

## УНИВЕРЗИТЕТ У БЕОГРАДУ

Факултет организационих наука

### НАСТАВНО-НАУЧНОМ ВЕЋУ

**Предмет:** Подобност теме и кандидата Милоша Живадиновића за израду докторске дисертације

Одлуком Наставно-научног већа Факултета организационих наука-Универзитета у Београду 05-01 бр. 3/38-8 од 26.03.2026. године именовани смо за чланове Комисије за преглед и одбрану приступног рада и оцену научне заснованости теме докторске дисертације кандидата **Милоша Живадиновића** под насловом:

**„Модел примене хомоморфне енкрипције на обуку система вештачке интелигенције”**

На основу материјала приложеног уз Захтев кандидата, Комисија подноси следећи

### ИЗВЕШТАЈ

#### 1. Подаци о кандидату

##### 1.1. Биографски подаци

Милош Живадиновић рођен је 06.08.1993. године у Београду. Завршио је Пету београдску гимназију у Београду, а Факултет организационих наука - смер Информациони системи и технологије уписује 2012. године. Завршио га је 2016. године са просечном оценом 8,84, а дипломирао исте године одбравивши дипломски рад „Употреба Керберос аутентикације у дистрибуираном телеметријском систему“. Исте године уписује мастер студије на Факултету организационих наука - смер Информационе технологије које завршава 2017. године са просеком 9,86. Одбранио је мастер рад 2017. године са темом „Управљање криптографским кључевима заснованих на *blockchain* технологији“. Докторске студије уписао је 2022. године на Факултету организационих наука - смер Информациони системи и технологије. Тренутни просек Милоша Живадиновића на докторским студијама је 10,00.

Од октобра 2015. до јануара 2016. године био је сарадник ван радног односа у оквиру Катедре за информационе технологије где је изводио вежбе из предмета Архитектура рачунара и оперативни системи, као и из предмета Рачунарске мреже и телекомуникације.

Од августа 2016. године до фебруара 2018. године био је запослен у компанији *NCR* на позицији *Sales Engineer*, док је од фебруара 2018. године до септембра 2019. године био запослен у компанији *FIS* на позицији *Senior Software Engineer*. У септембру 2019. године постаје запослен у компанији *United.Cloud* на позицији *Lead Software Engineer*, до јануара 2021. године када прелази у компанију *Oracle* на позицију *Senior Solutions Engineer*. Милош је био запослен у компанији *Oracle* до октобра 2025. године када прелази у *AIK Bank* на позицију *AI Solutions Expert*.

## 1.2. Стечено научноистраживачко искуство

У наставку ће бити приказане научноистраживачке активности кандидата. Оне обухватају радове објављене на конференцијама и у часописима, активности у извођењу наставе и преглед положених испита.

Током досадашњег рада Милош Живадиновић је објавио више радова у земљи и иностранству и учествовао на више међународних и домаћих скупова и конференција.

### **Зборници међународних научних скупова - М30**

- М. Živadinović, I. Milenković, and D. Simić, "Seraphim: Linux kernel module for resource management and command execution," *Proceedings of the XIV International Symposium of Organizational Sciences - Symorg2014*, Zlatibor, Srbija, Jun 2014.
- М. Živadinović, I. Milenković, and D. Simić, "Open source algorithms performance on unconstrained facial images," *Proceedings of the 1st EWG-DSS International Conference on Decision Support System Technology - ICDSSST 2015*, Beograd, Srbija, Maj 2015.
- М. Živadinović, I. Milenković, and D. Simić, "Cash, hash or trash - Hash function impact on system security," *Proceedings of the XV International Symposium of Organizational Sciences - Symorg2016*, Zlatibor, Srbija, Jun 2016.
- М. Živadinović and D. Simić, "Framework for verifying documents on the blockchain," *Proceedings of the XVI International Symposium of Organizational Sciences - Symorg2018*, Zlatibor, Srbija, 2018.
- М. Živadinović, "Application of Large Language Models for text mining: study of ChatGPT," *7th International Scientific Conference ITEMA 2023 – Selected Papers*, Dec. 2023.
- М. Živadinović, "Application of LLMs for Solving Algorithm Coding Tests in Recruitment," *LIMEN 2023 / 9 – Leadership, Innovation, Management and Economics: Integrated Politics of Research - SELECTED PAPERS*, Dec. 2023.
- М. Živadinović and D. Simić, "Blockchain-Based AI Model Integrity and Verification Framework," *Proceedings of the 19th International Symposium of Organizational Sciences - Symorg2024*, Zlatibor, Srbija, Jun 2024.
- М. Živadinović and D. Simić, "Resource efficient Internet-of-Things intrusion detection with spiking neural networks," *19th Conference on Computer Science and Intelligence Systems*, Beograd, Srbija. doi: [10.15439/2024F8800](https://doi.org/10.15439/2024F8800).
- М. Živadinović and D. Simić, "Blockchain-Based AI Model Integrity and Verification Framework," *Unlocking the Hidden Potentials of Organization Through Merging of Humans and Digitals*, vol. 1 Lecture Notes in Networks and Systems, no. 1680, vol. 1., Springer Nature Switzerland. [Online]. Dostupno: <https://link.springer.com/book/10.1007/978-3-032-08093-6>

