LXIX Konferencija ETRAN, Čačak, 9 - 12. Jun 2025.

Uporedna analiza performansi sigurnih virtuelnih mašina Google Cloud i lokalne infrastrukture

Teodora Radaljac
Katedra za računarsku tehniku i informatiku
Elektrotehnički fakultet, Univerzitet u Beogradu
Beograd, Srbija
teodora@etf.bg.ac.rs

Pavle Vuletić
Katedra za računarsku tehniku i informatiku
Elektrotehnički fakultet, Univerzitet u Beogradu
Beograd, Srbija
pavle.vuletic@etf.bg.ac.rs
ORCID: 0000-0001-5600-2652

Danko Miladinović
Katedra za računarsku tehniku i informatiku
Elektrotehnički fakultet, Univerzitet u Beogradu
Beograd, Srbija
danko@etf.bg.ac.rs

Žarko Stanisavljević
Katedra za računarsku tehniku i informatiku
Elektrotehnički fakultet, Univerzitet u Beogradu
Beograd, Srbija
zarko@etf.bg.ac.rs
ORCID: 0000-0003-0272-5139

***Apstrakt* — Ovaj rad se bavi uporednom analizom performansi sigurnih virtuelnih mašina (eng. *Confidential Virtual Machines* – CVM) u dva različita okruženja – lokalnoj infrastrukturi zasnovanoj na AMD SEV-SNP tehnologiji i javnoj cloud infrastrukturi Google Cloud-a. Poverljivo računanje predstavlja ključni mehanizam zaštite koji omogućava enkripciju memorije virtuelnih mašina i izolaciju podataka čak i od privilegovanog softvera. Rad se fokusira na dva glavna aspekta: vreme potrebno za atestaciju virtuelnih mašina i performanse izvršavanja distribuiranih zadataka putem Ray okvira. Eksperimentalna merenja pokazuju da lokalna SEV-SNP infrastruktura omogućava znatno bržu atestaciju i bolje performanse zadataka u poređenju sa cloud instancama koje koriste virtuelni *Trusted Platform Module* (vTPM) mehanizam. Iako cloud rešenja nude veću fleksibilnost i jednostavno skaliranje, lokalno okruženje obezbeđuje stabilnije performanse, niže kašnjenje i veću kontrolu nad sigurnosnim procesima.**

Ključne reči—AMD SEV-SNP, Google Cloud, atestacija, virtuelne mašine, distribuirano procesiranje, Ray okvir

I. Uvod

Sa intenzivnim razvojem računarstva dolazi do značajnih promena u načinu obrade podataka. Umesto tradicionalne lokalne obrade, sve više se primenjuju virtuelne mašine koje čine temelj savremenog računarstva u oblaku. Virtuelne mašine omogućavaju efikasnu raspodelu i izolaciju resursa na zajedničkoj fizičkoj infrastrukturi, što pruža korisnicima veću fleksibilnost i skalabilnost. Međutim, sa sve većom popularnošću usluga sistema u oblaku, naročito u sistemima sa velikim brojem korisnika, pojavljuje se potreba za dodatnim slojevima sigurnosti koji prevazilaze tradicionalne pristupe. Jedan od najvažnijih mehanizama za zaštitu podataka i integriteta izvršavanja jesu takozvane sigurne enklave (eng. *Trusted Execution Environment*s – TEE) [1]. One omogućavaju izvršavanje programskog koda u izolovanom, hardverski zaštićenom prostoru, štiteći aplikacije i podatke od neovlašćenog pristupa, uključujući i pokušaje pristupa od strane privilegovanog sistemskog softvera poput operativnih sistema ili hipervizora. Korisnicima modernih računarskih sistema ključno je da obradu svojih podataka izvršavaju brzo, efikasno i sigurno. Performanse takvih sigurnih sistema zavise, između ostalog, od dva ključna faktora: procesa atestacije i efikasnosti distribuiranog procesiranja. Atestacija je postupak kojim se proverava i potvrđuje integritet i sigurnosno stanje virtuelne mašine, obično pre nego što joj se omogući pristup poverljivim podacima. Time se obezbeđuje da se VM nalazi u verifikovanom okruženju, smanjujući rizik od kompromitovanja podataka tokom njenog rada. Distribuirano procesiranje omogućava paralelnu obradu velikih količina podataka, raspoređivanjem zadataka na više računarskih čvorova istovremeno. Zbog svoje efikasnosti i jednostavnosti primene u distribuiranim okruženjima, kao okvir za realizaciju ovakvog pristupa odabran je Ray [2]. U ovom radu analiziramo i poredimo performanse dva različita okruženja: gde su virtuelne mašine zasnovane na javnoj infrastrukturi Google Cloud [3], i lokalnih virtuelnih mašina baziranih na AMD SEV-SNP tehnologiji [4]. Glavni cilj istraživanja je poređenje performansi ova dva pristupa kroz jasno definisana eksperimentalna merenja: prvo, kroz merenje vremena potrebnog za proces atestacije, koji prethodi izvršavanju u distribuiranom okruženju, i zatim, kroz merenje performansi konkretnih zadataka distribuiranih pomoću Ray okvira. Dobijeni rezultati pružiće jasniju sliku o tome kako različite arhitekture i implementacije sigurnosnih mehanizama utiču na efikasnost obrade podataka.

