

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Оцена научне заснованости теме докторске дисертације кандидата Данка Миладиновића, мастер инжењера електротехнике и рачунарства, под насловом „Употреба сигурних виртуелних машина за безбедно израчунавање више страна“.

Одлуком 266/35 бр. од 10.2.2026. године, именовани смо за чланове Комисије за оцену научне заснованости теме докторске дисертације кандидата Данка Миладиновића под насловом „Употреба сигурних виртуелних машина за безбедно израчунавање више страна“ (енг. *The Use of Secure Virtual Machines for Secure Multiparty Computation*). Чланови комисије за оцену научне заснованости теме докторске дисертације су се сагласили и предложили незнатну промену наслова предложене теме тако да гласи: „Развој модела за безбедно израчунавање више страна коришћењем сигурних виртуелних машина“ (енг. *Development of a Model for Secure Multi-Party Computation Using Secure Virtual Machines*)

На основу материјала приложеног уз Захтев кандидата, Комисија подноси следећи

ИЗВЕШТАЈ

1. Подаци о кандидату

1.1. Биографски подаци

Миладиновић Данко рођен је 01.02.1994. у Београду. Завршио је основу школу Бранко Радичевић, а потом је уписао и завршио Математичку гимназију.

Након завршене гимназије 2013. уписао је Електротехнички факултет, Универзитет у Београду, студијски програм Софтверско инжењерство. Током студија је био демонстратор на неколико предмета при Катедри за рачунарску технику и информатику. Дипломирао је 2017. године са просечном оценом 9,69. Дипломски рад „Развој конфигурабилне платформске 2Д видео-игре за два играча“ одбранио је са оценом 10.

Мастер академске студије на Електротехничком факултету у Београду, модул Софтверско инжењерство уписао је у октобру 2017. године. Током студија је био на пракси у фирми NVIDIA као софтверски инжењер. Мастер рад „Примена машинског учења у реализацији видео игре на Unity3D платформи“ је одбранио 2019. године са оценом 10. Просечна оцена на мастер студијама је 10,00.

Докторске академске студије на Електротехничком факултету у Београду уписао је школске 2019/2020, на модулу Рачунарска техника и информатика, и положио је све испите са просечном оценом 10,00. Током мастер и докторских студија објавио је један рад као први аутор у часопису са SCI листе и 8 научних радова на домаћим и страним конференцијама као аутор или коаутор.

Од школске 2017/2018. године почео је са радом на Електротехничком факултету у Београду као сарадник у настави, а од школске 2019/2020. као асистент. Тренутно је ангажован на предметима:

- Архитектура рачунара
- Основи рачунарске технике 2
- Архитектура и организација рачунара 2
- Микропроцесорски системи
- Развој безбедног софтвера
- Основи рачунарске технике 1
- Практикум из основа рачунарске технике.

Током периода у ком је запослен на Електротехничком факултету учествовао је на пројекту за развој система за безбедно израчунавање више страна *CoCoS.ai* и на међународном пројекту као предавач у оквиру УНДП програма за преквалификације у ИТ сектору, у организацији Електротехничког факултета у Београду.

1.2. Стечено научноистраживачко искуство

Данко Миладиновић је у свом истраживачком раду показао изузетно интересовање за област заштите података у употреби, са посебни нагласком на употребу сигурних виртуелних машина у безбедном израчунавању више страна.

Уписао је докторске академске студије школске 2019/2020. године на Електротехничком факултету Универзитета у Београду, на Модулу за рачунарску технику и информатику. Све испите предвиђене овим студијским програмом положио је са просечном оценом 10,00 и остварио 120 ЕСПБ. Списак положених испита приказан је у табели која следи:

Назив предмета	Оцена	ЕСПБ	Датум полагања испита
(19Д111ОПА) Одабрана поглавља из архитектуре рачунарских система	10	9	26.06.2023.
(19Д111ВИЕ) Вештачка интелигенција и експертски системи	10	9	18.09.2023.
(19Д111МИ) Медицинска информатика	10	9	22.09.2023.
(19Д111ИП) Интернет програмирање	10	9	28.08.2024.
(19Д111ММС) Мултимедијални системи - одабрана поглавља	10	9	30.08.2024.
(19Д111ССР) Софтверски системи за рад у реалном времену	10	9	06.09.2024.
(19Д111ВС) Виртуелна стварност	10	9	06.09.2024.
(19Д111РМС) Развој микропроцесорског софтвера	10	9	28.10.2025.
(19Д111АПС) Архитектуре за подршку софтверским системима	10	9	28.10.2025.
(19Д091УНР) Увод у научни рад	10	6	28.10.2025.