### **Радови објављени у часописима националног значаја (M52)**

- B. Marčeta and M. Živadinović, “Softverski definisane mreže - simulacija virtuelne računarske mreže upotrebom Mininet okruženja,” *InfoM*, no. 62/2017, pp. 34–39, 2017.

### **Саопштења са скупова националног значаја штампана у целини (M63)**

- M. Živadinović, I. Milenković, D. Starčević, and D. Simić, “Unapređenje bezbednosti Linux operativnog sistema primenom Seraphim kernel modula,” *Infotech 2014*, Arandelovac, Srbija, Jun 2014.
- Milenković and M. Živadinović, “Uticaj rezolucije slike na preciznost prepoznavanja lica,” *Infotech 2015*, Arandelovac, Srbija, Jun 2015.
- M. Živadinović, I. Milenković, and D. Simić, “Klasifikacija i korišćenje mobilnih uređaja za potrebe biometrije,” *ITEO 2015*, Banjaluka, Bosna i Hercegovina.
- Milenković, M. Živadinović, and D. Simić, “Poređenje rešenja otvorenog koda za prepoznavanje lica,” *ITEO 2015*, Banjaluka, Bosna i Hercegovina.
- M. Živadinović, I. Milenković, and D. Simić, “Izmenjena Bitcoin arhitektura kao sredstvo evidentiranja bankarskih transakcija,” *Infotech 2016*, Arandelovac, Srbija, Jun 2016.
- M. Živadinović, “Upotreba blockchain tabela u zaštiti integriteta podataka,” *Zbornik radova 28. IKT konferencija YUINFO 2022*, Kopaonik, Srbija, Mar. 2022.
- M. Živadinović and D. Simić, “Klasifikacija blokova na Ethereum blockchain-u primenom Multi-Layer Perceptron neuronske mreže i deep learninga,” *Zbornik radova 29. IKT konferencija YUINFO 2023*, Kopaonik, Srbija, Mar. 2023.
- M. Živadinović and D. Simić, “Utvrđivanje neispravnih odgovora od strane ChatGPT,” *Zbornik radova 30. IKT konferencija YUINFO 2024*, Kopaonik, Srbija, Mar. 2024.
- M. Živadinović and D. Simić, “Neuromorfno računarstvo i tačne mašine stanja u sistemima za otkrivanje upada nad CIC-IDS2017 skupom podataka,” *Zbornik radova 31. IKT konferencija YUINFO 2025*, Kopaonik, Srbija, Mar. 2025.
- M. Živadinović and D. Simić, “Primena velikih jezičkih modela u naučnom istraživanju,” *SYMOPIS 2025*, Palić, Srbija, Sept. 2025.

Следи списак положених предмета на докторским студијама са оценама и ЕСПБ бодовима:

Редни број	Ознака предмета	Назив предмета	Оцена	ЕСПБ
1	Д22057	Напредне биометријске технологије	10 (десет)	10
2	Д22078	Расположивост, балансирање оптерећења и виртуелизација	10 (десет)	10
3	Д22100	Технологије управљања подацима	10 (десет)	10
4	Д22046	Методе заштите у електронском пословању – одабрана поглавља	10 (десет)	10
5	Д22085	Системи заштите информационих система	10 (десет)	10
6	Д22027	Интеракција човека и рачунара – одабрана поглавља	10 (десет)	10
7	Д22082	Савремена истраживања у области информационих система и технологија	10 (десет)	10
8	Д22064	Одабрана поглавља из техника заштите у рачунарским мрежама	10 (десет)	10
9	Д22021	Заштита рачунарских система – одабрана поглавља	10 (десет)	10

Кандидат је дана 09.04.2026. године успешно одбранио приступни рад за израду докторске дисертације под називом „Модел примене хомоморфне енкрипције на обуку система вештачке интелигенције”.

