УНИВЕРЗИТЕТ У НОВОМ САДУ **ОБРАЗАЦ – 4**
ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА

ИЗВЕШТАЈ О ОЦЕНИ ПОДОБНОСТИ ТЕМЕ, КАНДИДАТА И МЕНТОРА ЗА ИЗРАДУ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

I ПОДАЦИ О КОМИСИЈИ

Орган који је именовао комисију: Наставно-научно веће Факултета техничких наука

Датум именовања комисије: 25.12.2025.

Састав комисије именоване у складу са *Правилима докторских студија Универзитета у Новом Саду*:

1.	др Гилезан Силвиа	Редовни професор	Теоријска и примењена математика
	презиме и име	звање	ужа научна област
	Факултет техничких наука, Нови Сад		Председник
	установа у којој је запослен-а		функција у комисији
2.	др Огњановић Зоран	Научни саветник	Математичке науке
	презиме и име	звање	ужа научна област
	Математички институт САНУ		Члан
	установа у којој је запослен-а		функција у комисији
3.	др Гајић Душан	Ванредни професор	Примењене рачунарске науке и информатика
	презиме и име	звање	ужа научна област
	Факултет техничких наука, Нови Сад		Члан
	установа у којој је запослен-а		функција у комисији
4.	др Маринковић Весна	Ванредни професор	Рачунарство и информатика
	презиме и име	звање	ужа научна област
	Математички факултет, Београд		Члан
	установа у којој је запослен-а		функција у комисији
5.	др Прокић Иван	Доцент	Теоријска и примењена математика
	презиме и име	звање	ужа научна област
	Факултет техничких наука, Нови Сад		Члан
	установа у којој је запослен-а		функција у комисији

II ПОДАЦИ О КАНДИДАТУ

1. Име, име једног родитеља, презиме: Милица, Милош, Кнежевић
2. Датум рођења: 20.3.1980. Место и држава рођења: Бајина Башта, Србија

II.1 Основне или интегрисане студије

Година уписа: 1999 Година завршетка: 2005 Просечна оцена током студија: 9,07

Универзитет: Универзитет у Београду

Факултет: Математички факултет

Студијски програм: Рачунарство и информатика

Стечено звање: дипломирани математичар

II.2 Мастер или магистарске студије

Година уписа: 2015 Година завршетка: 2015 Просечна оцена током студија: 9,67

Универзитет: Универзитет у Новом Саду

Факултет: Факултет техничких наука

Студијски програм: Математика у техници

Стечено звање: мастер инжењер примењене математике

Научна област: математика

Наслов завршног рада: Мере сличности XML података и примене у откривању дупликата

II.3 Докторске студије

Година уписа: 2016

Универзитет: Универзитет у Новом Саду

Факултет: Факултет техничких наука

Студијски програм: Математика у техници

Број ЕСПБ до сада остварених: 120 Просечна оцена током студија: 10,00

II.4 Приказ научних и стручних радова кандидата

Р. бр.	аутори, наслов рада, *часопис*, **волумен** (година) странице од-до, DOI или ISBN/ISSN	категорија
1.	**Knežević, M.**, Tomović, S., & Mihaljević, M. J. Attack Scenarios and Security Analysis of a Blockchain and PUF-based Lightweight Authentication Protocol for Wireless Medical Sensor Networks. *IEEE Internet of Things Journal,* **12**(23), 2025, 51010-51025, doi:10.1109/JIOT.2025.3612005	M21a+
Рад припада проблематици докторске дисертације:	**ДА** НЕ ДЕЛИМИЧНО	

Р. бр.	аутори, наслов рада, *часопис*, **волумен** (година) странице од-до, DOI или ISBN/ISSN	категорија
2.	Mihaljević, M. J., **Knežević, M.**, Urošević, D., Wang, L., & Xu, S. An approach for blockchain and symmetric keys broadcast encryption based access control in IoT. *Symmetry,* **15**(2), 2023, 299. doi:10.3390/sym15020299	M21
Рад припада проблематици докторске дисертације:	**ДА** НЕ ДЕЛИМИЧНО	

Р. бр.	аутори, наслов рада, *часопис*, **волумен** (година) странице од-до, DOI или ISBN/ISSN	категорија
3.	Mihaljević, M. J., Todorović, M., & **Knežević, M**. An evaluation of power consumption gain and security of flexible green pool mining in public blockchain systems. *Symmetry,* **15**(4), 2024, 924. doi:10.3390/sym15040924	M21
Рад припада проблематици докторске дисертације:	ДА НЕ **ДЕЛИМИЧНО**	

Р. бр.	аутори, наслов рада, *часопис*, **волумен** (година) странице од-до, DOI или ISBN/ISSN	категорија
4.	Tomović, S., **Knežević, M.**, & Mihaljević, M. J. Analysis and correction of the attack against the LPN-problem based authentication protocols. *Mathematics,* **9**(5), 2021, 573. doi:10.3390/math9050573	M21a+
Рад припада проблематици докторске дисертације:	ДА НЕ **ДЕЛИМИЧНО**	