Досадашњи резултати кандидата приказани су кроз више публикација на домаћим и међународним конференцијама, као и једног рада у часопису са SCI листе. У наставку следи списак публикација на којима је Данко Миладиновић аутор/коаутор:

Радови у часописима са SCI листе (M20):

1. D. Miladinović, A. Milaković, M. Vukasović, Ž. Stanisavljević, P. Vuletić, **Secure Multiparty Computation Using Secure Virtual Machines**, Electronics, Vol. 13, No. 5, pp. 1 - 25, Mar, 2024, doi: 10.3390/electronics13050991. [M22]
ISSN: 2079-9292

Радови на међународним конференцијама (M30):

1. I. Kulic, P. Vuletic and D. Miladinovic, **Early Attestation of the Confidential Virtual Machine with Full Disk Encryption Support**, 2025 33rd Telecommunications Forum (TELFOR), pp. 1-4, Belgrade, Serbia, 2025 [M33]
ISBN: 979-8-3315-9357-5
2. T. Radaljac, D. Miladinović, Ž. Stanisavljević and P. Vuletić, **Secure Distributed Computing in Cloud Using Trusted Execution Environments**, 2024 32nd Telecommunications Forum (TELFOR), Belgrade, Serbia, November 2024, pp. 1-4, doi: 10.1109/TELFOR63250.2024.10819070. [M33]
ISBN: 979-8-3503-9106-0
3. M. Dodović, M. Ogrizović, D. Miladinović, D. Drašković, **Enhancing Sentiment Analysis in Product Reviews: Fine-Tuning BERT for Class Imbalance and Optimal Sequence Representation**, Disruptive Information Technologies for a Smart Society. ICIST 2024. Lecture Notes in Networks and Systems, vol 860, pp. 348 - 359, Springer, Cham, Serbia, September, 2024. [M33]
ISBN: 978-3-031-71419-1
4. D. Miladinović, J. Popović, N. Korolija, **The Evolution of Big Data Analytics Solutions in the Cloud**, 2022 9th International Conference on Electrical, Electronic and Computing Engineering IcETRAN 2022 (IcETRAN), pp. 600 - 606, ETRAN Society, Novi Pazar, Serbia, Jun, 2022. [M33]
ISBN: 978-86-7466-930-3
5. D. Miladinović, M. Bojović, V. Jelisavčić, N. Korolija, **Hybrid Manycore Dataflow Processor**, 2022 9th International Conference on Electrical, Electronic and Computing Engineering IcETRAN 2022 (IcETRAN), pp. 606 - 611, ETRAN Society, Novi Pazar, Serbia, Jun, 2022. [M33]
ISBN: 978-86-7466-930-3
6. Đ. Madić, D. Miladinović, Ž. Stanisavljević, **A Comparison of Selected Systems For Learning About SQLi Vulnerability Suitable for Academic Uses**, 2022 9th International Conference on Electrical, Electronic and Computing Engineering IcETRAN 2022 (IcETRAN), pp. 784 - 789, Novi Pazar, Srbija, Jun, 2022. [M33]
ISBN: 978-86-7466-930-3
7. M. Vukasović, D. Miladinović, A. Milaković, P. Vuletić, Ž. Stanisavljević, **Programming Applications Suitable for Secure Multiparty Computation Based on Trusted Execution Environments**, 2022 30th Telecommunications Forum (TELFOR), Belgrade, Serbia, 2022, pp. 1-4, Belgrade, Nov, 2022. [M33]
ISBN: 978-1-6654-7273-9