### 1.3. Оцена подобности кандидата за рад на предложеној теми

Узимајући у обзир:

- резултате остварене током досадашњег образовања;
- резултате истраживања на тему биометрије, *blockchain* технологије, безбедности оперативних система и рачунарских мрежа, примене великих језичких модела који су публиковани на научно-стручним конференцијама и у часописима;
- радно искуство у примени савремених информационих система и вештачке интелигенције;

закључује се да је Милош Живадиновић у потпуности квалификован и припремљен да тему докторске дисертације самостално истражује и да оствари научно-стручне доприносе у тој области.

## **2. Предмет и циљ истраживања**

Предмет овог истраживања је изводљивост модела примене хомоморфне енкрипције на системе вештачке интелигенције који би омогућио безбедан начин обуке и дељења података за обуку.

Истраживање обухвата дефинисање начина рада модела кроз успостављање корака од почетне активације модела до употребе обученог система вештачке интелигенције над хомоморфно

шифрованим подацима. Као део даљег истраживања, неопходно је утврдити потпуне критеријуме и применљивост различитих хомоморфних шема које се користе за очување безбедности и приватности података.

У домену дистрибуиране обуке вештачке интелигенције потребно је поставити претпоставке система, као и начине рада са више врста хомоморфних шема и различитим системима вештачке интелигенције.

Општи циљ овог истраживања је развој модела примене хомоморфне енкрипције на системе вештачке интелигенције уз очување безбедности и приватности података учесника који се користе за обуку.

Постављени општи циљ остварује се кроз реализацију следећих специфичних циљева. Први специфични циљ односи се на критичку анализу постојећих приступа дистрибуиране обуке система вештачке интелигенције са идентификацијом ограничења у контексту општих система вештачке интелигенције.

Други специфични циљ представља анализу концепата хомоморфног шифровања, парцијалних и потпуних шема хомоморфног шифровања и развој смерница и показне архитектуре хомоморфних шема за поступке усклађивања података обуке и обуку система вештачке интелигенције.

Трећи специфични циљ је поставка, развој и експериментална примена решења заснованог на описаном моделу примене хомоморфне енкрипције на обуку система вештачке интелигенције. Резултат овог специфичног циља може се сматрати прототипом решења које имплементира већ поменути модел у више конфигурација. Предмет рада представљају детекција аномалија и колаборативно одређивање података.

Остваривањем постављених циљева доприноси се развоју теоретских основа и практичних решења у области дистрибуиране обуке система вештачке интелигенције, превазилазећи ограничења установљена мањком безбедности и мањком тајности корисничких података који се користе у системима вештачке интелигенције.

Почетна листа библиографских извора који ће се користити приликом израде докторске дисертације:

- [1] OpenAI, "ChatGPT." Accessed: Jul. 18, 2023. [Online]. Available: <https://chat.openai.com>
- [2] "Google Scholar." Accessed: Dec. 21, 2025. [Online]. Available: <https://scholar.google.com/>
- [3] "Semantic Scholar | AI-Powered Research Tool." Accessed: Dec. 21, 2025. [Online]. Available: <https://www.semanticscholar.org/>
- [4] "ResearchRabbit: AI Tool for Smarter, Faster Literature Reviews." Accessed: Dec. 21, 2025. [Online]. Available: <https://www.researchrabbit.ai>
- [5] I. Damgård, M. Jurik, and J. B. Nielsen, "A generalization of Paillier's public-key system with applications to electronic voting," *Int. J. Inf. Secur.*, vol. 9, no. 6, pp. 371–385, Dec. 2010, doi: 10.1007/s10207-010-0119-9.
- [6] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *Advances in Cryptology — EUROCRYPT '99*, J. Stern, Ed., Berlin, Heidelberg: Springer, 1999, pp. 223–238. doi: 10.1007/3-540-48910-X\_16.
- [7] Y. Wu, S. Cai, X. Xiao, G. Chen, and B. C. Ooi, "Privacy preserving vertical federated learning for tree-based models," *Proc. VLDB Endow.*, vol. 13, no. 12, pp. 2090–2103, Aug. 2020, doi: 10.14778/3407790.3407811.
- [8] H. Wang, Q. Wang, Y. Ding, S. Tang, and Y. Wang, "Privacy-preserving federated learning based on partial low-quality data," *J. Cloud Comput.*, vol. 13, no. 1, p. 62, Mar. 2024, doi: 10.1186/s13677-024-00618-8.



