https://doi.org/10.37528/FTTE/9788673954455/POSTEL.2021.027

MODELOVANJE BEZBEDNOSTI I ALOKACIJA RESURSA U CLOUD OKRUŽENJU PRIMENOM AUKCIJA

Branka Mikavica, Dražen Popović
Univerzitet u Beogradu - Saobraćajni fakultet,
b.mikavica@sf.bg.ac.rs, d.popovic@sf.bg.ac.rs

Rezime: *Cloud resursi su dostupni u formi virtuelnih mašina (VM) sa odgovarajućim kapacitetima za obradu i skladištenje podataka. Bezbednost VM, kao i njihova alokacija i tarifiranje, od presudnog su značaja kako za cloud provajdere, tako i za korisnike cloud servisa. U pogledu bezbednosti, VM su najugroženiji segment u cloud okruženju. U kontekstu alokacije i tarifiranja cloud resursa, aukcije se smatraju obećavajućim rešenjem, budući da podstiču maksimizaciju prihoda cloud provajdera i omogućavaju fer alokaciju resursa onim korisnicima koji ih najviše vrednuju. U ovom radu je predložen model za procenu bezbednosti na nivou VM. Analizirane su različite strategije kreiranja ponuda korisnika cloud servisa za različite nivoe zaštite VM, i to u slučaju primene dve vrste aukcija, Uniform price i Generalized Second-price. Prikazani su rezultati primene ova dva mehanizma aukcija i njihovo poređenje u odnosu na vrednosti pobedničkih ponuda, prihoda cloud provajdera i izgubljene dobiti zbog neraspoloživosti VM usled napada.*

Ključne reči: *cloud virtuelne mašine, aukcija, kreiranje ponuda, tarifiranje, bezbednost*

1. Uvod

Zahvaljujući dinamičkoj organizaciji *cloud* resursa u formi virtuelnih mašina, VM (*Virtual Machines*), virtuelizaciji i elastičnosti, moguće je obezbediti fleksibilno upravljanje resursima na zahtev. Bezbednost se smatra jednim od osnovnih stubova *cloud* okruženja, koje utiče na *cloud* provajdere, korisnike *cloud* servisa, i sve ostale relevantne učesnike. U zavisnosti od toga koja komponenta u *cloud* okruženju je pod uticajem napada, mogu se javiti različite posledice. Napadi na VM često narušavaju zaštitu podataka [1, 2]. Moguća je krađa kriptografskih ključeva i drugih osetljivih podataka sa VM koja je meta napada. Najčešće, VM napadača se nalazi na istom hostu kao i ciljna VM. Tada se tokom kreiranja VM ubacuje maliciozni kod. Sadržaj VM može biti potencijalna meta napada tokom migracije VM sa jednog hosta na drugi. Takođe, moguća je i pojava „krađe resursa“ usled napada. Bezbednost VM značajno utiče na bezbednost celog *cloud* sistema. Nivo bezbednosti i analiza uticaja na performanse sistema su važna pitanja koja je neophodno adekvatno rešiti. U tom kontekstu, unapređenje performansi je jedan od osnovnih ciljeva *cloud* provajdera, dok korisnici *cloud* servisa očekuju zadovoljenje svojih zahteva u procesu obezbeđivanja servisa uz prihvatljive cene.