Радови на домаћим конференцијама (M60):

1. Т. Радаљац, Д. Миладиновић, П. Вулетић, Ж. Станисављевић, **Упоредна анализа перформанси Google Cloud и локалне инфраструктуре**, 2025 LXIX конференција ЕТРАН, Друштво за ЕТРАН, Београд и Академска мисао, pp. 241-246, Београд, Чачак, Јун, 2025. [M63]
ISBN: 978-86-6200-032-3

На основу члана 101. Статута Универзитета у Београду, члана 74. Статута Универзитета у Београду-Електротехничког факултета и захтева студента, одобрено је продужење рока за

завршетак студија до истека троструког броја школских година потребних за реализацију уписаног студијског програма.

1.3. Оцена подобности кандидата за рад на предложеној теми

Кандидат је испунио све обавезе предвиђене наставним планом и програмом докторских студија: Студијски истраживачки рад I (15 ЕСПБ), Студијски истраживачки рад II (15 ЕСПБ) и Научно стручни рад (3 ЕСПБ). Такође, кандидат је до тренутка писања овог извештаја објавио један рад у научном часопису са SCI листе као првопотписани аутор, те три рада на међународним конференцијама који су из области поверљивог рачунарства (енг. *confidential computing*), односно коришћења модерних процесорских енклава за заштиту података током обраде.

Дана 24.02.2026. године, кандидат Данко Миладиновић је на Електротехничком факултету Универзитета у Београду усмено полагао испит о подобности предложене теме докторске дисертације и кандидата (докторски испит), пред комисијом у саставу:

- проф. др Павле Вулетић, доктор електротехничких наука, редовни професор, Електротехнички факултет, Универзитет у Београду
- проф. др Ненад Јовичић, доктор електротехничких наука, ванредни професор, Електротехнички факултет, Универзитет у Београду
- проф. др Дејан Симић, доктор електротехничких наука, редовни професор, Факултет организационих наука, Универзитет у Београду

На јавној усменој одбрани предложене теме Комисија је кандидата оценила оценом **задовољно**.

Разматрајући претходно приказане резултате досадашњег рада кандидата Данка Миладиновића и, узимајући у обзир све положене испите и стручне обавезе током докторских студија, успешну одбрану теме докторске дисертације, као и до сада објављене научне радове, Комисија је утврдила да је кандидат показао да је стекао неопходно искуство за самосталан научно-истраживачки рад. Комисија је мишљења да је кандидат способан да током израде докторске дисертације оствари резултате и доприносе који могу бити приказани и верификовани од стране међународне научне заједнице. Комисија сматра да кандидат Данко Миладиновић испуњава све суштинске и формалне услове да приступи изради докторске дисертације на предложеној теми.

2. Предмет и циљ истраживања

Предмет истраживања је проблем сигурне обраде података на уређајима трећих страна каква се среће у окружењима инфраструктура у облаку (енг. *cloud infrastructure*). Сигурна обрада података подразумева да подаци ни у једном тренутку нису видљиви неауторизованим актерима. Оно за шта постоје решења већ дуже време су заштита података током мировања (енг. *data at rest*) енкрипцијом на диску и заштита података током преноса (енг. *data in transit*) различитим сигурним комуникационим протоколима. У случају да се обрада података врши у оквиру инфраструктуре која је у власништву компаније за коју се развија апликација која ће обрађивати податке, онда није потребна додатна заштита поред поменутих.

Проблем настаје када се за потребе апликације користе алгоритми за обраду података који захтевају велику процесорску моћ, попут алгоритама машинског учења и/или вештачке интелигенције. С обзиром на то да је у овом случају често превише скупо да се успостави

сопствена инфраструктура, једно од решења које се појавило у претходном периоду је коришћење инфраструктуре у облаку. Иако овакав приступ економски има смисла, увођење новог ентитета у сигурносни модел, у овом случају пружаоца услуга у облаку (енг. *cloud provider*), захтева и додатни ниво заштите података. Наиме, користећи рачунарство у облаку, корисници могу да изнајме инфраструктуру са довољно јаком процесорском снагом да обраде податке [1], али то подразумева да приступ њиховим подацима сада има и пружалац услуга у облаку и то чак и када је примењена заштита података током мировања и приликом преноса. Подаци у том случају нису заштићени у тренутку када се нађу у оперативној меморији приликом извршавања апликације, па их неки злонамерни пружалац услуга у облаку, или неки његов злонамерни запослени, може тада видети у оригиналном облику.