- [9] Y. Zhang *et al.*, “Reparable threshold Paillier encryption scheme for federated learning,” *Soft Comput.*, vol. 29, no. 7, pp. 3659–3664, May 2025, doi: 10.1007/s00500-025-10640-w.
- [10] K. Cheng *et al.*, “SecureBoost: A Lossless Federated Learning Framework,” Apr. 07, 2021, *arXiv*: arXiv:1901.08755. doi: 10.48550/arXiv.1901.08755.
- [11] T. Fan, W. Chen, G. Ma, Y. Kang, L. Fan, and Q. Yang, “SecureBoost+: Large Scale and High-Performance Vertical Federated Gradient Boosting Decision Tree,” Jun. 19, 2024, *arXiv*: arXiv:2110.10927. doi: 10.48550/arXiv.2110.10927.
- [12] L. Xie, J. Liu, S. Lu, T. Chang, and Q. Shi, “An Efficient Learning Framework For Federated XGBoost Using Secret Sharing And Distributed Optimization,” *ACM Trans. Intell. Syst. Technol.*, vol. 13, no. 5, pp. 1–28, Oct. 2022, doi: 10.1145/3523061.
- [13] F. Zhang, L. Wang, C. Cui, Q. Meng, and M. Yang, “EVFeX: An efficient vertical federated XGBoost algorithm based on optimized secure matrix multiplication,” *Signal Process.*, vol. 227, p. 109686, Feb. 2025, doi: 10.1016/j.sigpro.2024.109686.
- [14] Y. Guo *et al.*, “Efficient and Privacy-Preserving Federated Learning based on Full Homomorphic Encryption,” Mar. 18, 2024, *arXiv*: arXiv:2403.11519. doi: 10.48550/arXiv.2403.11519.
- [15] J. H. Cheon, A. Kim, M. Kim, and Y. Song, “Homomorphic Encryption for Arithmetic of Approximate Numbers,” in *Advances in Cryptology – ASIACRYPT 2017*, vol. 10624, T. Takagi and T. Peyrin, Eds., in Lecture Notes in Computer Science, vol. 10624. , Cham: Springer International Publishing, 2017, pp. 409–437. doi: 10.1007/978-3-319-70694-8\_15.
- [16] H. Sun, Y. Zhang, Z. Xu, R. Zhang, and M. Li, “MK-FLFNN: A Privacy-Preserving Vertical Federated Learning Framework For Heterogeneous Neural Network Via Multi-Key Homomorphic Encryption,” *2023 26th Int. Conf. Comput. Support. Coop. Work Des. CSCWD*, pp. 552–558, May 2023, doi: 10.1109/CSCWD57460.2023.10152691.
- [17] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. 2016.
- [18] C. J. C. H. Watkins and P. Dayan, “Q-learning,” *Mach. Learn.*, vol. 8, no. 3, pp. 279–292, May 1992, doi: 10.1007/BF00992698.
- [19] F. Rosenblatt, “Perceptron Simulation Experiments,” *Proc. IRE*, vol. 48, no. 3, pp. 301–309, Mar. 1960, doi: 10.1109/JRPROC.1960.287598.
- [20] “DLMF: §1.16 Distributions ▶ Topics of Discussion ▶ Chapter 1 Algebraic and Analytic Methods.” Accessed: Oct. 24, 2025. [Online]. Available: <https://dlmf.nist.gov/1.16#iv>
- [21] S. R. Dubey, S. K. Singh, and B. B. Chaudhuri, “Activation Functions in Deep Learning: A Comprehensive Survey and Benchmark,” Jun. 28, 2022, *arXiv*: arXiv:2109.14545. Accessed: Feb. 24, 2023. [Online]. Available: <http://arxiv.org/abs/2109.14545>
- [22] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, “Learning representations by back-propagating errors,” *Nature*, vol. 323, no. 6088, pp. 533–536, Oct. 1986, doi: 10.1038/323533a0.
- [23] G. F. Simmons, *Calculus with analytic geometry*, 2. ed. New York, NY: McGraw-Hill, 1996.
- [24] G. Cybenko, “Approximation by superpositions of a sigmoidal function,” *Math. Control Signals Syst.*, vol. 2, no. 4, pp. 303–314, Dec. 1989, doi: 10.1007/BF02551274.
- [25] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet Classification with Deep Convolutional Neural Networks,” in *Advances in Neural Information Processing Systems*, Curran Associates, Inc., 2012. Accessed: Oct. 24, 2025. [Online]. Available: [https://proceedings.neurips.cc/paper\\_files/paper/2012/hash/c399862d3b9d6b76c8436e924a68c45b-Abstract.html](https://proceedings.neurips.cc/paper_files/paper/2012/hash/c399862d3b9d6b76c8436e924a68c45b-Abstract.html)
- [26] H. Cunningham, A. Ewart, L. Riggs, R. Huben, and L. Sharkey, “Sparse Autoencoders Find Highly Interpretable Features in Language Models,” Oct. 04, 2023, *arXiv*: arXiv:2309.08600. doi: 10.48550/arXiv.2309.08600.
- [27] R. C. Staudemeyer and E. R. Morris, “Understanding LSTM -- a tutorial into Long Short-Term Memory Recurrent Neural Networks,” Sep. 12, 2019, *arXiv*: arXiv:1909.09586. Accessed: Feb. 24, 2023. [Online]. Available: <http://arxiv.org/abs/1909.09586>