Р. бр.	аутори, наслов рада, *часопис*, **волумен** (година) странице од-до, DOI или ISBN/ISSN	категорија
5.	**Knežević, M.**, Tomović, S., & Mihaljević, M. J. Man-in-the-middle attack against certain authentication protocols revisited: Insights into the approach and performances re-evaluation. *Electronics,* **9**(8), 2020, 1296. doi:10.3390/electronics9081296	M22
Рад припада проблематици докторске дисертације:	ДА НЕ **ДЕЛИМИЧНО**	

Р. бр.	аутори, наслов рада, *часопис*, **волумен** (година) странице од-до, DOI или ISBN/ISSN	категорија
6.	Todorović, M., **Knežević, M.**, Ševerdija, D., Jelić, S., & Mihaljević, M. J. Implementation Framework of a Blockchain Based Infrastructure for Electricity Trading Within a Microgrid. In *Collaborative Computing: Networking, Applications and Worksharing. LNICS,* **561**, 2024, 38-53 doi:10.1007/978-3-031-54521-4_3	M33
Рад припада проблематици докторске дисертације: ДА НЕ **ДЕЛИМИЧНО**		

III ОЦЕНА ПОДОБНОСТИ ТЕМЕ

Оцена:

III.1 формулације наслова тезе

Дизајн и безбедносне карактеристике аутентификационих протокола заснованих на блокчејн приступима

Комисија сматра да је предложени наслов тезе подобан.

Предложени наслов тезе је подобан? ДА

III.2 предмета (проблема) истраживања

Аутентификација је процес провере идентитета корисника, уређаја и система, и кључна је за безбедну комуникацију. Аутентификациона решења су доминантно централизована и ослањају се на трећу страну од поверења, задужену за регистрацију корисника, управљање креденцијалима и проверу идентитета. Међутим, кроз децентрализацију се могу умањити ризици који настају као последица SPoF (Single Point of Failure), а блокчејн приступи се истичу као алтернатива која уклања потребу за централним ауторитетом.

Истраживања у области аутентификационих протокола заснованих на блокчејн приступима претежно су усмерена на нове предлоге дизајна у којима се више, а понекад и сви, кораци аутентификације измештају на блокчејн. У неким решењима приметан је имплицитни циљ максимизације употребе блокчејна без јасних критеријума оправданости, што може довести до кашњења у извршавању или трошкова који нису у складу са реалним захтевима система. Стога је неопходно пажљивом анализом идентификовати делове процеса чијом се интеграцијом са блокчејном постиже стварна корист.

Једно од недовољно истражених питања је могућност примене блокчејн технологије као средства за спречавање конкретних, претходно идентификованих напада и недостатака постојећих аутентификационих протокола. Истраживања су претежно фокусирана на дизајн потпуно нових протокола у које се блокчејн укључује у циљу децентрализације система, а без директног повезивања са специфичним рањивостима. Насупрот томе, испитивање могућности употребе блокчејна за унапређење безбедности постојећих протокола, кроз прецизно циљање утврђених недостатака, представља релевантан, а недовољно истражен правац.

Приметан је чест изостанак софтверске имплементације предложених протокола на адекватно одабраној блокчејн платформи, као и експерименталне анализе са циљем утврђивања практичне примењивости и реалистичности решења. Стога је тешко проверити тврдње о изводљивости и ефикасности решења и упоредити међусобно конкурентне предлоге протокола. Ово мотивише приступ евалуацији протокола који подразумева софтверску имплементацију, доступност изворног кода и експерименталну валидацију.

Комисија сматра да је предмет истраживања подобан за израду докторске дисертације, с обзиром на актуелност и научну релевантност теме, која има потенцијал да донесе нове научне доприносе и отвара даље правце за нова истраживања.

Предмет истраживања је подобан? ДА

III.3 познавања проблематике на основу изабране литературе са списком литературе

Бројна су истраживања која испитују и показују потенцијал блокчејн технологије као интегралне компоненте у дизајну аутентификационих протокола. Препознато је да кључне карактеристике блокчејна, а то су децентрализација, транспарентност и непроменљивост, пружају потенцијал за унапређење безбедности и поузданости аутентификационих система.

У [1] дат је предлог протокола који се заснива на конзорцијумском Hyperledger Fabric блокчејну и токену LiIDCoin (Lightweight IDentity Coin) који представља средство за верификацију идентитета. Све трансакције у мрежи односе се на управљање LiIDCoin токеном.

Решење из [2] имплементира двофакторску аутентификацију корисника за приступ сензорским подацима где је додатно средство провере OTP (One-Time-Password) токен. Генерисање, дистрибуција и верификација токена је децентрализована кроз Ethereum блокчејн и паметне уговоре.

Радови [3][4] решавају проблем централизованости аутентификације у паметним електроенергетским мрежама (енг. smart grid). Регистрација је у [3] централизована, а аутентификација децентрализована кроз Hyperledger блокчејн и паметне уговоре. Протокол [4] омогућава узајамну аутентификацију бројила и провајдера услуга, а паметни уговор управља иницијализацијом система, генерисањем кључева и провером идентитета. Један од најновијих протокола за smart grid [5] усмерен је на побољшање перформанси и безбедности.

AgroMobiBlock [6] омогућава аутентификацију и безбедно дељење података прикупљених сензорима у системима паметне пољопривреде користећи специјализоване блокове AuthCred за чување кредицијала и SensorData за податке са сензора.