Како би власник података био уверен да су подаци потпуно сигурни у претходно описаној ситуацији, они морају да се заштите и током њихове обраде (енг. *data in use*) [2]. Заштита података током обраде је могућа или коришћењем криптографских техника попут хомоморфне енкрипције [3] или од недавно коришћењем хардверски подржаних сигурних окружења за извршавање (енг. *trusted execution environment*), на пример *AMD Secure Encrypted Virtualization (SEV)* [4] или *Intel TDX*. Сигурна окружења за извршавање имају значајно боље перформансе у односу на хомоморфну енкрипцију, која у овом тренутку није на нивоу који би омогућио њену практичну употребу за сложенија израчунавања, због сложености извођења и потребе отклањања нагомиланог шума.

Коришћењем заштите података у мировању, преносу и обради, власник података може да заштити своје податке и од злонамерног пружаоца услуга у облаку. Најновије технологије сигурних окружења извршавања омогућавају корисницима да заштите целе виртуелне машине. Овако заштићене виртуелне машине се називају и сигурне виртуелне машине. Сигурне виртуелне машине, у комбинацији са заштитом података у преносу и мировању, омогућавају нове сценарије извршавања у облаку. Један од тих сценарија је безбедно израчунавање више страна (енг. *secure multiparty computation*) за које такође постоје решења заснована на криптографским механизмима која су лоших перформанси [8]. У овом сценарију више учесника једног конзорцијума би послало своје податке, а један од њих би послао свој алгоритам у сигурну виртуелну машину. Послати алгоритам би затим обрадио послате податке, при чему би била обезбеђена приватност послатих података, односно свака страна би имала увид само у своје податке [10] и резултате обраде, али не и у податке других страна или сам алгоритам. Тренутно један од перспективних начина да се имплементира безбедно израчунавање више страна, управо је коришћење сигурних виртуелних машина, али је потребно решити бројне изазове попут креирања и покретања проверљиво сигурне верзије оперативног система, провере интегритета окружења за извршавање виртуелних машина кроз атестацију од стране свих учесника, спречавања превара од стране појединих потенцијално малициозних учесника конзорцијума који учествују у израчунавању, успостављања поверења свих учесника и слично.

Главни циљ овог истраживања је развој новог модела и система за безбедно израчунавање више страна коришћењем сигурних виртуелних машина. Поред тога, како би главни циљ био постигнут додатни циљеви истраживања су: свеобухватна анализа различитих механизма за безбедно израчунавање више страна, компаративна анализа различитих технологија за успостављање окружења за сигурно извршавање [11], развоја система за безбедну комуникацију између сигурне виртуелне машине и учесника израчунавања [12], као и анализа сигурности и перформанси новог модела [15] и система за безбедно израчунавање више страна коришћењем сигурних виртуелних машина.

Значај овог истраживања јесте потенцијални развој система који може да се користи да унапреди пословање и истраживања у различитим областима, како у приватном, тако и у јавном сектору [16] где је недостатак капацитета за све сложенија рачунарска израчунавања све израженији. Један од случајева коришћења оваквог система јесте здравство [19], где би више болница могло да удружи приватне податке својих пацијената како би извршили

опсежнију анализу над овим подацима у циљу ефикасније дијагностике различитих болести, али уз потпуно очување приватности података. Други пример могућег коришћења оваквих система јесте банкарство [20]. Различите банке би могле да на безбедан начин удруже своје податке и тако анализирају трансакције својих корисника коришћењем система за безбедно израчунавање више страна и на тај начин детектују потенцијалне преваре, без откривања осетљивих пословних података конкуренцији.