- [28] A. Vaswani *et al.*, “Attention is All you Need,” presented at the Neural Information Processing Systems, Jun. 2017. Accessed: Dec. 10, 2023. [Online]. Available: <https://www.semanticscholar.org/paper/Attention-is-All-you-Need-Vaswani-Shazeer/204e3073870fae3d05bcbc2f6a8e263d9b72e776>
- [29] Y. LeCun *et al.*, “Backpropagation Applied to Handwritten Zip Code Recognition,” *Neural Comput.*, vol. 1, no. 4, pp. 541–551, Dec. 1989, doi: 10.1162/neco.1989.1.4.541.
- [30] D. H. Hubel and T. N. Wiesel, “Receptive fields of single neurones in the cat’s striate cortex,” *J. Physiol.*, vol. 148, no. 3, pp. 574–591, Oct. 1959, doi: 10.1113/jphysiol.1959.sp006308.
- [31] J. J. Hopfield, “Neural networks and physical systems with emergent collective computational abilities,” *Proc. Natl. Acad. Sci.*, vol. 79, no. 8, pp. 2554–2558, Apr. 1982, doi: 10.1073/pnas.79.8.2554.
- [32] P. J. Werbos, “Backpropagation through time: what it does and how to do it,” *Proc. IEEE*, vol. 78, no. 10, pp. 1550–1560, Oct. 1990, doi: 10.1109/5.58337.
- [33] K. Cho *et al.*, “Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation,” Sep. 03, 2014, *arXiv*: arXiv:1406.1078. doi: 10.48550/arXiv.1406.1078.
- [34] M. J. White, “GPU prices and availability (Q3 2025): How much are GPUs today?,” *Digital Trends*. Accessed: Nov. 02, 2025. [Online]. Available: <https://www.digitaltrends.com/computing/gpu-price-tracking/>
- [35] Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated Machine Learning: Concept and Applications,” Feb. 13, 2019, *arXiv*: arXiv:1902.04885. doi: 10.48550/arXiv.1902.04885.
- [36] C. Gentry, “Computing arbitrary functions of encrypted data,” *Commun. ACM*, vol. 53, no. 3, pp. 97–105, Mar. 2010, doi: 10.1145/1666420.1666444.
- [37] R. L. Rivest, L. Adleman, and M. L. Dertouzos, “ON DATA BANKS AND PRIVACY HOMOMORPHISMS”, 1978.
- [38] T. ElGamal, “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” in *Advances in Cryptology*, G. R. Blakley and D. Chaum, Eds., Berlin, Heidelberg: Springer, 1985, pp. 10–18. doi: 10.1007/3-540-39568-7\_2.
- [39] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, 1978.
- [40] S. Goldwasser and S. Micali, “Probabilistic encryption,” *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, Apr. 1984, doi: 10.1016/0022-0000(84)90070-9.
- [41] I. Damga and M. Jurik, “A Generalisation, a Simplification and Some Applications of Paillier’s Probabilistic Public-Key System”, *BRICS Rep. Ser.*, Dec. 2000.
- [42] L. G. Valiant, “Completeness classes in algebra,” in *Proceedings of the eleventh annual ACM symposium on Theory of computing*, in STOC ’79. New York, NY, USA: Association for Computing Machinery, Apr. 1979, pp. 249–261. doi: 10.1145/800135.804419.
- [43] C. Krüger and B. Moriya, “A Performance Comparison of the Homomorphic Encryption Schemes CKKS and TFHE”, *Pap. 20251460*, 2025.
- [44] *microsoft/SEAL*. (Feb. 16, 2026). C++. Microsoft. Accessed: Feb. 16, 2026. [Online]. Available: <https://github.com/microsoft/SEAL>
- [45] *homenc/HElib*. (Feb. 13, 2026). C++. homenc. Accessed: Feb. 16, 2026. [Online]. Available: <https://github.com/homenc/HElib>
- [46] “OpenFHE.org – OpenFHE – Open-Source Fully Homomorphic Encryption Library.” Accessed: Feb. 16, 2026. [Online]. Available: <https://openfhe.org/>
- [47] F. Boemer, Y. Lao, R. Cammarota, and C. Wierzynski, “nGraph-HE: A Graph Compiler for Deep Learning on Homomorphically Encrypted Data,” Apr. 02, 2019, *arXiv*: arXiv:1810.10121. doi: 10.48550/arXiv.1810.10121.
- [48] N. Dowlin, R. Gilad-Bachrach, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, “CryptoNets: Applying Neural Networks to Encrypted Data with High Throughput and Accuracy”, 2016.

