4-55/122
16.03.2022.

UNIVERZITET SINGIDUNUM
Departman za poslediplomske studije
Danijelova 32, Beograd

VEĆU DEPARTMANA ZA POSLEDIPLOMSKE STUDIJE

Odlukom Veća Departmana za poslediplomske studije broj _4 - 18/2022_ od 28.01.2022. godine, određeni smo za članove Komisije za ocenu i odbranu doktorske disertacije kandidata Nikole Pavlovića pod nazivom „Povećanje bezbednosti i privatnosti integrisanjem blokčejn interfejsa u arhitekturu interneta stvari"

o čemu podnosimo sledeći

IZVEŠTAJ

1. Osnovni podaci o kandidatu i doktorskoj disertaciji

Kandidat Nikola Pavlović rođen je 29.12.1994. god. u Beogradu, gde je završio osnovnu i srednju školu. Zemunsku gimnaziju je završio 2014. god. na prirodno-matematičkom smeru. Osnovne akademske studije završio je 2018. god. na Fakultetu za informatiku i računarstvo, Univerziteta Singidunum. Master akademske studije upisuje iste godine i završava 2019. god. na studijskom programu: "Savremene informacione tehnologije" na Univerzitetu Singidunum sa prosečnom ocenom 10.

Od 2018. god kandidat je zaposlen u kompaniji StuntCoders doo kao Medior Software developer na razvoju ecommerce rešenja, poboljšavanju bezbednosti sistema, održavanju servera i razvoju dodataka za Wordpress i Magento platformu.

Doktorske akademske studije na studijskom programu Napredni sistemi zaštite na Univerzitetu Singidunum, upisao je školske 2019/2020 godine.

Kandidat ima sledeće objavljene radove kategorije M21 čime je ispunjen preduslov za odbranu doktorske disertacije:

[1.] **Pavlović, N.**, *Šarac, M., Adamović, S. et al. An approach to adding simple interface as security gateway architecture for IoT device. Multimed Tools Appl (2021). https://doi.org/10.1007/s11042-021-11389-8*

[2.] Šarac, M., **Pavlović, N.**, Bacanin, N., Al-Turjman, F., & Adamović, S. (2021). Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device

Security Gateway Architecture. Energy Reports. https://doi.org/10.1016/j.egyr.2021.07.078

Preostali objavljeni radovi:

Spisak rezultata M33

[1.] **Pavlović, N.,** *Šarac, M. Blockchain implementation for IoT devices, Blockchain of Things. In: Zdravković, M., Trajanović, M., Konjović, Z. (Eds.) ICIST 2021 Proceedings, pp.149-153, 2021*

[2.] **Pavlović. N.,** *M. Šarac, S. Adamović, M. Mravik, "Enchantment of Magento CMS Security," in Sinteza 2019 - International Scientific Conference on Information Technology and Data Related Research, Belgrade, Singidunum University, Serbia, 2019, pp. 223-228. doi:10.15308/Sinteza-2019-223-228*

[3.] **Pavlović N.,** *S. Adamović, "Development of a Cryptographic Solution Based on Kerberos for Database Security," in Sinteza 2018 - International Scientific Conference on Information Technology and Data Related Research, Belgrade, Singidunum University, Serbia, 2018, pp. 3-8. doi:10.15308/Sinteza-2018-3-8*

Doktorska disertacija kandidata Nikole Pavlovića je urađena na ukupno 137 strana, od čega 14 strana čine prilog i spisak literature. Spisak literature obuhvata 130 referenci koje čine naučni radovi, knjige, zbornici radova, zakonski propisi kao i elektronski izvori. Uz osnovni tekst disertacija sadrži i 28 slika i 5 tabela.

Doktorska disertacija kandidata Nikole Pavlovića je bila podvrgnuta proveri softverom za ustanovljavanje preklapanja/plagijarizma (iThenticate Plagiarism Detection Software). *Ukupan procentualni iznos zapaženih preklapanja iznosi 7% disertacije.*

2. Predmet i cilj istraživanja

Predmet istraživanja je analiza kriptografskih bezbednosnih svojstava uređaja interneta stvari pri mrežnoj komunikaciji preko interneta. Analiza blokčejn tehnologije i mogućnost sinteze blokčejn tehnologije sa arhitekturom interneta stvari i omogućavanjem stvaranja bezbedne mreže i korišćenje blokčejn tehnologije za unapređenje bezbednosti i privatnosti podataka sa kojima rade uređaji interneta stvari.

Cilj istraživanja je sinteza blokčejn tehnologije i naprednih kriptografskih algoritama sa uređajima i protokolima interneta stvari i omogućavanje da se primene tehnike validacije blokčejn tehnologije kao i unapredi bezbednost i privatnost podataka primenom naprednih kriptografskih algoritama.

3. Hipotetički okvir istraživanja

Opšta hipoteza od koje se krenulo u istraživanje u disertaciji je: „Blokčejn i distribuirana infrastruktura omogućavaju da u komunikaciji između pametnih uređaja ili udaljenih servisa bude primenjen moderni kriptografski algoritam i da se omogući laka distribucija kriptoloških ključeva"

Posebna hipoteza koja proizilazi iz opšte je: „Kombinovanjem više kriptografskih algoritama zajedno sa sistemima validacije i autentifikacije koji se koriste u blokčejn infrastrukturi moguće je poboljšati bezbednost komunikacije između pametnih uređaja i servisa bez znatnog uticaja na performanse sistema"

Pojedinačne hipoteze koje su korišćene u disertaciji su:

- Postojeće metode napada na pametne uređaje je moguće sprečiti ili bar smanjiti mogućnosti njihovog izvođenja i efekte samih napada.
- Procena nivoa sigurnosti koji treba postići.
- Broj uređaja koji će koristiti sistem.
- Kompromis između troškova razvoja i performansi sistema.
- Razmena ključeva i primena naprednih kriptografskih algoritama zavisi od udaljenih servisa i podrške proizvođača pametnog uređaja.
- Limitacija u količini memorije pri čuvanju podataka u blokčejn bazu podataka kao i primena kompresije.
- Komunikacija između pametnih uređaja se validira i upisuje u blokčejn bazu kao transakcije i time se ima čitav uvid u samu aktivnost infrastrukture.