Најрелевантније референце из отворене литературе у вези са тезом су:

- [1] Chen, K. Confidential High-Performance Computing in the Public Cloud. *IEEE Internet Comput* **2023**, 27, 24–32, doi:10.1109/MIC.2022.3226757.
- [2] Rashid, F.Y. The Rise of Confidential Computing: Big Tech Companies Are Adopting a New Security Model to Protect Data While It's in Use - [News]. *IEEE Spectr* **2020**, 57, 8–9, doi:10.1109/MSPEC.2020.9099920.
- [3] Ogburn, M., Turner, C., & Dahal, P. (2013). Homomorphic encryption. *Procedia Computer Science*, vol. 20, pp. 502-509, 2013
- [4] Peisert, S. Trustworthy Scientific Computing. *Commun ACM* **2021**, vol. 64, no. 5, pp. 18–21, May, 2021, doi:10.1145/3457191.
- [5] Kaplan, D. Protecting VM Register State with SEV-ES. *White paper* **2017**, 13.
- [6] Sev-Snp, A.M.D. Strengthening VM Isolation with Integrity Protection and More. *White Paper*, January **2020**, 53, 1450–1465.
- [7] Slemmer, A.; Deml, S. Swiss Cheese to Cheddar: Securing AMD SEV-SNP Early Boot Available online: <https://www.decentriq.com/article/swiss-cheese-to-cheddar-securing-amd-sev-snp-early-boot> (accessed on 30 January 2024).
- [8] Evans, D.; Kolesnikov, V.; Rosulek, M. A Pragmatic Introduction to Secure Multi-Party Computation. *Foundations and Trends® in Privacy and Security* **2018**, 2, 70–246, doi:10.1561/33000000019.
- [9] El-Hindi, M.; Ziegler, T.; Heinrich, M.; Lutsch, A.; Zhao, Z.; Binnig, C. Benchmarking the Second Generation of Intel SGX Hardware. In *Proceedings of the Proceedings of the 18th International Workshop on Data Management on New Hardware; Association for Computing Machinery: New York, NY, USA*, vol. 10322, pp 477–497, 2022.
- [10] Yang, Y.; Huang, X.; Liu, X.; Cheng, H.; Weng, J.; Luo, X.; Chang, V. A Comprehensive Survey on Secure Outsourced Computation and Its Applications. *IEEE Access* **2019**, 7, 159426–159465.
- [11] Mo, J.; Gopinath, J.; Reagen, B. HAAC: A Hardware-Software Co-Design to Accelerate Garbled Circuits. In *Proceedings of the Proceedings of the 50th Annual International Symposium on Computer Architecture; 2023*; pp. 1–13.
- [12] Sardar, M.U.; Musaev, S.; Fetzer, C. Demystifying Attestation in Intel Trust Domain Extensions via Formal Verification. *IEEE access* **2021**, 9, 83067–83079.
- [13] Coker, G., Guttman, J., Loscocco, P., Herzog, A., Millen, J., O'Hanlon, B., Ramsdell, J., Segall, A., Sheehy, J. and Sniffen, B., 2011. Principles of remote attestation. *International journal of information security*, vol. 10, no. 2, pp.63-81.
- [14] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and Pan, W., “Remote ATtestation procedureS (RATS) Architecture,” RFC 9334, Jan. 2023, doi: 10.17487/RFC9334.
- [15] Akram, A.; Giannakou, A.; Akella, V.; Lowe-Power, J.; Peisert, S. Performance Analysis of Scientific Computing Workloads on General Purpose TEEs. In *Proceedings of the 2021 IEEE International Parallel and Distributed Processing Symposium (IPDPS); IEEE, January 2021*; pp. 1066–1076.
- [16] Laud, P.; Kamm, L.; Veeningen, M. *Applications of Secure Multiparty Computation*; Ios Press, 2015; Vol. 13;.
- [17] Volgushev, N.; Schwarzkopf, M.; Getchell, B.; Varia, M.; Lapets, A.; Bestavros, A. Conclave: Secure Multi-Party Computation on Big Data. In *Proceedings of the Proceedings of*

the Fourteenth EuroSys Conference 2019; Association for Computing Machinery: New York, NY, USA, 2019.