- [49] C. Juvekar, V. Vaikuntanathan, and A. Chandrakasan, "GAZELLE: A Low Latency Framework for Secure Neural Network Inference," presented at the 27th USENIX Security Symposium (USENIX Security 18), 2018, pp. 1651–1669. Accessed: Feb. 16, 2026. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity18/presentation/juvekar>
- [50] B. Reagen *et al.*, "Cheetah: Optimizing and Accelerating Homomorphic Encryption for Private Inference," Oct. 08, 2020, *arXiv*: arXiv:2006.00505. doi: 10.48550/arXiv.2006.00505.
- [51] Q. Pang, J. Zhu, H. Möllering, W. Zheng, and T. Schneider, "BOLT: Privacy-Preserving, Accurate and Efficient Inference for Transformers," in *2024 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA: IEEE, May 2024, pp. 4753–4771. doi: 10.1109/SP54263.2024.00130.
- [52] "Home - FATE." Accessed: Jan. 12, 2026. [Online]. Available: <https://fate.readthedocs.io/en/latest/>
- [53] "PySyft: Data Science on data you are not allowed to see," Syft Documentation. Accessed: Jan. 12, 2026. [Online]. Available: <https://docs.openmined.org/en/latest/index.html>
- [54] "NVIDIA FLARE," NVIDIA Developer. Accessed: Jan. 12, 2026. [Online]. Available: <https://developer.nvidia.com/flare>
- [55] "Flower Framework Documentation," Flower. Accessed: Jan. 12, 2026. [Online]. Available: <https://flower.ai/docs/framework/index.html>
- [56] "IBM watsonx.ai and watsonx.governance." Accessed: Jan. 12, 2026. [Online]. Available: <https://www.ibm.com/docs/en/watsonx/w-and-w/2.1.0?topic=solutions-federated-learning>

### 3. Полазне хипотезе

#### 3.1 Општа хипотеза

Могуће је развити и математички формализовати модел примене хомоморфне енкрипције на обуку система вештачке интелигенције.

