIKA ZASNOVAN NA PRIMENI BIOMETRIJE U SISTEMIMA ELEKTRONSKOG PLAĆANJA**“. Tema disertacije odgovara istraživačkom radu koji je kandidat prikazao tokom doktorskih studija.

3. PROBLEM, PREDMET I CILJ ISTRAŽIVANJA

Model autentifikacije korisnika primenom biometrije u sistemima elektronskog plaćanja zahteva analizu postojećih modela kako bi se identifikovali nedostaci i ograničenja. Ograničenja mogu biti u vezi sa sigurnošću, zaštitom privatnosti, potrebom za poboljšanjem korisničkog iskustva i nesposobnošću implementacije u postojeće sisteme elektronskog plaćanja sa ATM i POS infrastrukturom. Svakom od ovih nedostataka treba pristupiti radi daljeg unapređenja, a cilj je formirati novi model koji će poboljšati nedostatak biometrijske autentifikacije u sistemima elektronskog plaćanja. Razvoj novog modela predstavlja nadogradnju postojećih rešenja i ima za cilj prevazilaženje nedostataka kako bi se obezbedila neophodna sigurnost u procesu elektronskog plaćanja. Korišćenje biometrijskih podataka u procesu autentifikacije korisnika elektronskog plaćanja ima za svrhu zaštitu sistema, ali takođe i očuvanje zdravlja korisnika izbegavajući fizički kontakt sa uređajem za autentifikaciju. U sistemima elektronskog plaćanja, važno je primeniti jednostavne metode autentifikacije koje će zadovoljiti potrebe korisnika za jednostavnim procesom, dok banke istovremeno traže visok nivo sigurnosti. Novi model biometrijske autentifikacije u sistemima elektronskog plaćanja treba da reši ove izazove pružajući sigurnost, zaštitu privatnosti i poboljšano korisničko iskustvo. Osim toga, važno je da novi model bude efikasan i pouzdan u autentifikaciji korisnika kako bi se osigurala sigurna elektronska transakcija. Novi model bi trebao da pruži balans između sigurnosti i jednostavnosti korišćenja, kako bi zadovoljio potrebe i očekivanja korisnika, ali i zahteve finansijskih institucija. U zaključku, razvoj novog modela biometrijske autentifikacije za sisteme elektronskog plaćanja zahteva pažljivo razmatranje postojećih nedostataka i ograničenja. Kroz primenu naprednih biometrijskih tehnologija i integraciju različitih faktora autentifikacije, može se postići siguran, praktičan i efikasan sistem autentifikacije koji zadovoljava potrebe svih učesnika u procesu elektronskog plaćanja.

Predmet istraživanja ove doktorske disertacije je mogućnost realizacije modela biometrijske autentifikacije u elektronskom plaćanju. Novi model će omogućiti korisnicima novo iskustvo korišćenja sistema elektronskog plaćanja, posebno u situacijama kada korisnik nosi zaštitne rukavice ili maske za lice. Ovaj model će kombinovati sigurnost i zaštitu privatnosti, eliminirajući potrebu za čuvanjem biometrijskih templejtova korisnika i tako i za dodatnom memorijom. Razvoj takvog modela će unaprediti postojeće modele biometrijske autentifikacije i rešiti probleme vezane za skladištenje velike količine biometrijskih podataka koji se koriste u procesu autentifikacije. Doktorska disertacija će se fokusirati na istraživanje različitih modela biometrijske autentifikacije i razvoj novog modela koji će biti primenjiv u širokom spektru oblasti, uključujući elektronsko plaćanje. Doktorska disertacija će dati doprinos razvoju novog modela biometrijske autentifikacije u elektronskom plaćanju i drugim oblastima. Ovaj model će predstavljati korak napred u obezbeđivanju sigurnijeg i efikasnijeg sistema autentifikacije, pružajući prednosti kako korisnicima, tako i pružiocima usluga elektronskog plaćanja.

Cilj istraživanja ove doktorske disertacije je razvoj novog modela biometrijske autentifikacije za sistem elektronskog plaćanja koji se može implementirati uz pomoć određene tehnologije. Glavni cilj novog modela je povećanje primenljivosti u novim aplikacijama, istovremeno obezbeđujući visok nivo sigurnosti ličnih biometrijskih podataka, koji neće biti čuvani u memoriji. Ideja je da se ovim modelom pruže nove mogućnosti bez potrebe za izmenom infrastrukture sistema elektronskog plaćanja. Za postizanje ovog cilja, u pristupnom radu izvršena su detaljna istraživanja i analiza dostupne naučne literature o postojećim metodama i modelima autentifikacije. Proučavane su tri različite prednosti koje će biti razmatrane u okviru istraživanja. Prva prednost je primena u zahtevnijim aplikacijama, tokom čijeg korišćenja korisnici nose zaštitne rukavice i maske za lice. Ovaj novi model bi trebao biti prilagodljiv i omogućiti autentifikaciju i u tim uslovima. Druga prednost koja će se razmotriti je sigurnost ličnih biometrijskih podataka. Novi model će biti osmišljen tako da neće zahtevati skladištenje biometrijskih podataka u memoriji, čime se smanjuje potencijalni rizik od zloupotrebe ili krađe podataka. Ovaj pristup obezbeđuje dodatnu zaštitu privatnosti korisnika. U cilju postizanja navedenih prednosti, doktorska disertacija će se fokusirati na razvoj novog modela biometrijske autentifikacije za elektronsko plaćanje. Ovaj model će biti dizajniran tako da bude praktičan za implementaciju u postojeće sisteme elektronskog plaćanja, ne zahtevajući značajne promene u infrastrukturi. Kroz istraživanje, ova doktorska disertacija će dati doprinos unapređenju biometrijske autentifikacije u oblasti elektronskog plaćanja, pružajući bolje korisničko iskustvo.