- [18] Bahmani, R.; Barbosa, M.; Brasser, F.; Portela, B.; Sadeghi, A.-R.; Scerri, G.; Warinschi, B. Secure Multiparty Computation from SGX. In: 2017; pp. 477–497.
- [19] Ahammed, M. F., & Labu, M. R. (2024). Privacy-preserving data sharing in healthcare: advances in secure multiparty computation. *Journal of Medical and Health Studies*, vol. 5, no. 2, pp. 37-47.
- [20] Bogdanov, D.; Talviste, R.; Willemson, J. Deploying Secure Multi-Party Computation for Financial Data Analysis: (Short Paper). In Proceedings of the Financial Cryptography and Data Security: 16th International Conference, FC 2012, Kralendijk, Bonaire, February 27-March 2, 2012, Revised Selected Papers 16; 2012; pp. 57–64.

3. Полазне хипотезе

Предложено истраживање полази од следећих хипотеза:

- Безбедно израчунавање више страна коришћењем сигурних виртуелних машина надмашује друге приступе предложене у научној литератури по добијеним перформансама.
- Безбедно израчунавање више страна коришћењем сигурних виртуелних машина надмашује друге приступе предложене у научној литератури по добијеној сигурности.
- Технологија доступна за успостављање сигурних виртуелних машина се може сматрати поузданом.
- Употреба сигурних виртуелних машина за успостављање сигурних окружења за извршавање надмашује друге технологије по добијеним перформансама.
- Употреба сигурних виртуелних машина за успостављање сигурних окружења за извршавање надмашује друге технологије по добијеној сигурности.
- Могуће је имплементирати модел и систем за безбедно израчунавање више страна коришћењем сигурних виртуелних машина који ће бити употребљив у реалним случајевима коришћења.

4. Научне методе истраживања

Предложене методе истраживања укључују свеобухватни преглед научне литературе о могућим решењима за безбедно израчунавање више страна, уз посебан фокус на истраживању примене сигурних виртуелних машина за безбедно израчунавање више страна, као и предности и недостатке оваквог приступа у односу на алтернативне приступе. Након тога, биће истражене технологије које омогућавају успостављање сигурних окружења за извршавање. И овде ће бити направљена претрага постојеће научне литературе, али и спецификација произвођача конкретних технологија уз посебан фокус на начинима формирања и секвенци покретања сигурне виртуелне машине, као и предностима и недостатцима ове технологије у односу на друге приступе. Затим ће бити извршена сигурносна анализа саме технологије и процени степена зрелости и ограничења под којим се технологија може користити. По завршетку спроведених анализа биће осмишљен нови модел за безбедно израчунавање више страна коришћењем сигурних виртуелних машина, а потом и имплементиран систем у виду прототипа осмишљеног модела. На крају ће бити спроведене одговарајуће анализе осмишљеног модела и то: анализа перформанси и анализа сигурности.

5. Очекивани научни допринос

Очекује се да доприноси овог рада буду:

- Преглед и свеобухватна анализа постојећих механизма за безбедно израчунавање више страна.

- Преглед и свеобухватна анализа постојећих технологија за успостављање сигурних окружења за извршавање.
- Креирање модела за безбедно израчунавање више страна коришћењем сигурних виртуелних машина.
- Дефинисање сигурног начина за комуникацију између корисника и сигурне виртуелне машине, кроз укључивање атестација у сигурносну комуникацију између учесника у безбедном израчунавању више страна са сигурном виртуелном машином.
- Сигурносна подешавања кернела сигурне виртуелне машине како би се пружила додатна подршка сигурним виртуелним машинама.
- Формална евалуација сигурности осмишљеног модела за безбедно израчунавање више страна коришћењем сигурних виртуелних машина.
- Експериментална евалуација имплементираног система за безбедно израчунавање више страна коришћењем сигурних виртуелних машина кроз тестирање перформанси са различитим алгоритмима и подацима отвореног приступа, као и тестирање система са различитим алгоритмима за машинско учење.