EBCPA [7] и BCGS [8] су аутентификациони протоколи за VANET (Vehicle Ad-hoc Network) фокусирани на условну приватност, која подразумева анонимност корисника осим у случају безбедносних или законских захтева. У EBCPA [7] RSU (Road Side Units) одржавају блокчејн, а кроз паметни уговор се управља кључевима и аутентификацијом. Јавни кључеви су анонимни, а једино овлашћени ентитет Менаџер може открити идентитет учесника. Возила се аутентификују кроз ZKP (Zero-Knowledge Proof) доказе, показујући поседовање одговарајућег тајног кључа. За имплементацију су разматрани Ethereum и Hyperledger Fabric. BCGS [8] решава међудоменску аутентификацију возила. Условна приватност се постиже групним потписима које издаје доменски Менаџер. Hyperledger Fabric блокчејн и паметни уговори користе се само за аутентификацију међу ентитетима из различитих домена.

BUAMH [9] је намењен за аутентификацију и управљање кључевима у FANET (Flying Ad-Hoc Networks). BUAMH се ослања на паметне уговоре за иницијализацију система, генерисање криптографских кључева, регистрацију ентитета и управљање листом учесника по задацима. Користи конзорцијумски блокчејн са прилагођеном структуром блока и нови ICM (Identity Consensus Mechanism) консензус базиран на PBFT (Practical Byzantine Fault Tolerance), са фокусом на верификацију идентитета и додељених задатака.

У [10] дат је протокол за паметне куће где су аутентификација, провера права приступа и бележење аутентификационих догађаја реализовани кроз паметне уговоре на конзорцијумском блокчејну.

EPIoT [11] је децентрализовани оквир у ком власници IoT уређаја могу подешавати поставке приватности и права приступа подацима. Регистрација, аутентификација и управљање правима приступа реализују се кроз паметне уговоре. За имплементацију је одабран Quorum, грана Ethereum-а намењена реализацији затворених система.

Поуздано повезивање ентитета са њима припадајућим јавним кључевима, остварује се кроз PKI (Public Key Infrastructure) оквир, који омогућава и аутентификацију путем криптографских кључева. Традиционална PKI ослања се на сертификационо тело (Certificate Authority - CA) које издаје сертификат за јавни кључ након провере припадајућег власника кључа. Оваква архитектура је централизована и подразумева апсолутно поверење у CA. Неке децентрализоване PKI архитектуре ослањају се на блокчејн како би омогућиле јавну и независну верификацију сертификата и спречиле њихово фалсификовање. Једна децентрализована PKI која се ослања на IOTA блокчејн дата је у [12]. IOTA користи Tangle структуру, која представља усмерени ациклични граф а не блокчејн ланац, и пружа бољу скалабилност и трансакције без накнаде.

ProofChain [13] и D2XChain [14] користе Ethereum блокчејн и задржавају компатибилност са X.509 стандардом.

SemiDec-PKI [15] и ETHERST [16] имплементирају Web of Trust модел помоћу Ethereum блокчејна. Оба решења укључују механизме награде и казне, имплементиране помоћу Ethereum ERC-20 токена, којима се стимулише поштено понашање. Додатно, SemiDec-PKI подржава различите врсте сертификата не фокусирајући се искључиво на SSL/TLS сертификате.

Аутентификациони протоколи за RFID, технологију бежичне идентификације и праћења објеката, активна су и изазовна истраживачка област због ограничених ресурса RFID уређаја (тагова). Протоколи из [17] и [18] инспирисали су многа каснија истраживања. Након што је криптоанализа [19][20] показала рањивости протокола [17], он је даље унапређиван у [21], [22], [23]. Идеје из [18] послужиле су као референтно полазиште за нове протоколе [21], [24], [25].

Актуелни тренд у дизајну lightweight аутентификационих протокола је употреба Physically Unclonable Functions (PUF). PUF је једносмерна функција која за дати challenge (улаз) даје response (излаз) и служи као дигитални „отисак прста“ уређаја. Примери неких аутентификациона решења која, поред блокчејн компоненте, укључују и PUF су дати у [26], [27], [28], [29].

Истраживање у тези ће се усредсредити и на тему и резултате из [30-43].

[1] Zhang, Y. et al. (2022). A Lightweight Authentication Scheme Based on Consortium Blockchain for Cross-Domain IoT. *Secur. Commun. Netw.*, 2022, 9686049.

[2] Abubakar, M. et al. (2022). A lightweight and user-centric two-factor authentication mechanism for IoT based on blockchain and smart contract. *Proc. SMARTTECH*, 91–96.

[3] Wang, J. et al. (2019). Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. *IEEE Trans. Ind. Inform.*, 16(3), 1984-1992.

[4] Wang, W. et l. (2021). Secure and efficient mutual authentication protocol for smart grid under blockchain. *Peer-to-Peer Netw. Appl.*, 14(5), 2681-2693.

[5] Ponnuru, R. B. et al. (2025). Robust authentication and key agreement protocol for smart microgrid environment. *J. Inf. Secur. Appl.*, 94, 104202.

[6] Vangala, A. et al. (2023). Blockchain-enabled authenticated key agreement scheme for mobile vehicles-assisted precision agricultural IoT networks. *IEEE Trans. Inf. Forensics Secur.*, 18, 904–919.