4. POČETNA LISTA BIBLIOGRAFSKIH IZVORA KOJI ĆE BITI KORIŠĆENI U IZRADI DOKTORSKE DISERTACIJE

U nastavku teksta je data početna lista bibliografskih izvora koji će biti korišćeni u izradi doktorske disertacije:

- [1] Talom F., Tengeh R. (2020): "The Impact of Mobile Money on the Financial Performance of the SMEs in Douala", Cameroon, Sustainability, vol.12, DOI: <https://doi.org/10.3390/su12010183>
- [2] Subaramaniam K., Garding J.M., Kolandaisamy R., Jalil A.B. (2020): "The impact of E-Wallets for current generation" Adv. Res. Dyn. Control Syst., vol12, 751–759, DOI: 10.5373/JARDCS/V12SP1/20201126
- [3] Md Arif H., Shukur Z., Kamrul H., Salih Al-Khaleefa A. (2020): "A Review on Electronic Payments Security", Symmetry, vol12, 1344; DOI:10.3390/sym12081344
- [4] Noor A.M., Chariri A., Rahardja S. (2020): "The effect of electronic payments security on e-commerce consumer perception: An extended model of technology acceptance", Manag. Sci. Lett., vol10, 1473–1480. DOI: 10.5267/j.msl.2019.12.020
- [5] Kim S. S. (2020): "Purchase Intention in the Online Open Market: Do Concerns for E-Commerce Really Matter?", Sustainability 12, no. 3: 773. DOI:10.3390/su12030773
- [6] Chun Se-Hak. (2019): "E-Commerce Liability and Security Breaches in Mobile Payment for e-Business Sustainability" Sustainability 11, no. 3: 715. DOI: 10.3390/su11030715
- [7] Xiao L., Qibei L., Feipeng G. (2020): "Mobile Personalized Recommendation Model based on Privacy Concerns and Context Analysis for the Sustainable Development of M-commerce" Sustainability 12, no. 7: 3036. DOI: 10.3390/su12073036
- [8] Nappi M., Ricciardi S., Tistarelli M. (2018): "Context Awareness in Biometric Systems and Methods: State of the Art and Future Scenarios", Imavis, DOI:10.1016/j.imavis.2018.05.001
- [9] Partila P, Tovarek J, Ilk GH, Rozhon J (2020) Deep learning serves voice cloning: how vulnerable are automatic speaker verification systems to spoofing trials? IEEE Commun Mag 58(2):100–105. <https://doi.org/10.1109/MCOM.001.1900396>
- [10] Shirvanian M, Vo S, Saxena N (2019): "Quantifying the breakability of voice assistants", In: 2019 IEEE international conference on pervasive computing and communications (PerCom), IEEE. <https://doi.org/10.1109/PERCOM.2019.8767399>

- [11] Dobbie S. (2020): "Challenge of biometric security for banks. *Biometric Technol Today* vol(3):5–7. DOI:10.1016/S0969-4765(20)30037-0
- [12] Kang J. (2018): "Mobile payment in Fintech environment: Trends, security challenges, and services. *Human-Centric Comput. Inf. Sci.* vol.8, 32. DOI: 10.1186/s13673-018-0155-4
- [13] Daimi K., Guillermo F., Hernández L. E. (2022): "Breakthroughs in Digital Biometrics and Forensics", ISBN: 978-3-031-10706-1 DOI:10.1007/978-3-031-10706-1
- [14] Velásquez I., Caro A., Rodríguez A. (2018): "Authentication schemes and methods: A systematic literature review", *Inf. Software Technol.* Vol.94, pages 30–37. DOI: 10.1016/j.infsof.2017.09.012.
- [15] Al Kabir M. A., Elmedany W. (2022): "An Overview of the Present and Future of User Authentication", 4th IEEE Middle East and North Africa Communications Conference (MENACOMM), Jordan, pp.10-17, DOI: 10.1109/MENACOMM57252.2022.9998304.
- [16] Bošnjak L., Brumen B. (2019): "Rejecting the death of passwords: Advice for the future", *Computer Science and Information Systems 2019*, Volume 16, Pages: 313-332, DOI: 10.2298/CSIS180328016B
- [17] Reese K., Smith T., Dutson J., Armknecht J., Cameron J., Seamons K. (2019): "A Usability Study of Five Two-Factor Authentication Methods", Brigham Young University, Proceedings of the Fifteenth Symposium on Usable Privacy and Security. Santa Clara, ISBN 978-1-939133-05-2
- [18] Talib A. A., Salman A. D. (2022): "An Efficient Electronic Payment Using Biometric Authentication", *Iraq Journal Of Computers, Communications, Control And Systems Engineering*, vol.22(3). Web link: <https://www.iasj.net/iasj/download/ee3d0e4ced7c3894>
- [19] Ceccanti A., Vianello E., Giacomini F. (2020): "Beyond X. 509: token-based authentication and authorization in practice", *EPJ Web of Conferences*, Vol. 245, DOI: 10.1051/epjconf/202024503021
- [20] Nyangaresi V. O., Ogundoyin S. O. (2021): "Certificate based authentication scheme for smart homes", 3rd Global Power, Energy and Communication Conference (GPECOM) pp. 202-207. DOI: 10.1109/GPECOM52585.2021.9607322.
- [21] Prabakaran D., Ramachandran S. (2022): "Multi-factor authentication for secured financial transactions in cloud environment", *CMC-Computers, Materials & Continua*, Vol.70(1), pp.1781-1798. DOI: <https://doi.org/10.1057/s41284-023-00378-1>
- [22] Vijay Koundinya V., Shwetha B. (2020): "A Review on Single Sign on as an Authentication Technique", *International Research Journal of Engineering and Technology (IRJET)*, Volume:07 Issue:06, p-ISSN: 2395-0072, e-ISSN: 2395-0056.
- [23] Wiefeling S., Dürmuth M., Luigi L. (2020): "More than just good passwords? A study on usability and security perceptions of risk-based authentication", In *Annual Computer Security Applications Conference, ACSAC* (pp. 203-218). DOI:10.1145/3427228.3427243
- [24] Jiayi C. (2022): "Adaptive User Authentication on Mobile Devices", *UWSpace*. <http://hdl.handle.net/10012/18452>
- [25] Munonye K., Péter M. (2022): "Machine learning approach to vulnerability detection in OAuth 2.0 authentication and authorization flow", *International Journal of Information Security*, vol.21(2), pp. 223-237. DOI: <https://doi.org/10.1007/s10207-021-00551-w>
- [26] Vinod V. M., Murugesan G., Mekala V., Thokaiandal S., Vishnudevi M., Siddharth, S. M. (2021): "A low-cost portable smart card based attendance system", In *IOP Conference Series: Materials Science and Engineering*, Vol.1012, No.1. DOI: 10.1088/1757-899X/1012/1/012046
- [27] Hassan A., Shukur Z., Hasan M. K. (2020): "An improved Time-Based one time password authentication framework for electronic payments", *Int. J. Adv. Comput. Sci. Appl*, vol.11, pp. 359-366. DOI: 10.14569/IJACSA.2020.0111146
- [28] Li S., Xu C., Zhang Y., Zhou, J. (2022): "A Secure Two-Factor Authentication Scheme from Password-Protected Hardware Tokens", *IEEE Transactions on Information Forensics and Security*, vol.17, pp.3525-3538. DOI: 10.1109/TIFS.2022.3209886
- [29] Aura T., Sethi M., Peltonen A. (2021): "Nimble Out-of-Band Authentication for EAP (EAP-NOOB)", *RFC 9140*, DOI: 10.17487/RFC9140
- [30] Kheshaifaty N., Gutub A. (2021): "Engineering graphical captcha and AES crypto hash functions for secure online authentication". *Journal of Engineering Research*, DOI: 10.36909/jer.13761