#### 3.2 Помоћне хипотезе

X1 - Могуће је дефинисати архитектуру модела примене хомоморфне енкрипције на обуку система вештачке интелигенције. Предложена архитектура омогућава различитим учесницима безбедан начин обуке система вештачке интелигенције и његову дистрибуцију без дешифровања података.

X2 – Комбинацијом хомоморфних шема за усклађивање података и за обуку система вештачке интелигенције могуће је успоставити механизме који омогућавају и гарантују безбедност података који припадају појединачном учеснику, онемогућавајући осталим учесницима увид у дешифроване податке приликом њихове обраде.

### 4. Научне методе истраживања

Опште научне методе истраживања које ће бити употребљене јесу аналитичко-синтетичка, дедуктивно логичка, системски приступ и компаративни приступ.

Посебне методе које ће се користити за реализацију истраживања и евалуацију постављених хипотеза су:

- Преглед и анализа расположиве литературе која припада научним областима релевантним за предмет истраживања
- Критичка анализа тренутног стања дистрибуиране обуке вештачке интелигенције
- Експериментална провера предложеног модела развојем прототипа решења и његово тестирање



- Развој математичког модела који обухвата понашање модела примене хомоморфне енкрипције на обуку вештачке интелигенције кроз формализацију елемената система и њихових међуодноса.

## 5. Очекивани научни, стручни и друштвени доприноси

Очекивани научни доприноси овог рада су следећи:

- Преглед и систематизација литературе у области дистрибуиране обуке система вештачке интелигенције
- Преглед и систематизација литературе у области хомоморфне енкрипције
- Развој модела примене хомоморфне енкрипције на обуку система вештачке интелигенције
- Развој архитектуре модела примене хомоморфне енкрипције на обуку система вештачке интелигенције
- Развој прототипа модела примене хомоморфне енкрипције на обуку система вештачке интелигенције.

Очекивани стручни доприноси овог рада су:

- Развој прототипа модела примене хомоморфне енкрипције на обуку система вештачке интелигенције који може бити примењен у индустријским окружењима
- Дефинисање скупа критеријума и смерница за одабир одговарајућих хомоморфних шема у зависности од контекста примене система вештачке интелигенције
- Развој референтне архитектуре за имплементацију система приватности података у дистрибуираним системима вештачке интелигенције применљивих у доменама финансија, здравства и телекомуникација
- Експериментална евалуација перформанси модела који пружа практичне смернице за будуће имплементације и итерације модела
- Допринос стандардизацији приступа приватне обуке система вештачке интелигенције кроз успостављање формалних критеријума усклађености са заштитом података о личности

Друштвени доприноси резултата истраживања односе се на могућност решавања различитих друштвених проблема, од којих су најважнији:

- Унапређење заштите података о личности у системима вештачке интелигенције који обрађују осетљиве податке чиме се доприноси поштовању људских права
- Омогућавање безбедне сарадње између организација које располажу осетљивим подацима (здравствене установе, финансијске институције, државни органи) без потребе за централизацијом или откривањем података трећим лицима

- Смањење препрека за ширу примену вештачке интелигенције у регулисаним индустријама, што дугорочно може допринети унапређењу квалитета услуга у здравству, јавној управи и финансијском сектору
- Допринос развоју етичке и одговорне вештачке интелигенције кроз механизме смањивања изложености података и контроле власника над сопственим подацима
- Подршка развоју дигиталних компетенција и истраживачког капацитета у области напредне криптографије и приватности у системима вештачке интелигенције кроз научне радове, истраживања, конференције и софтверска решења.

## 6. План истраживања и структура рада

План истраживања докторске дисертације приказан је у следећој табели:

		Meseci trajanja											
		1	2	3	4	5	6	7	8	9	10	11	12
Faze izrade doktorske disertacije	Faza 1	■	■										
	Faza 2		■	■									
	Faza 3				■								
	Faza 4					■							
	Faza 5						■	■					
	Faza 6								■	■			
	Faza 7										■	■	■
	Faza 8										■	■	■

Табела 1 План истраживања

Фазе израде докторске дисертације са њиховим трајањем по табели су описане испод:

Фаза 1 - Прикупљање релевантних библиографских референци: месеци 1 и 2

Фаза 2 - Анализа прикупљене литературе са прегледом тренутног стања: месеци 2 и 3