6. План истраживања и структура рада

Истраживање је предвиђено да се састоји од следећих корака:

- Претрага литературе и анализа постојећих механизма за безбедно израчунавање више страна.
- Претрага и компаративна анализа различитих технологија за успостављање сигурних окружења за извршавање са фокусом на технологији која се ће се користити за развој прототипа решења.
- Истраживање различитих начина креирања сигурних виртуелних машина, као и укључивање подршке за заштиту података приликом мировања и током преноса.
- Анализа различитих начина сигурне, атестиране комуникације између учесника безбедног израчунавања више страна са сигурном виртуелном машином. Биће описан рад истражених решења и биће упоређене предности и мане истражених решења.
- Дефинисање модела за безбедно израчунавање више страна коришћењем сигурних виртуелних машина. Биће дефинисан протокол комуникације између сигурне виртуелне машине и свих учесника безбедног израчунавања више страна који треба да укључи и сигурну комуникацију између учесника и сигурне виртуелне машине.
- Имплементација система за безбедно израчунавање више страна коришћењем сигурних виртуелних машина, што подразумева имплементацију алата за комуникацију са сигурном виртуелном машином, имплементацију алата који ће се извршавати у сигурној виртуелној машини, као и креирање саме сигурне виртуелне машине.
- Евалуација осмишљеног модела и имплементираног система. За модел ће бити спроведена формална евалуација сигурности, док ће за систем бити извршена мерења брзине извршавања различитих алгоритама у оквиру сигурне виртуелне машине како би се анализом добијених резултата утврдило у којој мери је предложено решење спорије у односу на обичне виртуелне машине.

7. Закључак и предлог

На основу приложене документације и стеченог целокупног утиска о теми докторске дисертације и досадашњег научног рада кандидата Данка Миладиновића, мастер инжењера електротехнике и рачунарства, Комисија је дошла до следећих закључака:

1. Кандидат испуњава све формалне и суштинске потребне услове прописане Законом о високом образовању, Статутом Универзитета у Београду и Статутом Електротехничког факултета Универзитета у Београду, за израду докторске дисертације.
2. Чланови Комисије за оцену научне заснованости теме су се сагласили и предложили незнатну промену наслова предложене теме кандидата Данка Миладиновића тако да уместо пресложеног наслова „Употреба сигурних виртуелних машина за безбедно израчунавање више страна“ гласи: „Развој модела за безбедно израчунавање више страна коришћењем сигурних виртуелних машина“ (енг. *Development of a Model for Secure Multi-Party Computation Using Secure Virtual Machines*).
3. Предложена тема **„Развој модела за безбедно израчунавање више страна коришћењем сигурних виртуелних машина“** јесте научно заснована и савремена, а резултати који ће проистећи израдом ове докторске дисертације представљаће значајан и оригиналан допринос међународној научној заједници. Тема припада ужој научној области Рачунарска техника и информатика.

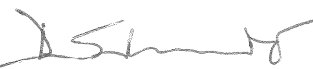
На основу свега претходно изложеног, Комисија са задовољством предлаже Наставно-научном већу Електротехничког факултета Универзитета у Београду да кандидату Данку Миладиновићу одобри израду докторске тезе под насловом **„Развој модела за безбедно израчунавање више страна коришћењем сигурних виртуелних машина“** (енг. *Development of a Model for Secure Multi-Party Computation Using Secure Virtual Machines*), под менторством др Жарка Станисављевића, ванредног професора Електротехничког факултета Универзитета у Београду.

У Београду, 26.2.2026.

ЧЛАНОВИ КОМИСИЈЕ



др Павле Вулећић, редовни професор
Универзитет у Београду – Електротехнички факултет



др Дејан Симић, редовни професор
Универзитет у Београду – Факултет организационих наука



др Ненад Јовичић, ванредни професор
Универзитет у Београду – Електротехнички факултет