- [31] Lyastani S. G., Schilling M., Neumayr M., Backes M., Bugiel S. (2020): "Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication", In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 268-285). DOI: 10.1109/SP40000.2020.00047
- [32] Balajee R. M., Jayanthi K., Murali M. (2022): "Image-Based Authentication Security Improvement by Randomized Selection Approach", In Inventive Computation and Information Technologies: Proceedings of ICICIT, pp. 61-71. DOI: DOI: 10.1007/978-981-16-6723-7_6
- [33] Parmar V., Sanghvi H., Patel R. H., Pandya A. S. (2022): "A Comprehensive Study on Passwordless Authentication", In 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) (pp. 1266-1275). DOI: 10.1007/s11416-023-00484-z
- [34] Solomon A., Michaelshvili M., Bitton R., Shapira B. (2022): "Contextual security awareness: A context-based approach for assessing the security awareness of users, Knowledge-Based Systems", Volume 246, ISSN 0950-7051, DOI:10.1016/j.knosys.2022.108709
- [35] ROLanrewaju R.F., Khan B. (2021): "A Frictionless and Secure User Authentication in Web-Based Premium Applications", In IEEE Access, Vol. 9, pp. 129240-129255, DOI: 10.1109/ACCESS.2021.3110310.
- [36] Thomas P.A., Preetha M. (2023): "A broad review on non-intrusive active user authentication in biometrics", J Ambient Intell Human Comput vol.14, pp.339–360, DOI:10.1007/s12652-021-03301-x
- [37] Arias-Cabarcos P., Krupitzer C., Becker C. (2019): "A survey on adaptive authentication, ACM Comput. Surv. 52 (4), DOI: 10.1145/3336117
- [38] Jain A.K., Nandakumar K., Ross A. (2016): "50 Years of biometric research: Accomplishments, challenges, and opportunities", Pattern Recognit. Lett. 79, pp. 80–105. DOI: 10.1016/j.patrec.2015.12.013
- [39] Yang W., Wang S., Shahzad M., Zhou W. (2021): "A cancelable biometric authentication system based on feature-adaptive random projection", J. Inform. Secur. Appl. DOI: 10.1016/j.jisa.2020.102704
- [40] Shah S. W., Kanhere S. S. (2019): "Recent Trends in User Authentication – A Survey", Institute of Electrical and Electronics Engineers (IEEE), Vol. 7, pp. 112505–112519, DOI: 10.1109/access.2019.2932400
- [41] Sankalp B. (2014): „Authenticating Transactions using Bank–Verified Biometrics“. <https://arxiv.org/ftp/arxiv/papers/1407/1407.3366.pdf>
- [42] Badovinac Nenad, Simic Dejan (2019): "E-Payment Systems Using Multi-Card Smart Card", Book of Springer Proceedings in series: Springer Proceedings in Business and Economics – XIII Balkan Conference on Operational Research, ISBN 978-3-030-21989-5, pg. 237-249.
- [43] Shafiq U., Coughlan J., (2012): "Usability based reliable and cashless payment system (RCPS)", International Journal of Innovative Computing, Information and Control ICIC International, ISSN 1349-4198, pp. 2747.
- [44] Rawlson K (2016) Biometrics in banking & financial services, June 27–29. Web link: <https://www.biometricupdate.com/201604/special-report-biometrics-and-banking-2>
- [45] Nappi M., Ricciardi S., Tistarelli M. (2018): "Context awareness in biometric systems and methods: State of the art and future scenarios", Image Vis. Comput. 76 pp. 27–37. [http://refhub.elsevier.com/S2405-9595\(23\)00050-4/sb4](http://refhub.elsevier.com/S2405-9595(23)00050-4/sb4)
- [46] Zhang C., Yao L., Huang C., Gu T. (2020): "DeepKey: A multimodal biometric authentication system via deep decoding gaits and brainwaves", ACM Trans. Intell. Syst. Technol. 11 (4), DOI: <https://doi.org/10.1016/bs.acc.2020.02.007>
- [47] Ingale M., Cordeiro R., Thentu S (2020): "ECG Biometric Authentication: A Comparative Analysis", In IEEE Access, vol.8, pp.117853-117866, DOI: 10.1109/ACCESS.2020.3004464.
- [48] Thomas P.A., Preetha K. (2023): "A broad review on non-intrusive active user authentication in biometrics", J Ambient Intell Human Comput 14, 339–360, DOI: 10.1007/s12652-021-03301-x
- [49] Heruatmadja C., Meyliana A. N., Hidayanto N.: (2023): "Biometric as Secure Authentication for Virtual Reality Environment: A Systematic Literature Review," 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, 2023, pp. 1-7, DOI: 10.1109/ICONAT57137.2023.10080713.