[7] Lin, C., Huang, X., & He, D. (2023). EBCPA: Efficient blockchain-based conditional privacy-preserving authentication for VANETs. *IEEE Trans. Dependable Secure Comput.*, 20(3), 1818–1832.

[8] Chen, B. et al. (2023). BCGS: Blockchain-assisted privacy-preserving cross-domain authentication for VANETs. *Veh. Commun.*, 41, 100602.

[9] Xie, H. et al. (2024). A blockchain-based ubiquitous entity authentication and management scheme with homomorphic encryption for FANET. *Peer-to-Peer Netw. Appl.*, 17(2), 569–584.

[10] Yang, H., Guo, Y., & Guo, Y. (2024). Blockchain-based cloud-fog collaborative smart home authentication scheme. *Comput. Netw.*, 242, 110240.

[11] Kashif, M., & Kalkan, K. (2024). EPIoT: Enhanced privacy preservation based blockchain mechanism for internet-of-things. *Comput. Netw.*, 238, 110107.

[12] Wang, S. et al. (2022). DAG blockchain-based lightweight authentication and authorization scheme for IoT devices. *J. Inf. Secur. Appl.*, 66, 103134.

[13] Saleem, T. et al. (2022). ProofChain: An X. 509-compatible blockchain-based PKI framework with decentralized trust. *Comput. Netw.*, 213, 109069.

[14] Akram, J., & Anaissi, A. (2024). Decentralized PKI framework for data integrity in spatial crowdsourcing drone services. *Proc. ICWS*, 643–653.

[15] Turan, E., Sen, S., & Ergun, T. (2024). A semi-decentralized PKI based on blockchain with a stake-based reward-punishment mechanism. *IEEE Access*, 12, 60705–60721.

[16] Koa, C. G., Heng, S. H., & Chin, J. J. (2025). New Ethereum-based distributed PKI with a reward-and-punishment mechanism. *Blockchain Res. Appl.*, 6(1), 100239.

[17] Sidorov, M. et al. (2019). Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains. *IEEE Access*, 7, 7273–7285.

[18] Jangirala, S., Das, A.K., & Vasilakos, A.V. (2020). Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing

Environment. *IEEE Trans. Ind. Inform.*, 16(11), 7081–7093.

[19] Safkhani, M., & Bagheri, N. (2019). Cryptanalysis of two recently proposed ultralightweight authentication protocol for IoT. *arXiv*, abs/1907.11322.

[20] D'Arco, P., & Ansaroudi, Z.E. (2020). Secret Disclosure Attacks on a Recent Ultralightweight Mutual RFID Authentication Protocol for Blockchain-Enabled Supply Chains. *Proc. SoCPaR*.

[21] Kumar, S., Banka, H., & Kaushik, B. (2023). Ultra-lightweight blockchain-enabled RFID authentication protocol for supply chain in the domain of 5G mobile edge computing. *Wirel. Netw.*, 29, 2105–2126.

[22] Liang, W. et al. (2021). A Mutual Security Authentication Method for RFID-PUF Circuit Based on Deep Learning. *ACM Trans. Internet Technol.*, 22(1), 1–20.

[23] Trinh, C. et al. (2020). A Novel Lightweight Block Cipher-Based Mutual Authentication Protocol for Constrained Environments. *IEEE Access*, 8, 165536–165550.

[24] Tariq, T. et al. (2025). A Blockchain-Assisted Authentication Protocol for RFID-Enabled Supply Chain Management System. *IEEE Trans. Netw. Sci. Eng.*, 12(4), 3108–3117.

[25] Islam, M.E. et al. (2023). User authentication and access control to blockchain-based forensic log data. *EURASIP J. Inf. Secur.*, 2023, 1.

[26] Wang, W. et al. (2022). Blockchain and PUF-Based Lightweight Authentication Protocol for Wireless Medical Sensor Networks. *IEEE Internet Things J.*, 9(11), 8883–8891.

[27] Yu, S., & Park, K. (2024). PUF-Based Robust and Anonymous Authentication and Key Establishment Scheme for V2G Networks. *IEEE Internet Things J.*, 11, 15450–15464.

[28] Kang, T., Woo, N., & Ryu, J. (2024). Enhanced Lightweight Medical Sensor Networks Authentication Scheme Based on Blockchain. *IEEE Access*, 12, 35612–35629.

[29] Hu, H. et al. (2025). Provably secure and lightweight authentication protocol using PUF and blockchain for smart grids. *J. Supercomput.*, 81, 949.

[30] Almadani, M.S. et al. (2023). Blockchain-Based Multi-Factor Authentication: A Systematic Literature Review. *Internet Things (Neth.)*, 23, 100844.

[31] Avoine, G., Carpent, X., & Hernandez-Castro, J. (2016). Pitfalls in Ultralightweight Authentication Protocol Designs. *IEEE Trans. Mobile Comput.*, 15(9), 2317–2332.

[32] Belfaik, Y. et al. (2024). A Comparative Study of Protocols' Security Verification Tools: Avispa, Scyther, ProVerif, and Tamarin. In *Int. Conf. Digit. Technol. Appl.* (pp. 118–128). Cham: Springer Nature Switzerland.