Tarifiranje pristupa *cloud* resursima je još jedno vrlo značajno pitanje u *cloud* okruženju. Mehanizmi aukcija, kao tipičan primer dinamičkih mehanizama tarifiranja, obezbeđuju varijaciju cene kroz podsticanje konkurencije između korisnika *cloud* servisa i vrše alokaciju resursa onim korisnicima koji te resurse najviše vrednuju. Adekvatno postavljeni mehanizmi aukcija mogu pružiti podsticaj korisnicima da kreiraju istinite ponude, odnosno, da za ponude biraju svoja stvarna vrednovanja pristupa *cloud* resursima. Kreiranje ponuda u aukciji je složen, često netransparentan proces, što je primarni razlog nedovoljne primene dinamičkih tarifnih mehanizama, uprkos nižim cenama u poređenju sa fiksnim tarifnim mehanizmima. Međutim, aukcije se smatraju efektivnim, obećavajućim rešenjem za optimizaciju prihoda *cloud* provajdera. Do sada su predloženi brojni mehanizmi aukcija u *cloud* okruženju, kao što su *Uniform price*, *Second-price*, kombinatorne aukcije, dvostruke aukcije, itd [3]. Većina predloženih mehanizama tarifiranja za cilj ima tarifiranje i alokaciju resursa, bez osvrta na bezbednost sistema. U ovom radu je izršeno modelovanje bezbednosti VM uz tarifiranje i alokaciju resursa primenom aukcija. U zavisnosti od garantovanog nivoa bezbednosti, korisnici *cloud* servisa biraju jednu od tri moguće strategije kreiranja ponuda. Primenjena su dva mehanizma aukcija, *Uniform price* i *Generalized Second-price*. Cilj rada je analiza i poređenje ova dva mehanizma aukcija u zavisnosti od opterećenja u mreži i podsticaja korisnika *cloud* servisa da kreiraju istinite ponude. Pored toga, analizirani su prihodi i izgubljena dobit *cloud* provajdera.

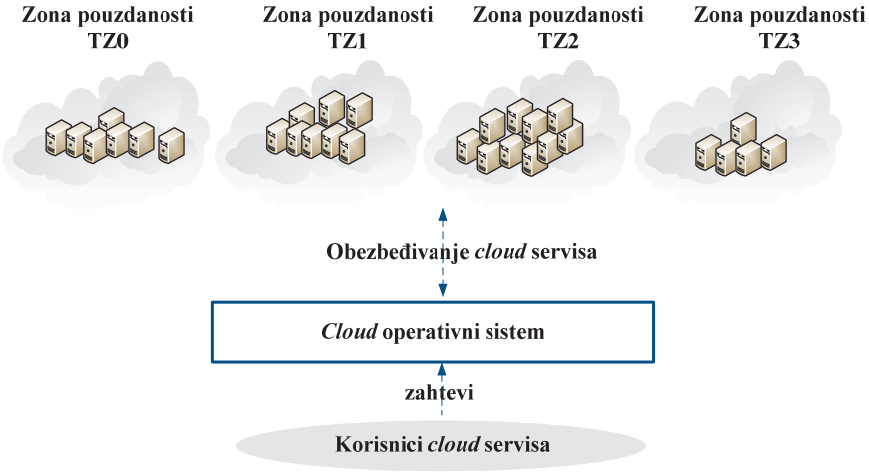
Rad je organizovan na sledeći način. Nakon uvoda, u drugom delu rada je prikazano modelovanje bezbednosti VM, uvedene su strategije kreiranja ponuda i objašnjeni su koraci u procesu aukcija. Treći deo rada predstavlja analizu rezultata. Na kraju rada data su zaključna razmatranja.

2. Postavka problema

Arhitektura analiziranog *cloud* sistema prikazana je na Slici 1. Najznačajniji deo date strukture je *cloud* operativni sistem koji se nalazi u okviru fizičkog sloja. Njegova primarna uloga je upravljanje infrastrukturom, virtuelnim mašinama i opremom, hardverskim i softverskim resursima. Takođe, operativni sistem je zadužen za obradu korisničkih zahteva za pristup *cloud* resursima. U procesu obezbeđivanja *cloud* servisa, korisnički zahtevi se dostavljaju odgovarajućoj VM koja će izvršiti opsluživanje zahteva. Povratne informacije o rezultatima opsluživanja zahteva se šalju nazad od VM ka *cloud* operativnom sistemu. Zahtev za pristup *cloud* resursima se smatra opsluženim ako je isti obrađen, a potvrdne informacije su poslate *cloud* operativnom sistemu. Raspoloživost VM je od krucijalnog značaja za obezbeđivanje *cloud* resursa. Resursi *cloud* sistema obuhvataju sve hardverske i softverske resurse (resurse za skladištenje podataka, servere i virtuelnu infrastrukturu) koji se organizaciju u formi VM. U opštem slučaju, VM su indivialno dostupne standardnim načinima pristupa Internetu. Upravo iz tog razloga su veome podložne malicioznim napadima.