- [50] ISO/IEC JTC1 SC27 Security Technique. Information Technology - Security Techniques - Biometric Information Protection, International Organization for Standardization, 2022. <https://www.iso.org/standard/75302.html> (accessed Feb. 15, 2022).
- [51] Marcel S., Nixon M.S. Fierrez J: (2019): "Evans Handbook of Biometric Anti-Spoofing", In (Eds.), Advances in Computer Vision and Pattern Recognition. Springer International Publishing. DOI10.1007/978-3-319-92627-8
- [52] Riseul Ryu, Soonja Yeom, David Herbert, Julian Dermoudy (2023): "The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction", ICT Express, ISSN 2405-9595, DOI: 10.1016/j.icte.2023.04.003.
- [53] Otta S.P., Panda S., Gupta M., Hota C. (2023): "A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure", Future Internet 2023, DOI:10.3390/fi15040146
- [54] Shoroog A., Lama A., Nouf A. (2022): "A Comprehensive Overview on Biometric Authentication Systems using Artificial Intelligence Techniques", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 13, No. 4. Web link: https://thesai.org/Downloads/Volume13No4/Paper_91-A_Comprehensive_Overview_on_Biometric_Authentication_Systems.pdf
- [55] Zukarnain Z.A., Muneer A., Ab Aziz (2022): "Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges", Symmetry, DOI:10.3390/sym14040821
- [56] Xuerui W., Zheng Y., Rui Z. (2021) "Attacks and defenses in user authentication systems: A survey, Journal of Network and Computer Applications, Accepted April 2021. DOI:10.1016/j.jnca.2021.103080
- [57] Wenzheng L., Xiaofeng W., Wei P. (2020): "State of the Art: Secure Mobile Payment", National University of Defense Technology, China. DOI:10.1109/ACCESS.2019.2963480
- [58] Sarah A., Stacey W. (2020): "A Review of Literature on Accessibility and Authentication Techniques", In The 22nd International ACM Sigaccess Conference on Computers and Accessibility (ASSETS '20), DOI:10.1145/3373625.3418005
- [59] Napa B., Jonathan W., Nasir M. (2019): "Emerging NUI-based Methods for User Authentication: A New Taxonomy and Survey", IEEE. DOI: 10.1109/TBIOM.2019.2893297
- [60] Zhang R., Zheng Y. (2019): "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification", IEEE, DOI:10.1109/ACCESS.2018.2889996
- [61] Choi, D. Chung C.Y. (2019): "Sustainable online shopping logistics for customer satisfaction and repeat purchasing behavior: Evidence from China", Sustainability, 11. DOI:10.3390/su11205626
- [62] Iovane G., Bisogni C. Nappi M: "An Encryption Approach Using Information Fusion Techniques Involving Prime Numbers and Face Biometrics," in IEEE Transactions on Sustainable Computing, vol. 5, no. 2, pp. 260-267, DOI: 10.1109/TSUSC.2018.2793466.
- [63] Therar H., Mohammed E., Ali A (2020): "Biometric Signature based Public Key Security System", 2020 International Conference on Advanced Science and Engineering (ICOASE), pp. 1-6, DOI: 10.1109/ICOASE51841.2020.9436615
- [64] Auer R., Böhme R., Wadsworth A. (2020): "An introduction to public-private key cryptography in digital tokens", BIS Quarterly Review, p.73. https://www.bis.org/publ/qtrpdf/r_qt2003.pdf#page=87
- [65] Godfrey-Welch, D., Lagrois R. (2018): "Blockchain in Payment Card Systems," SMU Data Science Review: Vol. 1: No. 1, Article 3. Available at: <https://scholar.smu.edu/datasciencereview/vol1/iss1/3>
- [66] Web site: <https://www.atlanticcouncil.org/cbdctracker/>
- [67] Derryl D., Filková Z., Packer F., Tiwari Siddharth (2019): "The design of digital financial infrastructure ", BIS Papers, No 106, <https://www.bis.org/publ/bppdf/bispap106.pdf>
- [68] Auer R., Böhme R., Wadsworth A. (2020): "An introduction to public-private key cryptography in digital tokens", BIS Quarterly Review, p.73. https://www.bis.org/publ/qtrpdf/r_qt2003.pdf#page=87
- [69] Auer R., Böhme R. (2020): "The technology of retail central bank digital currency", BIS Quarterly Review, https://www.bis.org/publ/qtrpdf/r_qt2003j.htm
- [70] Auer, R. (2019): "Embedded supervision: how to build regulation into decentralised finance ", BIS Working Papers, br. 811. <https://www.bis.org/publ/work811.htm>
- [71] Frost J. Gambacorta L., Huang Y., (2019): "BigTech and the changing structure of financial intermediation", BIS Working Papers, br. 779. <https://www.bis.org/publ/work779.htm>