Do sada ova vrsta istraživanja nije odrađena. Vršena su upoređivanja sigurnosnih aspekata različitih cloud provajdera [5] (Azure, Google Cloud), ali ne i upoređivanje vremena potrebnog za dohvatanje atestacije.

U drugom poglavlju predstavljeni su koncept sigurnih virtuelnih mašina i njihova primena u savremenim sistemima. Treće poglavlje obrađuje tehničke detalje procesa atestacije u lokalnim SEV-SNP i Google Cloud vTPM okruženjima. U četvrtom poglavlju izložena je eksperimentalna postavka i metodologija merenja, dok peto poglavlje donosi rezultate poređenja performansi. Na kraju, u šestom poglavlju sledi diskusija i zaključak o prednostima i ograničenjima analiziranih rešenja.

ISBN 978-86-6200-032-3 ©2025 AM & ETRAN

https://doi.org/10.69994/69E25047

II. SIGURNE VIRTUELNE MAŠINE

Virtuelne mašine (eng. *Virtual Machines* - VM) predstavljaju softverski kreirana okruženja koja emuliraju funkcionalnosti fizičkih računara, omogućavajući pokretanje više operativnih sistema na zajedničkom hardveru. Za razliku od tradicionalnih pristupa gde je jedan računar rezervisan za jedan operativni sistem, korišćenjem virtuelizacije moguće je paralelno izvršavati više izolovanih sistema. Ovo omogućava efikasniju upotrebu raspoloživih resursa, kao što su procesorska snaga, memorija i prostor za skladištenje podataka. Centralnu ulogu u kreiranju i upravljanju VM instancama ima softver poznat kao hipervizor (eng. *hypervisor*). U zavisnosti od dostupne infrastrukture, virtuelne mašine mogu biti realizovane u okviru servisa u oblaku ili lokalnih serverskih sistema. Računarstvo u oblaku (eng. *Cloud Computing*) predstavlja model u kojem korisnici putem interneta pristupaju računarskim resursima (procesorskoj snazi, memoriji, prostoru za skladištenje). Umesto održavanja sopstvenog hardvera, usluge servisa u oblaku nude jednostavno skaliranje i upravljanje resursima prema potrebi. Provajderi servisa u oblaku poput Google Cloud-a omogućavaju korisnicima brzo kreiranje VM instanci različitih konfiguracija (vCPU, RAM, prostor) u zavisnosti od specifičnih zahteva. Lokalne virtuelne mašine, nasuprot tome, izvršavaju se na namenski pripremljenoj fizičkoj infrastrukturi kojom korisnik direktno upravlja. Ovakav pristup nudi viši stepen kontrole i stabilnije performanse, što je posebno značajno u scenarijima koji zahtevaju visoku sigurnost i privatnost. U okviru ovog rada, lokalna infrastruktura bazira se na serverima opremljenim AMD SEV-SNP procesorima u Laboratoriji za informacionu bezbednost ETF-a.