[33] Blanchet, B. (2014). Automatic Verification of Security Protocols in the Symbolic Model: The Verifier ProVerif. In Aldini, A., Lopez, J., & Martinelli, F. (Eds.), *Found. Secur. Anal. Des. VII, FOSAD 2012/2013 Lectures* (pp. 54–87). Cham: Springer.

[34] Cremers, C.J. (2008). The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols: Tool Paper. In *Int. Conf. Comput. Aided Verif.*, Springer, 414–418.

[35] Fatima, S. et al. (2024). On the Security of a Blockchain and PUF-Based Lightweight Authentication Protocol for Wireless Medical Sensor Networks. *Wireless Pers. Commun.*, 136(2), 1079–1106.

[36] Kannengieser, N. et al. (2022). Challenges and Common Solutions in Smart Contract Development. *IEEE Trans. Softw. Eng.*, 48(11), 4291–4318.

[37] Knežević, M., Tomović, S., & Mihaljević, M.J. (2025). Attack Scenarios and Security Analysis of a Blockchain and PUF-Based Lightweight Authentication Protocol for Wireless Medical Sensor Networks. *IEEE Internet Things J.*, 12(23), 2025, 51010-51025

[38] Lounis, K., & Zulkernine, M. (2023). Lessons Learned: Analysis of PUF-Based Authentication Protocols for IoT. *Digit. Threats: Res. Pract.*, 4(2), 1–33.

[39] Mihaljević, M.J., Knežević, M., Urošević, D., Wang, L., & Xu, S. (2023). An Approach for

Blockchain and Symmetric Keys Broadcast Encryption Based Access Control in IoT. *Symmetry*, 15(2), 299.

[40] Pham, H.A., Nguyen, C.T., & Lam, T.C. (2025). Blockchain Adoption for Authentication: A Survey. *Blockchain: Res. Appl.*, 100383.

[41] Qian, P. et al. (2023). Demystifying Random Number in Ethereum Smart Contracts: Taxonomy, Vulnerability Identification, and Attack Detection. *IEEE Trans. Softw. Eng.*, 49(7), 3793–3810.

[42] Shahidinejad, A., & Abawajy, J. (2024). An All-Inclusive Taxonomy and Critical Review of Blockchain-Assisted Authentication and Session Key Generation Protocols for IoT. *ACM Comput. Surv.*, 56(7), 1–38.

[43] Sharma, S., & Dwivedi, R. (2024). A Survey on Blockchain Deployment for Biometric Systems. *IET Blockchain*, 4(2), 124–151.

На основу пописа литературе који је наведен приликом пријаве теме докторске дисертације, комисија закључује да је кандидат детаљно проучио релевантну и актуелну научну грађу. Одабране библиографске јединице представљају адекватну основу за реализацију истраживања.

Избор литературе је одговарајући? ДА

III.4 циљева истраживања

Циљеви истраживања:

1. Анализа безбедности и ефикасности одабраних аутентификационих протокола, са посебним фокусом на енергетски и рачунарски економична (lightweight) решења намењена хетерогеним окружењима и уређајима са ограниченим ресурсима. Циљ је идентификација претходно недетектованих пропуста и потенцијалних вектора напада. Оваква анализа допринеће независној евалуацији постојећих протокола и омогућити увиде који ће послужити као основа за развој безбеднијих решења.
2. Формулисање смерница и предлога за унапређење аутентификационих решења заснованих на блокчејн приступима, са фокусом на повећање безбедности и ефикасности. Циљ је дефинисање принципа и приступа који омогућавају елиминацију уочених рањивости и боље искоришћење блокчејн својстава децентрализованости, транспарентности и непромењивости.
3. Софтверска евалуација и валидација предложених унапређења, кроз симулацију и моделовање у контролисаном окружењу ради процене изводљивости и безбедносних карактеристика. Циљ је обезбеђивање проверљивих резултата који ће омогућити независну евалуацију, репродуцибилност и потенцијалну интеграцију предложених решења у постојеће истраживачке и развојне оквире.

Комисија сматра да су наведени циљеви адекватно постављени и подобни за израду докторске дисертације.

Циљеви истраживања су одговарајући? ДА

III.5 очекиваних резултата (хипотезе)

Очекује се да анализа безбедности и ефикасности одабраних аутентификационих протокола резултира идентификацијом нових рањивости и потенцијалних вектора напада. На основу тих сазнања, истраживање ће омогућити формулисање смерница за унапређење аутентификационих решења заснованих на блокчејн приступима. Кроз софтверску евалуацију и симулацију у контролисаном окружењу, биће обезбеђени проверљиви и репродуцибилни резултати о изводљивости и безбедности предложених решења, што ће омогућити независну евалуацију и потенцијалну интеграцију у постојеће истраживачке и развојне оквире.

Комисија констатује да су наведени очекивани резултати добро дефинисани и да представљају значајан истраживачки допринос и основу за даља истраживања и примену у предметној области.