- [72] Web site: <https://consensys.net/solutions/payments-and-money/cbdc/>
- [73] Badovinac N., Simić D. (2023): "Biometric Creation of Digital Signatures and Their Application in Blockchain", *Sustainable Business Management and Digital Transformation: Challenges and Opportunities in the Post-COVID Era*. SymOrg 2022, Lecture Notes in Networks and Systems, vol 562. Springer. DOI:10.1007/978-3-031-18645-5_1
- [74] Tarik H., Katya D. (2022): "Security Considerations for a Central Bank Digital Currency" <https://www.federalreserve.gov/econres/notes/feds-notes/security-considerations-for-a-central-bank-digital-currency-20220203.html>
- [75] Kalinic Z, Marinkovic V, Molinillo S, Liébana-Cabanillas F (2019): "A multi-analytical approach to peer-to-peer mobile payment acceptance prediction", *Retail Consum Serv* vol.49 pp.143–153, DOI:10.1016/j.jretconser.2019.03.016
- [76] Mertens G, Gerritsen L, Duijndam S, Saleminck E, Engelhard IM (2020): "Fear of the coronavirus (COVID-19): Predictors in an online study conducted in March 2020. DOI:10.31234/osf.io/2p57j
- [77] Liébana-Cabanillas F., Muñoz-Leiva F., Molinillo S. (2022): "Do biometric payment systems work during the COVID-19 pandemic? Insights from the Spanish users' viewpoint", *Financ Innov* 8, DOI:10.1186/s40854-021-00328-z
- [78] Juniper Research (2021) Biometrics to secure over \$3 trillion in mobile payments by 2025. Retrieved from <https://www.juniperresearch.com/press/biometrics-to-secure-over-3-trillion-in-mobile>
- [79] Téllez J., Zeadally S. (2017): "Mobile payment systems: secure network architectures and protocols. Springer, Berlin, DOI: 10.1007/978-3-319-23033-7
- [80] Findbiometrics (2021). Retrieved from <https://findbiometrics.com/topics/alipay/>
- [81] Zirjawi N, Kurtanovic Z, Maalej W (2015): "A survey about user requirements for biometric authentication on smartphones", In: 2015 IEEE 2nd Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE). IEEE, pp 1–6. DOI: 10.1109/ESPRE.2015.7330160
- [82] Stickland J. (2021): "Where in the world are biometric payments taking off", *Biometric Technology Today* 2018(6), 8-10, DOI: 10.1016/S0969-4765(18)30082-1
- [83] Ahmad D., Hariri M. (2012): "User Acceptance of Biometrics in E-banking to improve Security", *Business Management Dynamics*, vol.2, no.1, pp 01-04, 2012. Web link: https://www.researchgate.net/publication/341215049_User_Acceptance_of_Biometrics_in_E-banking_to_improve_Security
- [84] Web site: <https://bankingblog.accenture.com/enabling-blockchain-drive-change>
- [85] Lee J. (2015): "Report shows growing public acceptance of biometric authentication", *Biometric Update*, weblink: <http://www.biometricupdate.com/201507/report-shows-growing-public-acceptance-ofbiometric-authentication>, (accessed 6/6 2017).
- [86] Sharma M.K. (2017): "Electronic Cash over the Internet, and Security Solutions", *Int. J. Adv. Res. Computer Sci.* vol.8(1), 229.
- [87] GSMA (2019): *Mobile Identity—Unlocking the Potential of the Digital Economy*. GSM Association. October 2019. Available online: https://www.gsma.com/identity/wp-content/uploads/2014/10/GSMA-SIA-paper_FINALNov-2014.pdf.
- [88] Salim A. Tripathi S. Tiwari R.K. (2019): "Applying Geo-Encryption and Attribute Based Encryption to Implement Secure Access Control in the Cloud", *Int. J. Comput. Netw. Commun.* Vol.11, DOI:10.5121/ijcnc.2019.11407
- [89] El-Soud M., Gaber T., AlFayez F., Eltoukhy M. (2021): "Implicit authentication method for smartphone users based on rank aggregation and random forest", *Alexandria Engineering Journal*, Vol. 60, Issue 1, pp.273-283, ISSN 1110-0168, DOI: 10.1016/j.aej.2020.08.006.
- [90] Nor Z.Z., Nur I.R., Ahmad, D.J., Farhan A.M. (2021): "Biometric Acceptance in Malaysia Voyage", *e-Security*, vol.50, pp.2–46.
- [91] Huaibe L. (2012): "Biometric identification of identity authentication technology", *Straits Sci.* vol.10, pp.41–43.
- [92] Feng W., Ge B.S., Yong C., Xianrong Z. (2020): "Identity Authentication Security Management in Mobile Payment Systems", *J. Glob. Inf. Manag.* DOI: 10.4018/JGIM.2020010110