III. ATESTACIJA U CVM

Sigurne virtuelne mašine predstavljaju posebnu vrstu VM-ova koji pružaju visok nivo zaštite i izolacije aplikacija i njihovih podataka tokom izvršavanja. Glavni cilj upotrebe CVM-ova jeste sprečavanje neovlašćenog pristupa osetljivim informacijama od strane privilegovanog softvera poput hipervizora ili host operativnog sistema.

Ključni korak u obezbeđivanju ovog nivoa zaštite jeste proces atestacije – postupak provere sigurnosti i integriteta VM-a pre nego što mu se dozvoli pristup poverljivim podacima. U nastavku će biti detaljno objašnjeni mehanizmi atestacije u dva različita okruženja: lokalnom sistemu zasnovanom na AMD SEV-SNP tehnologiji i infrastrukturi Google Cloud-a korišćenjem *OpenID Connect* (OIDC) [6] vTPM pristupa.

A. Atestacija AMD SEV-SNP virtuelnih mašina

AMD SEV-SNP (eng. *Secure Encrypted Virtualization – Secure Nested Paging*) [7] predstavlja naprednu sigurnosnu tehnologiju kompanije AMD koja omogućava sigurno izvršavanje virtuelnih mašina kroz hardverski podržanu enkripciju memorije i proveru integriteta pojedinačnih stranica memorije. Glavna svrha SEV-SNP tehnologije jeste pružanje visokog nivoa izolacije podataka, pri čemu virtuelna mašina ima ekskluzivno pravo pristupa sopstvenoj memoriji, potpuno štiteći podatke od pristupa hipervizora ili drugih softverskih slojeva. Kako bi se korisnicima i eksternim servisima omogućila provera integriteta VM-a pre nego što joj se poveri obrada poverljivih podataka, koristi se proces atestacije. Ovaj proces obuhvata generisanje, validaciju i potvrdu sigurnosnog stanja virtuelne mašine kroz niz kriptografski potpisanih izveštaja. Proces atestacije započinje odmah prilikom inicijalnog pokretanja virtuelne mašine. U momentu pokretanja, specijalizovani sigurnosni modul integrisan u AMD procesore, poznat kao AMD Secure Processor (ASP), automatski kreira skup jedinstvenih kriptografskih ključeva za svaku VM instancu posebno. Ti ključevi se generišu pomoću integrisanog, hardverski podržanog generatora slučajnih brojeva, što obezbeđuje njihovu jedinstvenost i otpornost na predviđanje. Nakon kreiranja, ključevi se čuvaju u specijalno izolovanom, hardverski zaštićenom prostoru unutar AMD Secure procesora. Ova oblast memorije je potpuno nedostupna drugim komponentama sistema, uključujući hipervizor i host operativni sistem, što sprečava bilo kakav pokušaj kompromitovanja ili zloupotrebe.

Ovako formirani kriptografski identitet služi kao temeljni sigurnosni element za sve buduće operacije povezane sa atestacijom. Nakon što je jedinstveni identitet virtuelne mašine formiran, sledeći korak je generisanje atestacionog izveštaja. Atestacioni izveštaj predstavlja detaljan kriptografski zaštićen dokument koji omogućava VM instanci da eksternim stranama potvrdi svoj integritet, legitimnost, sigurnosnu konfiguraciju i stanje. Proces generisanja atestacionog izveštaja odvija se kroz nekoliko koraka:

- Zahtev za generisanjem izveštaja: Virtuelna mašina šalje eksplicitan zahtev AMD SEV firmware-u unutar AMD Secure procesora da pripremi atestacioni izveštaj.
- Prikupljanje relevantnih informacija: Firmware potom prikuplja sve relevantne podatke koji opisuju trenutno stanje VM instance. Ovi podaci uključuju vrednosti heša bootloader-a (eng. *digest*), operativnog sistema i firmware-a (eng. *Measurement*), sigurnosne politike (eng. *Policy flags*), identifikatore procesora (eng. *Chip ID*), informacije o verziji platforme (eng. *Platform Info*), kao i dodatne korisnički definisane informacije (eng. *Report Data*).
- Digitalno potpisivanje izveštaja: Nakon prikupljanja svih informacija, AMD Secure Processor koristi privatni ključ AMD-ovog hardverskog modula kako bi generisao digitalni potpis. Ovaj potpis sprečava bilo kakvu naknadnu modifikaciju podataka u izveštaju, čime se garantuje integritet i autentičnost podataka.
- Dostavljanje izveštaja VM-u: Kompletan, potpisan atestacioni izveštaj prosleđuje se nazad virtuelnoj mašini, koja ga potom može proslediti za dalju proveru.

Poslednja faza procesa atestacije predstavlja validaciju atestacionog izveštaja koji je primljen od VM instance. Najpre se vrši provera digitalnog potpisa izveštaja korišćenjem javnog ključa AMD Root-of-Trust modula. Ovim korakom proverava se autentičnost izveštaja i osigurava da izveštaj potiče od legitimnog AMD Secure Processor-a, što sprečava bilo kakve pokušaje falsifikovanja ili zloupotrebe. Zatim se analiziraju vrednosti heša ključnih komponenti sistema, poređenjem sa očekivanim vrednostima. Na taj način potvrđuje se da su kernel, firmware i bootloader VM instance pokrenuti u originalnom, bezbednom stanju bez kompromitacija ili neželjenih modifikacija. Takođe se analiziraju sigurnosne politike VM-a, osiguravajući da su sve bezbednosne opcije u skladu sa zahtevima. Na kraju, proverava se jedinstvenost same platforme

kroz vrednosti identifikatora čipa i informacije o platformi. Po uspešnom završetku svih navedenih koraka zagarantovano je potpuno poverenje da se virtuelna mašina nalazi u očekivanom sigurnom stanju, spremna za bezbednu obradu poverljivih i kritičnih podataka.

B. *OIDC vTPM atestacija u Google Cloud-u*

Atestacija virtuelnih mašina u Google Cloud-u temelji se na drugačijem pristupu u poređenju sa lokalnom AMD SEV-SNP tehnologijom. U cloud okruženjima korisnici nemaju direktan pristup fizičkom sigurnosnom modulu kao što je AMD Secure Processor (ASP), pa se umesto toga koristi softverska verzija Trusted Platform Module (TPM), nazvana vTPM. Google Cloud, kroz implementaciju Confidential Computing platforme, primenjuje vTPM u kombinaciji sa OIDC protokolom kako bi obezbedio sigurnu i pouzdanu atestaciju svojih VM instanci. Trusted Platform Module (TPM) je specijalizovani hardverski modul koji se tradicionalno koristi za proveru integriteta platforme, bezbedno skladištenje kriptografskih ključeva i generisanje kriptografskih dokaza integriteta sistema. Međutim, u sistemima u oblaku poput Google Cloud-a, korisnici nemaju pristup fizičkim sigurnosnim modulima servera. Iz tog razloga Google koristi virtuelni TPM (vTPM), koji predstavlja softversku emulaciju TPM funkcionalnosti, omogućavajući iste sigurnosne mehanizme unutar virtuelnih mašina. Atestacija virtuelnih mašina u Google Cloud-u odvija se u nekoliko koraka:

- Pokretanje virtuelne mašine i inicijalno merenje integriteta: Prilikom pokretanja Google Cloud Confidential VM instance, vTPM modul virtuelne mašine automatski vrši inicijalna kriptografska merenja ključnih komponenti operativnog sistema, kao što su kernel, firmware i bootloader. Rezultati ovih merenja smeštaju se u posebne memorijske registre, poznate kao Platform Configuration Registers (PCR). PCR registri sadrže heš vrednosti koje identifikuju stanje i integritet ključnih softverskih komponenti VM instance prilikom njenog pokretanja.
- Generisanje TPM atestacionog dokaza od strane VM instance: U trenutku kada virtuelna mašina želi da dokaže svoju ispravnu konfiguraciju i sigurnosno stanje eksternim stranama ili servisu, VM generiše TPM atestacioni dokaz pomoću alata poput gotpm [8]. Atestacioni dokaz sadrži PCR heš vrednosti koje predstavljaju stanje integriteta virtuelne mašine i kriptografski se potpisuje korišćenjem privatnog ključa vTPM-a.
- Slanje TPM atestacionog dokaza Google Cloud Attestation servisu: Nakon generisanja TPM atestacionog dokaza, VM instanca šalje ovaj dokaz Google Cloud Attestation servisu.
- Validacija atestacionog dokaza od strane Google Cloud Attestation servisa: Servis proverava da li je primljeni atestacioni dokaz potpisan legitimnim vTPM modulom. Nakon toga, proverava da li heš vrednosti ključnih komponenti VM-a odgovaraju očekivanim, unapred definisanim vrednostima i na kraju proverava nonce vrednost kako bi se obezbedila zaštita od napada ponovnog korišćenja.


```
{
"sub": "projects/123456789/attestors/cvm-instance",
"aud": "https://api.example.com",
"iat": 1718300000,
"exp": 1718303600,
"attestation_result": "SUCCESS",
"enclave_verified": true
}
```


Sl. 1 Primer OIDC tokena

- Izdavanje OIDC atestacionog tokena Sl. 1: Ukoliko sve prethodne provere budu uspešno izvršene, Google Cloud Attestation servis generiše OIDC token. Ovaj token je standardni JSON Web Token (JWT) koji VM koristi da eksternim servisima dokaže svoju autentičnost, integritet i sigurno stanje.

IV. Eksperimentalna postavka

U cilju evaluacije performansi sigurnih virtuelnih mašina i distribuiranog sistema, eksperimenti su sprovedeni u dva različita okruženja: lokalnoj infrastrukturi zasnovanoj na AMD SEV-SNP tehnologiji i okruženju baziranom na Google Cloud Confidential VM instancama.