U *cloud* sistemu koji je posmatran u ovom radu, pristup VM je obezbeđen kroz proces aukcija. Imajući u vidu da je neophodan dovoljan broj učesnika na tržištu da bi bilo moguće ostvariti maksimizaciju prihoda u dugom roku [3], pretpostavlja se da je broj korisnika *cloud* servisa, označen sa M, veći od broja dostupnih VM. Bez gubitka opštosti, analiza je izvršena u N uzastopnih vremenskih intervala. Broj korisnika koji iniciraju zahtev za pristup *cloud* resursima može se modelovati primenom Poasonove raspodele sa

parametrima, λ_h i λ_l, za periode visokog i niskog opterećenja u mreži, respektivno [3]. U slučaju pojave malicioznog napada, raspoloživost VM zavisi od primenjenog mehanizma zaštite VM.



Slika 1. Arhitektura cloud sistema

Kako bi inicirao zahtev za pristup *cloud* resursima, korisnik *cloud* servisa kreira ponudu. Prilikom dostavljanja ponude, korisnik definiše vrednost ponude, odnosno, maksimalnu cenu koju je spreman da plati po jednom vremenskom intervalu za datu VM u kojoj je implementiran mehanizam zaštite odgovarajućeg intenziteta. Pod terminom „intenzitet“, u ovom kontekstu, smatra se složenost algoritma za zaštitu bezbednosti, odnosno, nivo bezbednosti [4]. Nakon završetka procesa aukcije, virtuelne mašine se alociraju onim korisnicima *cloud* servisa koji su pobedili u aukciji. Vrednost koju korisnici *cloud* servisa plaćaju za inicijalizaciju VM nije vrednost ponude, već vrednost cene koja se definiše u procesu aukcije. Cena za pristup VM i prihod *cloud* provajdera zavise od primenjenog mehaniza aukcije.

2.1 Modelovanje bezbednosti VM

U pogledu bezbednosti, virtuelne mašine su najugroženiji segment *cloud* sistema. Procena nivoa bezbednosti VM i analiza prethodnih napada, u sprezi sa primenom odgovarajućih mehanizama zaštite, može unaprediti bezbednost *cloud* sistema. U opštem slučaju, pojava napada predstavlja slučajan događaj. Kada je ugrožena raspoloživost VM usled napada, moguća je pojava kašnjenja i otkaza pri opsluživanju korisničkih zahteva. U najkritičnijem slučaju, napadi mogu smanjiti broj raspoloživih VM, čime se značajno narušavaju performanse sistema. Smatra se da je većina napada neorganizovana i spontana, sa slučajnim intervalom međudolazaka [4]. U ovom radu, verovatnoća pojave napada se obeležava sa $p_m \in (0,1)$. Implementacija različitih mehanizama može zaštititi *cloud* sistem u slučaju pojave napada. Međutim, njihova primena zauzima deo računarskih resursa i smanjuje kapacitet za obradu korisničkih zahteva. Moguća je i pojava kašnjenja u procesu obezbeđivanja *cloud* servisa. Dakle, primena mehanizama za zaštitu bezbednosti

utiče na performanse i na raspoloživost VM. Obim zauzetih računarskih resursa koje taj mehanizam zauzima zavisi od kompleksnosti primenjenog algoritma zaštite, odnosno, od nivoa zaštite. Pretpostavlja se da postoje tri različita intenziteta koja su definisana za mehanizam zaštite, i to: veliki, srednji i mali. Što je veći intenzitet zaštite, primenjeni algoritam je složeniji i veći je nivo bezbednosti.