- [93] Riseul R., Soonja Y., Soo-Hyung K., David H. (2021): Continuous Multimodal Biometric Authentication, IEEE Access, vol.9, pp.34541-34557, DOI: 10.1109/ACCESS.2021.3061589.
- [94] Gonzalo P., Monaco V., Tappert V. (2015): "Analyzing Impaired-User Input Scenarios for Keystroke Biometric Authentication". Ph.D. Dissertation. Pace University, New York, USA. Web link: <https://digitalcommons.pace.edu/dissertations/AAI3733917/>
- [95] Cipriani J. (2020): "iPhones Face ID now unlocks faster when you wear a face mask", web link: <https://www.cnet.com/how-to/iphones-face-id-nowunlocks-faster-when-you-wear-a-face-mask-heres-what-to-do/>
- [96] Shah S. W., Kanhere S. S. (2019): "Recent Trends in User Authentication – A Survey", In IEEE Access, Vol. 7, pp. 112505–112519). Institute of Electrical and Electronics Engineers (IEEE), DOI:10.1109/access.2019.2932400
- [97] Cavus N., Mohammed Y., Bulama M., Isah M. (2023): "Examining User Verification Schemes, Safety and Secrecy Issues Affecting M-Banking", Systematic Literature Review, 13(1). DOI: 10.1177/21582440231152379
- [98] Arias-Cabarcos P., Krupitzer C., Becker C. (2019): "A survey on adaptive authentication", ACM Computing Surveys (CSUR), vol.52(4), pp.1-30. DOI: 10.1145/3336117
- [99] Xie Y., Li P., Nedjah N., Gupta B. B., Taniar D., Zhang J. (2022): "Privacy protection framework for face recognition in edge-based Internet of Things", In Cluster Computing. Springer Science and Business Media LLC. DOI: 10.1007/s10586-022-03808-8
- [100] Thapliyal A., Verma O., Kumar A. (2022): "Multimodal Behavioral Biometric Authentication in Smartphones for Covid-19 Pandemic", International journal of electrical and computer engineering systems, Vol. 13 No. 9, DOI: <https://doi.org/10.32985/ijeces.13.9.6>
- [101] Prabakaran D., Ramachandran, S. (2022). Multi-factor authentication for secured financial transactions in cloud environment. CMC-Computers, Materials & Continua, vol.70(1), pp. 1781-1798. DOI: <https://doi.org/10.32604/cmc.2022.019591>
- [102] Solomon A., Michaelshvili M., Bitton R., Shapira B. (2022): "Contextual security awareness: A context-based approach for assessing the security awareness of users, Knowledge-Based Systems", Volume 246, ISSN 0950-7051, DOI:10.1016/j.knosys.2022.108709
- [103] Olanrewaju R. F., Khan B. U. I., Morshidi M. A. Anwar F., Kiah M. L. B. M. (2021): "A Frictionless and Secure User Authentication in Web-Based Premium Applications," in IEEE Access, vol. 9, pp. 129240-129255, DOI: 10.1109/ACCESS.2021.3110310.
- [104] Singh G., Kaushik D., Handa H., Kaur G., Chawla S. K., Elngar A. A (2021): "BioPay: A Secure Payment Gateway through Biometrics." Journal of Cybersecurity and Information Management (JCIM), vol.7, no.2, pp. 65-77. DOI: 10.5281/zenodo.5224633
- [105] Ahamed F., Farid F., Suleiman B., Jan Z., Wahsheh L. A., Shahrestani, S. (2022): "An Intelligent Multimodal Biometric Authentication Model for Personalised Healthcare Services", Future Internet, vol.14(8), DOI:10.3390/fi14080222
- [106] Xie Y., Li P., Nedjah N., Gupta B. B., Taniar D., Zhang J. (2022): "Privacy protection framework for face recognition in edge-based Internet of Things", In Cluster Computing. Springer Science and Business Media LLC, DOI: 10.1007/s10586-022-03808-8
- [107] Ali A., Baghel V.S., Prakash S. (2022): "A novel technique for fingerprint template security in biometric authentication systems", Vis Comput, DOI:10.1007/s00371-022-02726-5
- [108] Tran Q. N., Turnbull B. P., Wang M., Hu J. (2022): "A Privacy-Preserving Biometric Authentication System With Binary Classification in a Zero Knowledge Proof Protocol", In IEEE Open Journal of the Computer Society, Vol. 3, pp.1–10, DOI:10.1109/ojcs.2021.3138332
- [109] Ali A., Baghel V.S., Prakash S. (2022): "A novel technique for fingerprint template security in biometric authentication systems", Vis Comput, DOI:10.1007/s00371-022-02726-5
- [110] Xie Y., Li P., Nedjah N., Gupta B. B., Taniar D., Zhang J. (2022): "Privacy protection framework for face recognition in edge-based Internet of Things", In Cluster Computing. Springer Science and Business Media LLC, DOI:10.1007/s10586-022-03808-8