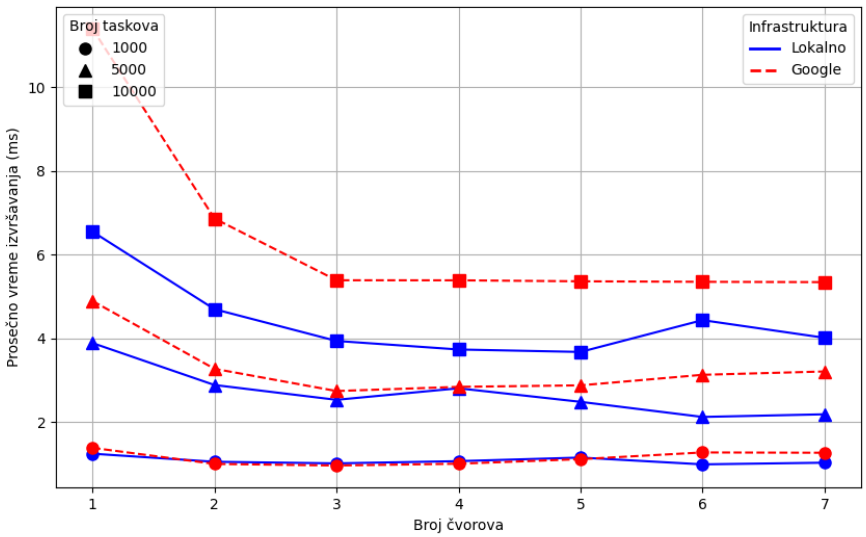
A. *Opis sistema*

Lokalna infrastruktura zasnovana je na serveru opremljenom AMD EPYC 7313P procesorom, koji podržava SEV, SEV-ES i SEV-SNP tehnologije i raspolaže sa 16 procesorskih jezgara, 64 GB RAM-a i 2 TB SSD-a. Virtuelne mašine su pokrenute korišćenjem QEMU emulatora, pri čemu je svaka instanca konfigurisana sa 4 vCPU jezgra i 4 GB RAM-a, uz mogućnost skaliranja do 32 jezgra i 30 GB memorije. U okruženju u oblaku, eksperimenti su sprovedeni na Google Cloud Confidential VM instancama, koje koriste AMD EPYC Milan procesore sa podrškom za Confidential Computing. Svaka instanca je konfigurisana sa 2 vCPU jezgra, pri čemu svako jezgro podržava 2 niti. Memorijski kapacitet svake instance iznosio je 8 GB RAM-a, dok je prostor za skladištenje bio ograničen na 10 GB SSD-a .

B. *Metodologija merenja*

Proces atestacije u lokalnom okruženju vršen je pomoću SEV-SNP mehanizma, gde je mereno vreme potrebno za generisanje i verifikaciju atestacionog izveštaja i sertifikata. Alat koji je korišćen za dohvatanje i verifikaciju atestacije je *snpguest* [9]. Merenja su ponovljena 100 puta, a vreme je beleženo tokom izvršavanja sledećih komandi:

- snpguest report attestation_report.bin – generisanje atestacionog izveštaja
- snpguest verify certs – provera validnosti sertifikata
- snpguest verify attestation – verifikacija atestacionog izveštaja



Sl. 2 Prosečno vreme izvršavanja za zadatak složenosti O(1)

U Google Cloud-u, atestacija je realizovana korišćenjem OIDC vTPM mehanizma, pri čemu je mereno vreme potrebno za generisanje OIDC atestacionog tokena putem komande:

- gotpm token – iniciranje i generisanje atestacionog tokena.

Za analizu performansi distribuiranog računarskog sistema korišćen je Ray okvir, pri čemu je na sedam virtuelnih mašina formiran distribuirani klaster. Jedna instanca služila je kao glavni čvor (eng. *head node*), dok su preostale bile radni čvorovi (eng. *worker nodes*). Ukupan broj čvorova u klasteru varirao je od 1 do 7 čvorova. Glavni čvor je inicijalizovao Ray klaster i delegirao zadatke radnim čvorovima, dok su oni paralelno izvršavali operacije.

Za testiranje performansi korišćeno je obično računanje kvadrata broja i Bubble Sort algoritam, implementiran kao Ray zadatak. Ovaj algoritam je izabran zbog svoje složenosti $O(n^2)$. Eksperiment je podrazumevao paralelno izvršavanje sortiranja velikog skupa nasumičnih podataka na radnim čvorovima, dok su rezultati prikupljani na glavnom čvoru.

Kako bi se ispitao uticaj opterećenja na performanse sistema, eksperiment je sproveden sa različitim brojem paralelnih zadataka – 1000, 5000 i 10000, pri čemu su merenja ponovljena 100 puta kako bi se izračunala prosečna vrednost za svaki nivo opterećenja i dati broj čvorova.

TABLE I. UPOREDNA ANALIZA VREMENA ATESTACIJE U DVA OKRUŽENJA

Okruženje	Vreme izvršavanja (ms)		
	Prosečno	***Minimalno***	***Maksimalno***
Google Cloud VM	1186,5	960	2245
Lokalni SEV-SNP	40,9	28,7	44,9

V. REZULTATI

A. *Rezultati atestacije*

Merenja na Google Cloud virtuelnim mašinama su pokazala da prosečno vreme atestacije u ovom sistemu iznosi 1186,5 ms, dok su zabeležene vrednosti varirale između 960 ms i 2245 ms, pri čemu su pojedine iteracije imale značajno veće trajanje u odnosu na prosečnu vrednost. S druge strane, u lokalnom SEV-SNP okruženju prosečno vreme atestacije iznosilo je 40,9 ms, sa opsegom rezultata od 28,7 ms do 44,9 ms (Tabela I). Rezultati merenja jasno ukazuju na značajnu razliku u vremenu atestacije između dva sistema. SEV-SNP atestacija u lokalnom okruženju pokazala se višestruko bržom u odnosu na OIDC vTPM atestaciju u Google Cloud-u, sa prosečnim vremenom koje je čak 29 puta kraće.