Очекивани резултати представљају значајан научни допринос? ДА

III.6 плана рада (на основу фаза истраживања и оријентационог садржаја дисертације из Обрасца 1)

Фазе истраживања:

- Дефинисање проблема и истраживачког оквира
- Систематизација доступних знања и приказ стања у области
- Анализа безбедности и ефикасности одабраних аутентификационих протокола у циљу идентификовања претходно недетектованих недостатака и потенцијалних вектора напада
- Формулисање смерница и предлога за унапређење постојећих решења са фокусом на отклањање уочених рањивости и повећање ефикасности
- Софтверска евалуација и валидација резултата
- Анализа резултата и извођење закључака

Оријентациони садржај докторске дисертације:

1. *Увод*
2. *Теоријске основе* – У овом поглављу уводе се кључни концепти и теоријске поставке релевантни за истраживање.
3. *Стање у области* – Ово поглавље даје преглед постојећих истраживања и решења у области аутентификационих протокола заснованих на блокчејн приступима, уз анализу трендова, ограничења и изазова.
4. *Анализа безбедности и ефикасности одабраних решења* – Ово поглавље садржи детаљну анализу безбедности и ефикасности одабраних аутентификационих протокола, уз идентификацију недостатака и вектора напада.
5. *Предлози за унапређења безбедности и ефикасности* – У овом поглављу дају се смернице, принципи и предлози за унапређење постојећих решења, са фокусом на елиминацију уочених рањивости и повећање ефикасности.
6. *Валидација резултата* – Ово поглавље обухвата софтверску евалуацију и валидацију предложених унапређења ради процене изводљивости и безбедносних карактеристика.
7. *Дискусија и закључци* – Ово поглавље сумира резултате истраживања и даје њихову критичку интерпретацију.
8. *Литература*

Комисија сматра да је план рада адекватно дефинисан и у складу са очекиваним резултатима истраживања.

План рада је одговарајући? ДА

III.7 метода и узорака истраживања

Истраживање ће обухватити теоријску анализу и софтверску евалуацију аутентификационих решења у складу са стандардима провере криптографских протокола. Анализа безбедности биће постављена у оквире успостављених формалних модела нападача којима се дефинишу способности нападача у погледу пресретања и манипулације комуникационим порукама. Анализирани протоколи биће моделовани у одговарајућим софтверским алатима, као што су ProVerif, Scyther, AVISPA и сл., како би се испитале њихове безбедносне карактеристике укључујући отпорност на нападе понављањем порука, нападе лажног представљања и Man-in-the-Middle (MiM) нападе.

За потребе оцене ефикасности аутентификационих протокола, истраживање ће укључити анализу трошкова израчунавања (број и тип криптографских операција), трошкова комуникације (величину и број порука), као и захтеване меморијске ресурсе. Посебно ће бити анализиран утицај корака и операција које се извршавају на блокчејну коришћењем адекватних показатеља перформанси. Евалуација ће бити спроведена у контролисаном окружењу и на адекватно одабраној блокчејн платформи.

Комисија сматра да методе одговарају потребама истраживања.

Метод и узорак су одговарајући? ДА

III.8 места, лабораторије и опреме за истраживачки рад

Рачунарски ресурси Математичког института САНУ

Услови за истраживачки рад су одговарајући? ДА

III.9 методе статистичке обраде података и осталих релевантних података

Није предвиђена статистичка обрада података.

Предложене методе су одговарајуће? ДА

IV ОЦЕНА ПОДОБНОСТИ КАНДИДАТА

Услови дефинисани за кандидата студијским програмом:

На основу Закона о високом образовању, као и у складу са Правилима докторских студија Универзитета у Новом Саду, која су усвојена на седници Сената Универзитета у Новом Саду одржаној 25.2.2021, и која су ступила на снагу 5.3.2021., а примењују се од 1.4.2021. године (Измене и допуне: 27.10.2022. године; 30.3.2023. године; 28.3.2024. године и 30.9.2025. године) и према Правилнику о упису, студирању на докторским академским студијама и стицању звања доктора наука, односно, доктора уметности Факултета техничких наука (број 01-195/11-1) од 7.10.2021. године, право да пријави тему докторске дисертације стиче студент докторских студија који је положио све испите одређене студијским програмом и који је одбранио Теоријске основе докторске дисертације.

Образложење: Кандидат Милица Кнежевић положила је све испите одређене студијским програмом Математика у техници и одбранила Теоријске основе докторске дисертације, чиме је стекла укупно 120 ЕСПБ. Преосталих 60 ЕСПБ стиче се спровођењем истраживања као и израдом и одбраном докторске дисертације. Кандидат је такође објавио два рада категорије М21а+, два рада категорије М21, један рад категорије М22 и један рад категорије М33, што показује да се кандидат на адекватан начин и у довољној мери ангажовао као истраживач. Комисија закључује да кандидат испуњава формалне услове и поседује научну и стручну компетентност за израду докторске дисертације.

Да ли кандидат испуњава дефинисане услове? ДА

V ОЦЕНА ПОДОБНОСТИ ПРЕДЛОЖЕНОГ МЕНТОРА

V.1 Биографија ментора (до 500 речи):

Др Миодраг Ј. Михаљевић је дописни члан Српске академије наука и уметности (од 2021. године), научни саветник и заменик директора Математичког института САНУ, као и руководилац Националног центра за сајбер безбедност и приватност. Ангажован је као наставник на докторским студијама студијског програма Математика у техници Факултета техничких наука у Новом Саду.