- [111] Kausar F. (2021): "Iris based cancelable biometric cryptosystem for secure healthcare smart card", In Egyptian Informatics Journal, Vol. 22, Issue 4, pp. 447–453, DOI:10.1016/j.eij.2021.01.004
- [112] Benamara N. K., Keche M., Wellington M. (2021): "Securing E-payment Systems by RFID and Deep Facial Biometry", 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA), pp. 1-7. DOI: 10.1109/CAIDA51941.2021.9425175.
- [113] Jayanthan J., Priya N. K., Kumar S.P., Sangeetha K. (2021): "Facial Recognition Controlled Smart Banking", IJRESM, vol.4, no.3, pp.185–187., Web link: <https://journal.ijresm.com/index.php/ijresm/article/view/615>
- [114] Abed M. H., Alsaedi A. H., Alfoudi A. D., Otebolaku A. M., Razooqi Y. S. (2020): "Palm Vein Identification based on hybrid features selection model", arXiv, DOI:10.48550/ARXIV.2007.16195
- [115] Misra A., Dev K., Rajasekaran M. (2020): "Secured Payment System Using Face Recognition Technique", AIP Conference Proceedings, vol. 2282, no. 1, pp. 1-9, DOI:10.1063/5.0028457
- [116] Singh G., Singh R. K., Saha R., Agarwal, N. (2020): "IWT Based Iris Recognition for Image Authentication, In Procedia Computer Science, Vol. 171, pp. 1868–1876). DOI: 10.1016/j.procs.2020.04.200
- [117] Sharma S., Bhatt M., Sharma P. (2020): "Face Recognition System Using Machine Learning Algorithm", In 2020 5th International Conference on Communication and Electronics Systems (ICCES) IEEE, DOI:10.1109/icc48766.2020.9137850
- [118] Abed M. H., Alsaedi A. H., Alfoudi A. D., Otebolaku A. M., Razooqi Y. S. (2020): "Palm Vein Identification based on hybrid features selection model", arXiv, DOI:10.48550/ARXIV.2007.16195
- [119] Toygar O., Babalola F. O., Bitirim Y. (2020): "FYO: A Novel Multimodal Vein Database with Palmar, Dorsal and Wrist Biometrics", In IEEE Access, Vol.8, pp.82461–82470, Institute of Electrical and Electronics Engineers (IEEE), DOI: 10.1109/access.2020.2991475
- [120] Ahmad F., Cheng L.M., Khan A. (2020): "Lightweight and Privacy-Preserving Template Generation for PalmVein-Based Human Recognition", In IEEE Transactions on Information Forensics and Security, Vol.15, pp.184–194, DOI:10.1109/tifs.2019.2917156
- [121] Sheettal J., Sree A. D., Haritha T., Ramya M., Pooja K. (2019): "Authentication of E-Payment using Face Recognition System", International Journal of Engineering Science and Computing, pp. 21776-21781.
- [122] Mai G., Cao K., Yuen P. C., Jain A. K. (2019): "On the Reconstruction of Face Images from Deep Face Templates", In IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 41, Issue 5, pp. 1188–1202, Institute of Electrical and Electronics Engineers (IEEE), DOI: 10.1109/tpami.2018.2827389
- [123] Yadav S., Vishwakarma V. P. (2019): "Extended interval type-II and kernel based sparse representation method for face recognition, In Expert Systems with Applications, Vol. 116, pp. 265–274, Elsevier BV, DOI:10.1016/j.eswa.2018.09.032
- [124] Dhikhi T., Rana A., Thakur A., Kapoor K. (2019): "Credit Card Transaction Based on Face Recognition Technology" Journal of Physics: Conference Series, vol.1362, no.1, pp.1-8, DOI:10.1088/1742-6596/1362/1/012109
- [125] Krishna K.P., Aithal P.S. (2018): "A Study on Fingerprint Hash Code Generation Based on MD5 Algorithm and Freeman Chain Code", International Journal of Computational Research and Development, Volume 3, Issue 1, pp.13-22, Available at SSRN: <https://ssrn.com/abstract=3100190>
- [126] Gaurang P., Debasis S. (2018): "A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security", Computers & Electrical Engineering, Vol. 69, pp. 461-478, DOI:10.1016/j.compeleceng.2018.01.028
- [127] Chun S.H. (2019): "E-commerce liability and security breaches in mobile payment for e-business sustainability", Sustainability, vol.11. DOI:10.3390/su11030715

[128] Zhang J., Luximon Y., Song Y. (2019): "The role of consumers' perceived security, perceived control, interface design features, and conscientiousness in continuous use of mobile payment services", Sustainability, vol.11. DOI: 10.3390/su11236843

[129] Argimbayeva G., Menasria I., Elshareif E., Lewis A.(2020): "The Impact of E- Wallet on ADNOC's Customer Satisfaction", In Proceedings of the 2020 the 11th International Conference on E-Education, E-Business, E-Management and E-Learning (IC4E 2020), Osaka, Japan, pp. 364–368. DOI: 10.1145/3377571.3377631

5. HIPOTEZE I ZADACI U ISTRAŽIVANJU

Hipoteze koje će biti proverene tokom istraživanja su:

H(1) – Moguće je razviti model biometrijske autentifikacije sa mogućnošću primene u post-COVID19 periodu u kojem je potrebno posvetiti brigu zdravstvenoj zaštiti.

H(2) – Moguće je razviti novu metodu za proveru autentifikacije korisnika platnih kartica sa PIN brojem koji je kreiran iz korisnikovih biometrijskih podataka.

H(3) – Metod biometrijske autentifikacije koji će se predstaviti transformiše biometrijske podatke u višeznamenasti PIN i u slučaju kada korisnik nosi masku na licu.

H(4) – Moguće je implementirati metodu biometrijske autentifikacije uz poboljšanje zaštite privatnosti biometrijskih podataka korisnika elektronskog plaćanja.

6. NAUČNE METODE ISTRAŽIVANJA

Da bi se potvrdile ili opovrgle postavljene hipoteze korišće se sledeće metode:

- analitičko-sintetičke,
- sistemski pristup,
- komparativni pristup,
- metode prikupljanja i analize postojećih naučnih rezultata,
- modeliranje i
- statističke metode.

Uradiće se sistematizacija dobijenih naučnih rezultata.

Posebne metode koje će se koristiti u istraživanju i evaulaciji postavljenih hipoteza su:

- Kritička analiza dostupne literature modela biometrijske autentifikacije.
- Upotreba statističkih metoda za analizu i prikaz rezultata.
- Analitičko-deduktivne metode korišće se za analizu podataka o postojećim modelima biometrijske autentifikacije.
- Metoda modeliranja korišće se za izradu modela biometrijske autentifikacije.
- Merenje relevantnih rezultata biće obavljeno pomoću standardnih statističkih metoda.