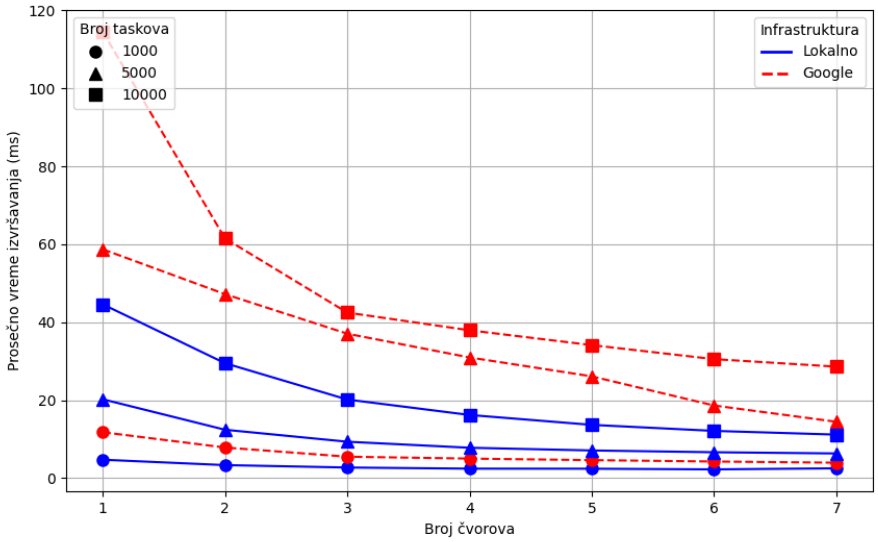
B. *Rezultati Ray zadataka*

Na Sl. 2. su prikazani rezultati merenja za zadatak složenosti $O(1)$ na lokalnoj i na Google infrastrukturi. Merenja su vršena za varijabilan broj zadataka i radnih čvorova. Takođe se može primetiti da prosečno vreme izvršavanja u nekim slučajevima ne opada sa porastom broja čvorova kada je zadat manji broj zadataka. Performanse su približno konstantne kada je zadato 1000 zadataka za obe infrastrukture.

Na Sl. 3. je prikazano merenje koje se odnosilo na izvršavanje zadatka složenosti $O(n^2)$. U ovom slučaju je razlika u performansama između lokalne i Google infrastrukture još primetnija. Lokalna infrastruktura ima manje prosečno vreme izvršavanja za svaku od mogućih konfiguracija. U svim slučajevima, za svaki mogući broj zadataka vidimo opadanje vremena izvršavanja sa porastom broja čvorova.

VI. DISKUSIJA I ZAKLJUČAK

Eksperimentalni rezultati jasno ukazuju na značajne razlike u performansama i skalabilnosti između lokalnog SEV-SNP sistema i Google Cloud VM instanci. Kroz analizu vremena