Дипломирао је 1979. године на Електротехничком факултету Универзитета у Београду, где је и магистрирао 1981. године, а докторску дисертацију одбранио је 1990. године на Војнотехничкој академији ЈНА у Загребу. Своју професионалну каријеру започео је 1979. године у Институту за примењену математику и електронику, где је радио до 1998. године. Од 1992. до 1998. године био је спољни сарадник Математичког института САНУ, а од 1998. године стално је запослен у овој институцији, где је 1999. године изабран за научног саветника, а од 2015. године обавља функцију заменика директора.

Аутор је преко 75 радова објављених у водећим међународним научним часописима као што су IEEE Transactions on Information Theory, IEEE Transactions on Communications, IEEE Communications Letters и други. Учествовао је на више од 50 међународних конференција, објавио преко 50 радова у националним публикацијама, као и више од 50 патената, софтвера и техничких извештаја. Његови радови су цитирани више од 3000 пута.

Био је руководилац бројних националних и међународних пројеката у областима криптологије, обраде слика и рачунарске топологије. Имао је гостујуће позиције у Јапану, укључујући Универзитет у Токију, SONY Computer Science Laboratories и AIST. За свој научни рад добио је више признања, укључујући Награду САНУ за десетогодишња остварења (2003–2012), а 2014. године изабран је за члана Academia Europaea. Укључен је у листу „2% најбољих светских научника“ Универзитета Стенфорд за 2020–2024.

Поред научног рада, др Михаљевић је активан као помоћни уредник и члан уредничких одбора више међународних часописа, и више пута је био члан Матичног одбора ресорног министарства у Србији.

V.2 Референце ментора из научне области којој припада тема докторске дисертације:

Р. бр.	аутори, наслов, *часопис*, **волумен** (година) број страница од-до, DOI или ISBN/ISSN	категорија
1.	Knežević, M., Tomović, S., & **Mihaljević, M. J.** Attack Scenarios and Security Analysis of a Blockchain and PUF-based Lightweight Authentication Protocol for Wireless Medical Sensor Networks. *IEEE Internet of Things Journal*, **12**(23), 2025, 51010-51025 doi:10.1109/JIOT.2025.3612005	M21a+
2.	**Mihaljević, M. J.**, Radonjić, A., Mijajlović, N., Wang, L., & Xu, S. An Integer Erasure Correction Coding and Its Application for Security Enhancement of Encryption. *IEEE Access,* **13**, 2025, 104728-104741. doi:10.1109/ACCESS.2025.3579919	M21
3.	Xu, S., He, H., **Mihaljević, M. J**., Zhang, S., Shao, W., & Wang, Q. DBC-MulBiLSTM: A DistilBERT-CNN feature fusion framework enhanced by multi-head self-attention and BiLSTM for smart contract vulnerability detection. *Computers & Electrical Engineering,* **123**, 2025, 110096. doi:10.1016/j.compeleceng.2025.110096	M21
4.	Xu, S., Dong, S., Wang, L., **Mihaljević, M. J.,** Zhang, S., Shao, W., & Wang, Q. Blockchain-based secure data sharing with overlapping clustering and searchable encryption. *Computer Standards & Interfaces,* **93**, 2025, 103979. doi:10.1016/j.csi.2025.103979	M21a
5.	Wang, Q., Wang, L., Xu, S., Zhang, S., Shao, W., & **Mihaljević, M. J.** Single-layer trainable neural network for secure inference. *IEEE Internet of*	M21a+

	Things Journal, **12**(3), 2025, 2968–2978. doi:10.1109/JIOT.2024.3480195	
6.	Xu, S., Zhang, L., Wang, L., **Mihaljević, M. J**., Zhang, S., Shao, W., & Wang, Q. Relay network-based cross-chain data interaction protocol with integrity audit. *Computers and Electrical Engineering,* **117**, 2024, 109262. doi:10.1016/j.compeleceng.2024.109262	M21
7.	Xu, S., Wang, F., Wang, L., **Mihaljević, M. J.,** Zhang, S., Shao, W., & Huang, Q. A sharding scheme based on graph partitioning algorithm for public blockchain. *Computer Modeling in Engineering & Sciences,* **139**(3), 2024, 3311–3327. doi:10.32604/cmes.2023.046164	M21
8.	**Mihaljević, M. J**., Todorović, M., & Knežević, M. An evaluation of power consumption gain and security of flexible green pool mining in public blockchain systems. *Symmetry,* **15**(4), 2023, 924. doi:10.3390/sym15040924	M21
9.	Zhang, S., Hu, C., Wang, L., **Mihaljević, M. J**., Xu, S., & Lan, T. A malware detection approach based on deep learning and memory forensics. *Symmetry,* **15**(3), 2023, 758. doi:10.3390/sym15030758	M21
10.	**Mihaljević, M. J.,** Knežević, M., Urošević, D., Wang, L., & Xu, S. An approach for blockchain and symmetric keys broadcast encryption based access control in IoT. *Symmetry,* **15**(2), 2023, 299. doi:10.3390/sym15020299	M21
11.	**Mihaljević, M. J**., Wang, L., Xu, S., & Todorović, M. An approach for blockchain pool mining employing the consensus protocol robust against block withholding and selfish mining attacks. *Symmetry,* **14**(8), 2022, 1711. doi:10.3390/sym14081711	M21
12.	**Mihaljević, M. J**., Wang, L., & Xu, S. An approach for security enhancement of certain encryption schemes employing error correction coding and simulated synchronization errors. *Entropy,* **24**(3), 2022, 406. doi:10.3390/e24030406	M22
13.	**Mihaljević, M. J.,** Radonjić, A., Wang, L., & Xu, S. Security enhanced symmetric key encryption employing an integer code for the erasure channel. *Symmetry,* **14**(8), 2022, 1709. doi:10.3390/sym14081709	M21
14.	Tomović, S., Knežević, M., & **Mihaljević, M. J.** Analysis and correction of the attack against the LPN-problem based authentication protocols. *Mathematics,* **9**(5), 2021, 573. doi:10.3390/math9050573	M21a+
15	**Mihaljević, M. J**. A blockchain consensus protocol based on dedicated time-memory-data trade-off. *IEEE Access,* **8**, 2020, 141258–141268. doi:10.1109/ACCESS.2020.3013199	M21a
16.	Knežević, M., Tomović, S., & **Mihaljević, M. J**. Man-in-the-middle attack against certain authentication protocols revisited: Insights into the approach and performances re-evaluation. *Electronics,* **9**(8), 2020, 1296. doi:10.3390/electronics9081296	M22
17.	**Mihaljević, M. J**. A security enhanced encryption scheme and evaluation of its cryptographic security. *Entropy,* **21**(7), 2019, 701. doi:10.3390/e21070701	M21
18.	**Mihaljević, M. J.,** & Oggier, F. (2019). Security evaluation and design elements for a class of randomized encryptions. *IET Information Security, 13*(1), 36–47. doi:10.1049/iet-ifs.2017.0271	M22
19.	**Mihaljević, M. J**., Kavčić, A., & Matsuura, K. An encryption technique for provably secure transmission from a high performance computing entity to a tiny one. *Mathematical Problems in Engineering,* **2016**, 2016, Article ID 7920495. doi:10.1155/2016/7920495	M22