4. Metodologija istraživanja

Metodologija istraživanja u ovom radu obuhvata složen i organizovan postupak zasnovan na logičkim načelima i strogim principima tipičnim za analizu i sintezu kriptografskih mehanizama dokazive bezbednosti. Složenost predmeta istraživanja zahteva primenu:

- Analiza osnovnih metoda
- Sintetičnih osnovnih metoda
- Opštih naučnih metoda

Ovaj izbor istraživačkih metoda je upotrebljen da se istraživanje i tok istraživačkog procesa u svim fazama, odnosno identifikaciju i definisanje problema, planiranje dizajna istraživanja, kritičkoj analizi sistema kao i formiranje zaključka u skladu sa osnovnim principima naučno istraživačkog rada.

5. Kratak prikaz sadržaja doktorske disertacije

Rad se sastoji iz 6 poglavlja, sadržajno struktuiranih na sledeći način:

U prvom poglavlju, uvodnom razmatranju, ukratko je izložena motivacija za ovu disertaciju, problem koji se razmatra i pristup njegovom rešavanju.

U drugom poglavlju uređen je pregled u oblasti istraživanja, prikazani nedostaci u bezbednosti uređaja interneta stvari, nedostaci blokčejn tehnologije kao i uređen pregled unapređenja bezbednosti i privatnosti sintezom prethodno dve pomenute tehnologije.

U trećem poglavlju prikazane su teorijske osnove istraživanja, urađen je pregled sistema za otkrivanje i sprečavanje napada, analizirana blokčejn tehnologija, način pravljena blokova i provera validnosti i tačnosti podataka, pregled interneta stvari i arhitekture koju koriste kao i protokola i potom urađen pregled modernih kriptografskih algoritama koji bi mogli da se integrišu u mrežne protokole interneta stvari.

U četvrtom poglavlju dat je predlog rešenja od generičke šeme do razvoja predloženog rešenja. Ovde se predlaže kako bi izgledalo predloženo rešenje, zatim razvija i analizira kako novo predloženo rešenje obezbeđuje i unapređuje bezbednost i privatnost podataka sa kojima rade uređaji interneta stvari.

U petom poglavlju se daje rezime istraživanja, pregled glavnih doprinosa disertacije kao i mogući pravci daljeg istraživanja u ovoj oblasti.

U šestom poglavlju je prikazan programski kod predloženog rešenja kao i komentari za dalje razumevanje pomenutog.

6. Postignuti rezultati i naučni doprinos doktorske disertacije

Potvrđeni doprinosi ovog rada su sledeći:

- Izvršen je pregled u oblasti, uočeni nedostaci u komunikaciji između uređaja interneta stvari i njihovoj interakciji sa servisima u oblaku.
- Izvršen je pregled postojećih programskih jezika, njihovih limitacija i urađena analiza koji bi bio najbolji za predloženo rešenje.
- Predložen je nov pristup za bazu podataka koja bi mogla da opsluži veliki broj uređaja bez uticaja na performanse predloženog rešenja.
- Predložen je sistem za prevenciju napada kao i sistem za detekciju napada koji bi se nalazio ispred blokčejn interfejsa kao dodatni nivo zaštite.
- Izvršen je pregled modernih kriptografskih rešenja i analiziran njihov uticaj na performanse sistema kao i stepen bezbednosti koji doprinosi predloženom rešenju.
- Dizajnirana je nova generička šema za integraciju blokčejn interfejsa sa dodatnim bezbednosnim mehanizmima.
- Analiziran je doprinos rada u sprečavanju modernih napada na uređaje interneta stvari, njihovo prevenciji kao i unapređenju privatnosti koji je od velikog značaja posebno u okruženjima gde se radi sa informacijama od velikog značaja.

- Predloženo rešenje daje mogućnost administracije većeg broja blokčejn mreža sa jednog programskog / hardverskog rešenja kao i opsluživanje velikog broja uređaja. Dodavanje i uklanjanje uređaja interneta stvari bez uticaja na druge članove mreže kao i mogućnost podešavanja bezbednosnih mehanizama svakog uređaja posebno.
- Jedinstveni doprinos ovog rada je integracija blokčejn tehnologija, validacije kao i mrežne strukture koje dolazi sa njom u internet stvari. Ovim pristupom povećana je inicijalno predložena privatnost, kao i bezbednost podataka dodavanjem dodatnih kriptografskih algoritama.

7. Mišljenje i predlog Komisije o doktorskoj disertaciji

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

Sagledavajući ukupnu ocenu doktorske disertacije kandidata Nikole Pavlovića_pod nazivom „Povećanje bezbednosti i privatnosti integrisanjem sigurnog blokčejn interfejsa u arhitekturu interneta stvari“ predlažemo Veću departmana za poslediplomske studije i Senatu Univerziteta Singidunum da prihvati napred navedenu doktorsku disertaciju i odobri njenu javnu odbranu.

Beograd, 15/03/2022.

Članovi komisije:

prof. dr Marko Šarac

prof. dr Saša Adamović

prof. dr Petar Spalević