Sl. 3 Prosečno vreme izvršavanja za zadatak složenosti $O(n^2)$

izvršavanja distribuiranih zadataka, vremena atestacije i sigurnosnih mehanizama, identifikovane su ključne prednosti i ograničenja oba pristupa. Lokalni SEV-SNP sistem pokazao je stabilnije performanse i znatno kraće vreme atestacije u poređenju sa Google Cloud VM instancama. Ova razlika postoji zbog arhitekturalnih razlika atestacionih mehanizama – Google Cloud koristi centralizovani servis za proveru TPM dokaza, što zahteva dodatnu mrežnu komunikaciju između VM instance i Google Cloud Attestation servisa, dok se SEV-SNP atestacija odvija direktno na hardveru, bez potrebe za eksternom validacijom, čime se značajno smanjuje vreme izvršenja procesa. Pored brzine atestacije, dodatni faktor koji je potrebno uzeti u obzir jeste nivo kontrole nad sigurnosnim mehanizmima. U lokalnom SEV-SNP sistemu, korisnik ima potpunu kontrolu nad atestacionim procesom, uz mogućnost direktne provere integriteta svake virtuelne mašine. Nasuprot tome, u okruženju u oblaku, atestacija zavisi od Google Cloud infrastrukture, pri čemu se poverenje oslanja na sigurnosne sertifikate koje izdaje Google. Ovaj model zahteva da korisnici veruju provajderu, dok lokalni sistem omogućava proaktivnu validaciju sigurnosti. Analiza performansi distribuirane obrade pomoću Ray okvira pokazala je da lokalni sistem postiže bolju skalabilnost. Vreme izvršavanja zadataka u lokalnom okruženju opadalo je skoro linearno sa povećanjem broja čvorova, dok je u Google Cloud-u smanjenje vremena bilo manje izraženo i pokazivalo veću

varijabilnost. Za ove rezultate je sigurno zaslužna i veća procesorska moć dostupna na lokalnoj infrastrukturi. Konkretno, na Google Cloud okruženju dostupna su 2 vCPU jezgra, dok su lokalno dostupna 4 sa mogućnošću skaliranja do 32 jezgra. Lokalni SEV-SNP sistem nudi niz prednosti, uključujući bržu atestaciju, stabilnije performanse, efikasnije skaliranje i potpunu kontrolu nad infrastrukturom, što omogućava precizniju optimizaciju i bolju sigurnost. Ključni izazovi u lokalnom sistemu jesu ograničena fleksibilnost i složenije održavanje. S druge strane, Google Cloud VM-ovi nude veću fleksibilnost, omogućavajući brzo prilagođavanje resursa, jednostavno upravljanje i automatizovane servise za monitoring, sigurnost i skaliranje.

LITERATURA

[1] M. Sabt, M. Achemlal and A. Bouabdallah, "Trusted Execution Environment: What It is, and What It is Not," 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 2015, pp. 57-64, doi: 10.1109/Trustcom.2015.357.

[2] P. Moritz, R. Nishihara, S. Wang, A. Tumanov, R. Liaw, E. Liang, M. Elibol, Z. Yang, W. Paul, M. I. Jordan, and I. Stoica. 2018. Ray: a distributed framework for emerging AI applications. In Proceedings of the 13th USENIX conference on Operating Systems Design and Implementation (OSDI'18). USENIX Association, USA, 561–577.

[3] Google, "Google Cloud," [Online]. Available: https://cloud.google.com/?hl=en. [Accessed: Apr. 23, 2025].

[4] AMD, "Secure Encrypted Virtualization (SEV)," [Online]. Available: https://www.amd.com/en/developer/sev.html. [Accessed: Apr. 23, 2025].

[5] G. Scopelliti, C. Baumann and J. T. Mühlberg, "Understanding Trust Relationships in Cloud-Based Confidential Computing," *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Vienna, Austria, 2024, pp. 169-176, doi: 10.1109/EuroSPW61312.2024.00023.

[6] D. Fett, R. Küsters, and G. Schmitz, "The Web SSO standard OpenID Connect: In-depth formal security analysis and security guidelines," *arXiv preprint arXiv:1704.08539*, 2017. [Online]. Available: https://arxiv.org/abs/1704.08539

[7] Advanced Micro Devices, *SEV Secure Nested Paging Firmware ABI Specification*, Rev. 1.57, Publication No. 56860, Jan. 2025. [Online]. Available: https://www.amd.com/content/dam/amd/en/documents/epyc-technical-docs/specifications/56860.pdf. [Accessed: Apr. 23, 2025].

[8] Google, "go-tpm-tools: High-level Go packages for TPM 2.0," GitHub. [Online]. Available: https://github.com/google/go-tpm-tools. [Accessed: Apr. 23, 2025].

[9] VirTEE, "snpguest: A SEV-SNP attestation library and tools," GitHub. [Online]. Available: https://github.com/virtee/snpguest. [Accessed: Apr. 23, 2025].