Ukupan broj VM je označen sa n . Pretpostavlja se da su *cloud* resursi podeljeni u zone pouzdanosti, TZ (*Trust Zones)*, kao i da sve VM u okviru jedne zone pouzdanosti primenjuju isti mehanizam zaštite, odnosno, mehanizam sa istim intenzitetom. U sistemu postoji četiri zone pouzdanosti, koje su označene sa TZ0, TZ1, TZ2 i TZ3. U TZ0 nije implementiran nijedan mehanizam zaštite. Zone pouzdanosti TZ1, TZ2 i TZ3 primenjuju mehanizam zaštite malog, srednjeg i velikog intenziteta, respektivno. U svakoj VM, tokom jednog vremenskog intervala može biti opslužen samo jedan zahtev, a svaki zahtev se može opslužiti tokom jednog vremenskog intervala.

Verovatnoća da je jedna VM raspoloživa u jednom vremenskom intervalu označena je sa p_a^h, p_a^m i p_a^l za zone pouzdanosti sa velikim, srednjim i malim intenzitetom datog mehanizma zaštite, respektivno. U slučaju da nije implementiran nijedan mehanizam zaštite, verovatnoća da je VM raspoloživa u datom vremenskom intervalu označena je sa p_a^0. U skladu sa obezbeđenim nivoom zašitite VM u okviru neke zone pouzdanosti, važi $p_a^0 < p_a^l < p_a^m < p_a^h$, pri čemu je $p_a^0, p_a^l, p_a^m, p_a^h \in (0,1)$. Broj raspoloživih VM u jednom vremenskom intervalu $i \in [1, N]$ u okviru zone pouzdanosti $k \in [0,3]$ označena je sa $n_{i,k}$. U slučaju kada mehanizam zaštite ne obezbedi raspoloživost svih VM, važi sledeće $\sum_{k=0}^{3} n_{i,k}$.

2.2 Strategije kreiranja ponuda

Da bi se određena VM inicirala u cilju izvršavanja zahteva korisnika za pristup *cloud* servisima, neophodno je da korisnici kreiraju ponudu u procesu aukcije. Kreiranjem ponude korisnici *cloud* servisa biraju odgovarajući nivo zaštite, odnosno, korisnik definiše zonu pouzdanosti sa mehanizmom zaštite koji je zadovoljavajućeg intenziteta. Istovremeno, korisnik definiše vrednost svoje ponude, odnosno, maksimalnu cenu po vremenskom intervalu koju je spreman da plati za izabranu VM. Skup svih korisnika koji kreiraju ponude u vremenskom intervalu $i \in [1, N]$ označen je sa B_i. Ponuda koju kreira korisnik $j \in B_i$ u vremenskom intervalu $i \in [1, N]$ za zonu pouzdanosti $k \in [0,3]$ može se izraziti kao $b_{i,j,k} = (\upsilon_{i,j}, k)$, gde $\upsilon_{i,j}$ predstavlja vrednost ponude, odnosno, cenu koju je korisnik spreman da plati za VM u izabranoj zoni pouzdanosti sa odgovarajućim nivoom zaštite. Takođe, važno je napomenuti da korisnici *cloud* servisa nemaju informacije o ponudama drugih korisnika. *Cloud* provajder alocira raspoložive VM korisnicima *cloud* servisa koji ih najviše vrednuju. Korisnici sa pobedničkim ponudama mogu inicirati VM, a za to plaćaju vrednost cene za datu VM.

U zavisnosti od primenjenog mehanizma aukcije i izabrane zone pouzdanosti, cene za VM se mogu razlikovati. Cene za zone pouzdanosti TZ0, TZ1, TZ2 i TZ3 u vremenskom intervalu $i, i \in [1, N]$ označene su kao $P_{i,0}, P_{i,1}, P_{i,2}$ i $P_{i,3}$, respektivno. Korisnici *cloud* servisa nisu unapred upoznati sa ovim cenama. Međutim, pretpostavlja se da su javno dostupne cene za VM po zonama pouzdanosti TZ0, TZ1, TZ2 i TZ3 u prethodnom vremenskom intervalu ($P_{i-1,0}, P_{i-1,1}, P_{i-1,2}$ i $P_{i-1,3}$, respektivno). Najveća cena je definisana za zonu pouzdanosti sa najvećim nivoom zaštite (zona pouzdanosti TZ3), dok je najmanja cena definisana za zonu pouzdanosti koja ne podrazumeva implementaciju mehanizma zaštite od napada (TZ0). Imajući u vidu ove cene, korisnik *cloud* servisa bira adekvatnu strategiju i kreira svoju ponudu. U ovom radu su predložene tri moguće strategije: *task-related*, *greedy* i *random* strategija kreiranja ponuda.