20.	Tomović, S., **Mihaljević, M. J.,** Perović, A., & Ognjanović, Z. A protocol for provably secure authentication of a tiny entity to a high performance computing one. *Mathematical Problems in Engineering,* **2016**, 2016, Article ID 9289050. doi:10.1155/2016/9289050	M22

V.3 Услови дефинисани за ментора у складу са *Правилима докторских студија Универзитета у Новом Саду* за област којој припада докторска дисерација:

На основу Закона о високом образовању, као и у складу са Правилима докторских студија Универзитета у Новом Саду, која су усвојена на седници Сената Универзитета у Новом Саду одржаној 25.2.2021, и која су ступила на снагу 5.3.2021., а примењују се од 1.4.2021. године (Измене и допуне: 27.10.2022. године; 30.3.2023. године; 28.3.2024. године и 30.9.2025. године) и према Правилнику о упису, студирању на докторским академским студијама и стицању звања доктора наука, односно, доктора уметности Факултета техничких наука (број 01-195/11-1) од 7.10.2021. године, ментор је по правилу наставник датог студијског програма, који поред услова, који су дефинисани стандардима за акредитацију, има најмање пет радова који су публиковани у часописима са импакт фактором са SCI листе, односно SCIe листе у претходних 10 година.

Образложење:

Комисија закључује да **др Миодраг Ј. Михаљевић** испуњава услове дефинисане за ментора у складу са Правилима докторских студија Универзитета у Новом Саду и оцењује се као **ПОДОБАН** за ментора на изради докторске дисертације кандидата.

Да ли ментор испуњава услове? ДА

VI ЗАКЉУЧАК

Тема је подобна	**ДА**
Кандидат је подобан	**ДА**
Ментор је подобан	**ДА**

Образложење о подобности теме, кандидата и ментора (до 500 речи):

Након детаљне анализе достављене пријаве, увида у до сада објављене радове кандидата и ментора, формулације теме, предмета и циља истраживања, показаног познавања области и очекиваних резултата комисија закључује:

- Предложена тема је подобна за израду докторске дисертације. Тема је актуелна, научно оправдана и добро дефинисана.
- Кандидат Милица Кнежевић испуњава неопходне услове и подобна је за израду предложене докторске дисертације.
- др Миодраг Ј. Михаљевић, научни саветник у Математичком институту САНУ и дописни члан САНУ, подобан је за ментора предложене докторске дисертације.

На основу изнетих закључака, Комисија предлаже Наставно-научном већу Факултета техничких наука у Новом Саду и органима Универзитета у Новом Саду да прихвате тему за израду докторске дисертације под насловом „Дизајн и безбедносне карактеристике аутентификационих протокола заснованих на блокчејн приступима“ кандидата Милице Кнежевић и да се за ментора именује др Миодраг Ј. Михаљевић.

Место и датум: Нови Сад, Београд 4.2.2026.

1. др Силвиа Гилезан, редовни професор
_____, председник

2. др Зоран Огњановић, научни саветник
_____, члан

3. др Душан Гајић, ванредни професор
_____, члан

4. др Весна Маринковић, ванредни професор
_____, члан

5. др Иван Прокић, доцент
_____, члан

НАПОМЕНА: *Члан комисије који не жели да потпише извештај јер се не слаже са мишљењем већине чланова комисије, дужан је да унесе у извештај образложење односно разлоге због којих не жели да потпише извештај и да исти потпише.*