7. OČEKIVANI DOPRINOSI ISTRAŽIVAČKOG RADA

Doprinos istraživanja je novi model i metod biometrijske autentifikacije sa fokusom na parametre prilagodljivosti novim aplikacijama i bez obaveze čuvanja biometrijskog templejta. Istraživanje će unaprediti postojeće modele i metode biometrijske autentifikacije kako bi se prevazišla ograničenja kao što su visoki troškovi implementacije i rad u post-covid 19 periodu. Metoda koja će se razviti namenjena

je implementaciji u postojeću infrastrukturu elektronskog plaćanja sa ATM i POS uređajima koji imaju kamere. Istraživanje će se fokusirati na razvoj novog modela i metode biometrijske autentifikacije koji će biti fokusirani na očuvanje sigurnosti i zaštitu privatnosti. Očekivani doprinos istraživanja je i razvoj metode autentifikacije PIN-om koji se kreira iz biometrijskih podataka slike lica.

Ovaj metod bi trebalo da omogući autentifikaciju korisnika čak i kada korisnici nose zaštitnu masku, što je posebno važno u post-covid 19 periodu. Naučni doprinosi doktorske disertacije biće rezultati istraživanja iz oblasti biometrijske autentifikacije:

1. Doprinos razvoja nove metode biometrijske autentifikacije.
2. Doprinos razvoja novog modela biometrijske autentifikacije.
3. Komparativna analiza modela biometrijske autentifikacije.
4. Komparativna analiza metoda biometrijske autentifikacije.
5. Identifikacija ograničenja postojećih modela biometrijskih autentifikacije.
6. Verifikacija novog modela kroz realizaciju u laboratorijskom okruženju.

Društveni doprinos se odnosi na unapređenje sistema elektronskog plaćanja u post-COVID19 periodu.

8. PLAN ISTRAŽIVANJA I STRUKTURA RADA

Plan istraživanja

Okvirni plan istraživanja po fazama je prikazan u sledećoj tabeli:

Red. Broj	Faza istraživanja	Trajanje faze (meseci)
1	Prikupljanje relevantnih bibliografskih referenci	1
2	Analiza prikupljene literature i pregled trenutnog stanja u oblasti	1
3	Razvoj novog modela	6
4	Praktična realizacija modela	1
5	Eksperimentalna provera modela	1
6	Obrada podataka	1
7	Pisanje doktorske disertacije	1

Struktura istraživanja

Okvirni sadržaj doktorske disertacije je:

1. Uvod
 - 1.1. Problem i predmet istraživanja
 - 1.2. Cilj istraživanja i polazne hipoteze
 - 1.3. Struktura rada
2. Biometrija
 - 2.1 Fiziološki biometrijski modaliteti
 - 2.2 Bihejvioristički biometrijski modaliteti
 - 2.3 Kombinovani biometrijski modaliteti
 - 2.4 Biometrijski sistemi
 - 2.5 Multimodalna biometrija
3. Elektronski platni sistemi
 - 3.1 Prikaz savremenih elektronskih platnih sistema
 - 3.2 Postojeće stanje problema u elektronskim platnim sistemima
4. Modeli i metode autentifikacije
 - 4.1 Modeli autentifikacije u platnim sistemima
 - 4.2 Metode autentifikacije u platnim sistemima
5. Modelovanje biometrijske autentifikacije
 - 5.1 Predlog novog modela biometrijske autentifikacije
 - 5.2 Predlog nove metode biometrijske autentifikacije
 - 5.3 Adaptibilna metoda biometrijske autentifikacije
6. Praktična primena predloženog modela i nove metode biometrijske autentifikacije
 - 6.1 Dostupni podaci za komparaciju rezultata
 - 6.2 Testno okruženje
 - 6.3 Eksperimentalni rezultati
 - 6.4 Analiza eksperimentalnih rezultata
7. Pravci daljeg razvoja
8. Zaključak
9. Rečnik termina i skraćenica
10. Literatura

9. ZAKLJUČAK I PREDLOG

Uvidom u profesionalne, akademske i istraživačke kvalifikacije i kompetencije kandidata Nenada Badovinca, potpisani članovi Komisije su saglasni da ovaj kandidat ispunjava sve preduslove za rad na predloženoj temi doktorske disertacije. Članovi Komisije su takođe mišljenja da su predloženi ciljevi, hipoteze, metode, plan i struktura dokorskog istraživanja konzistentni s prethodno definisanim predmetom i problemom dokorskog istraživanja, kao i da logično slede rezultate pristupnog rada koji je kandidat Nenad Badovinac odbranio pred ovom Komisijom 10. jula 2023. godine.

Članovi Komisije su saglasni i predlažu da se kandidatu Nenadu Badovincu odobri izrada doktorske disertacije pod modifikovanim nazivom „**MODEL AUTENTIFIKACIJE KORISNIKA ZASNOVAN NA PRIMENI BIOMETRIJE U SISTEMIMA ELEKTRONSKOG PLAĆANJA**“.

Uža naučna oblast teme je: Informacione tehnologije.

Za mentora se predlaže: prof. dr Dejan Simić

Prof. dr Dejan Simić ispunjava sve uslove akreditacionih pravila visokoškolskih ustanova i dopunske kriterijume. Radovi koje je mentor objavio u poslednjih deset godina, a koji su u vezi s naučnom oblašću disertacije, priloženi su uz ovaj referat.

U Beogradu, 10.07.2023.

MENTOR

.....
Prof. dr Dejan Simić,
redovni profesor, Fakultet organizacionih nauka,
Univerzitet u Beogradu

ČLANOVI KOMISIJE

.....
Prof. dr Miroslav Minović,
redovni profesor, Fakultet organizacionih nauka,
Univerzitet u Beogradu

.....
Prof. dr Boško Nikolić,
redovni profesor, Elektrotehnički fakultet,
Univerzitet u Beogradu