2.2.1 *Task-related* strategija kreiranja ponuda

U slučaju *task-related* strategije kreiranja ponuda, korisnici *cloud* servisa koji kreiraju ponudu za iniciranje VM u nekoj zoni pouzdanosti definišu vrednosti ponuda koje su bliske ceni za VM u odgovarajućoj zoni pouzdanosti u prethodnom vremenskom intervalu. U skladu s tim, dostavljene ponude od strane korisnika u vremenskom intervalu *i* za izabranu zonu pouzdanosti uzimaju vrednosti:

$$b^{I}_{i,j,k} \in \left[P_{i-1,k} - \delta, P_{i-1,k} + \delta \right], i \in [1, N], j \in \left[1, \left|B_i\right|\right], k \in [0, 3] \quad (1)$$

δ u (1) označava malo odstupanje od cene u odgovarajućoj zoni pouzdanosti u prethodnom vremenskom intervalu. Verovatnoća izbora ove strategije kreiranja ponuda je označena sa q^I.

2.2.2 *Greedy* strategija kreiranja ponuda

S obzirom na to da korisnici *cloud* servisa plaćaju vrednost cene za datu VM koja se definiše u procesu aukcije, a ne vrednost svoje ponude, korisnici mogu birati *greedy* strategiju kreiranja ponuda, a sve u cilju obezbeđivanja pobede u procesu aukcije i dobijanja prava iniciranja željene VM sa odgovarajućim nivoom zaštite. Na taj način, korisnici kreiraju ponude čije su vrednosti veće od vrednosti cena za VM u datoj zoni pouzdanosti u prethodnom vremenskom intervalu. U tom slučaju, vrednosti ponuda se mogu izraziti na sledeći način:

$$b^{II}_{i,j,k} \in \left[P_{i-1,k+1} - \delta, P_{i-1,3} + \delta \right], i \in [1, N], j \in \left[1, \left|B_i\right|\right], k \in [0, 3] \quad (2)$$

Kao i u prethodnoj strategiji kreiranja ponuda, δ u (2) označava malo odstupanje od cene za VM u datoj zoni pouzdanosti u prethodnom vremenskom intervalu. Ova strategija kreiranja ponuda se podudara sa *task-related* strategijom kreiranja ponuda za one zahteve koji se odnose na pristup VM sa najvećim nivoom zaštite. Verovatnoća izbora ove strategije kreiranja ponuda označava se sa q^{II}.

2.2.3 *Random* strategija kreiranja ponuda

Random strategija kreiranja ponuda podrazumeva da korisnici *cloud* servisa definišu vrednosti ponuda koje su u opsegu vrednosti cena VM u prethodnom vremenskom intervalu. Budući da korisnici *cloud* servisa nemaju informacije o vrednostima ponuda drugih korisnika, ova strategija se može smatrati i istinitom, odnosno, strategijom u kojoj korisnici za vrednost svojih ponuda definišu svoja stvarna vrednovanja. Vrednosti ponuda u slučaju izbora ove strategije kreiranja ponuda mogu se izraziti na sledeći način:

$$b_{i,j,k}^{III} \in \left[P_{i-1,0} - \delta, P_{i-1,3} + \delta \right], i \in \left[1, N\right], j \in \left[1, \left|B_i\right|\right], k \in \left[0,3\right] \quad (3)$$

Slično kao i u prethodnim strategijama kreiranja ponuda, δ u (3) označava malo odstupanje od cene za VM u datoj zoni pouzdanosti u prethodnom vremenskom intervalu. Verovatnoća izbora *random* strategije kreiranja ponuda označena je sa q^{III}. Takođe, važi da je $q^{I} + q^{II} + q^{III} = 1$.