Фаза 3 - Установљивање модела примене хомоморфне енкрипције на обуку система вештачке интелигенције: месец 4

Фаза 4 - Развој архитектуре прототипа модела примене хомоморфне енкрипције на обуку система вештачке интелигенције: месец 5

Фаза 5 - Развој прототипа модела примене хомоморфне енкрипције на обуку система вештачке интелигенције: месеци 6 и 7

Фаза 6 - Тестирање и евалуација прототипа у различитим условима рада: месеци 8 и 9

Фаза 7 - Израда текста докторске дисертације: месеци 10, 11 и 12

Фаза 8 - Публикација резултата истраживања: месеци 10, 11 и 12

Оквирно, структуру докторске дисертације сачињаваће следећа поглавља:

1. Увод
  - 1.1. Предмет и циљ истраживања
  - 1.2. Полазне хипотезе
  - 1.3. Структура дисертације
2. Системи вештачке интелигенције
  - 2.1. Машинско учење
  - 2.2. Неуронске мреже
  - 2.3. Дубоко учење
3. Хомоморфна енкрипција
  - 3.1. Основни концепти
  - 3.2. Парцијална хомоморфна енкрипција
  - 3.3. Потпуна хомоморфна енкрипција
4. Модел примене хомоморфне енкрипције на обуку система вештачке интелигенције
  - 4.1. Претпоставке окружења модела
  - 4.2. Дефиниција и начин рада модела
  - 4.3. Анализа применљивости модела
5. Спецификација корисничких захтева
  - 5.1. Примена модела за детекцију аномалија
  - 5.2. Примена модела за колаборативно одређивање података
6. Архитектура имплементације модела
  - 6.1. Генеричка архитектура модела примене хомоморфне енкрипције на обуку система вештачке интелигенције
  - 6.2. Архитектура модела примене хомоморфне енкрипције на обуку система вештачке интелигенције у домену детекције аномалија
  - 6.3. Архитектура модела примене хомоморфне енкрипције на обуку система вештачке интелигенције у домену колаборативног одређивања података
7. Развој прототипа предложених архитектура модела
  - 7.1. Развој прототипа решења примене хомоморфне енкрипције на обуку система вештачке интелигенције у домену детекције аномалија
  - 7.2. Развој прототипа решења примене хомоморфне енкрипције на обуку система вештачке интелигенције у домену колаборативног одређивања података
8. Евалуација перформанси прототипа примене хомоморфне енкрипције на обуку система вештачке интелигенције у домену детекције аномалија
9. Евалуација перформанси прототипа примене хомоморфне енкрипције на обуку система вештачке интелигенције у домену колаборативног одређивања података
10. Закључак
11. Литература

## 7. Закључак и предлог

Из изложеног се може закључити да кандидат Милош Живадиновић испуњава све услове предвиђене Законом о високом образовању за одобрење израде докторске дисертације под насловом **„Модел примене хомоморфне енкрипције на обуку система вештачке интелигенције”**.

Милош Живадиновић поседује неопходна знања из заштите података у савременим пословним системима, *blockchain* технологије, примене криптографије и великих језичких модела за успешан рад на докторској дисертацији.

Тема припада ужој научној области Информационе технологије и актуелна је. Добијени резултати могу допринети унапређењу заштите података, побољшањем пре свега сигурности

у системима у којима се примењује вештачка интелигенција и могу имати практичну примену у делу обуке система вештачке интелигенције.

На основу свега наведеног, комисија предлаже Наставно-научном већу да прихвати предложену тему и одобри израду пријављене докторске дисертације. За ментора докторске дисертације предлаже се др Дејан Симић, редовни професор Факултета организационих наука, Универзитета у Београду.

#### ЧЛАНОВИ КОМИСИЈЕ:

---

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

---

др Мирослав Миновић, редовни професор  
Факултет организационих наука  
Универзитет у Београду

---

др Борис Делибашић, редовни професор  
Факултет организационих наука  
Универзитет у Београду

---

др Иван Миленковић, доцент  
Факултет организационих наука  
Универзитет у Београду

---

др Бошко Николић, редовни професор  
Електротехнички факултет  
Универзитет у Београду

Београд, 09.04.2026.