2.3 Mehanizmi aukcija

Nakon prikupljanja svih ponuda za svaku zonu pouzdanosti, vrši se alokacija VM u skladu sa skupom pobedničkih ponuda, odnosno, svaki korisnik *cloud* servisa čija ponuda pripada skupu pobedničkih ponuda može inicirati VM sa zahtevanim nivoom zaštite. Iznosi koje korisnici plaćaju zavise od primenjenog mehanizma aukcije. U ovom radu, analizirane su dva mehanizma aukcija, *Uniform-price* i *Generalized Second-price*, u cilju određivanja prihoda i izgubljene dobiti *cloud* provajdera u procesu alokacije VM sa različitim nivoima bezbednosti.

Skup pobedničkih ponuda za svaku zonu pouzdanosti može se prikazati na sledeći način:

$$W_{i,k} \in \left\{ w_{i,1,k}, w_{i,2,k}, \cdots w_{i,n_{i,k},k} \right\}, i \in \left[1, N\right], k \in \left[0,3\right] \quad (4)$$

U (4), $w_{i,1,k}$ predstavlja ponudu najveće vrednosti za VM u zonama pouzdanosti $k \in \left[0,3\right]$ u vremenskom intervalu $i \in \left[1, N\right]$, $w_{i,2,k}$ predstavlja drugu najveću vrednost ponude, itd.

2.3.1 *Uniform-price* aukcija

U slučaju primene *Uniform-price* aukcije, svaki korisnik *cloud* servisa sa pobedničkom ponudom plaća istu cenu koja je jednaka najmanjoj dobitnoj ponudi. Vrednosti koje plaćaju korisnici koji dobijaju pravo iniciranja VM u procesu aukcije mogu se izraziti sledećim skupom:

$$W_{i,k}^{U} \in \left\{ w_{i,1,k}^{U}, w_{i,2,k}^{U}, \cdots w_{i,n_{i,k},k}^{U} \right\}, i \in \left[1, N\right], k \in \left[0,3\right] \quad (5)$$

S obzirom na to da svi korisnici koji su pobednici u aukciji plaćaju isti iznos, važi sledeće $w_{i,1,k}^{U} = w_{i,2,k}^{U} = \cdots = w_{i,n_{i,k},k}^{U} = w_{i,n_{i,k},k}$. Prihod *cloud* provajdera u slučaju primene *Uniform price* aukcije u vremenskom intervalu $i \in \left[1, N\right]$ može se izraziti na sledeći način:

$$R_i^U = \sum_{k=0}^{3} \sum_{t=1}^{\left|W_{i,k}^U\right|} w_{i,t,k}^U, i \in [1, N] \quad (6)$$

2.3.2 *Generalized Second-price* aukcija

U slučaju primene *Generalized Second-price* aukcije, korisnik koji dobija pravo iniciranja VM plaća vrednost sledeće najveće ponude iz skupa pobedničkih ponuda. Stoga, vrednosti koje korisnici plaćaju za iniciranje zahtevane VM u odgovarajućoj zoni pouzdanosti mogu se prikazati sledećim skupom:

$$W_{i,k}^G \in \left\{ w_{i,1,k}^G, w_{i,2,k}^G, \cdots w_{i,n_{i,k},k}^G \right\}, i \in [1, N], k \in [0,3] \quad (7)$$

Imajući u vidu pravila *Generalized Second-price* aukcije, važi sledeće $w_{i,1,k}^G = w_{i,2,k}$, $w_{i,2,k}^G = w_{i,3,k}, \cdots w_{i,n_{i,k},k}^G = w_{i,n_{i,k}+1,k}$. Prihod *cloud* provajdera u slučaju primene ovog mehanizma aukcije u vremenskom intervalu $i \in [1, N]$ može se prikazati kao:

$$R_i^G = \sum_{k=0}^{3} \sum_{t=1}^{\left|W_{i,k}^U\right|} w_{i,t,k}^G, i \in [1, N] \quad (8)$$

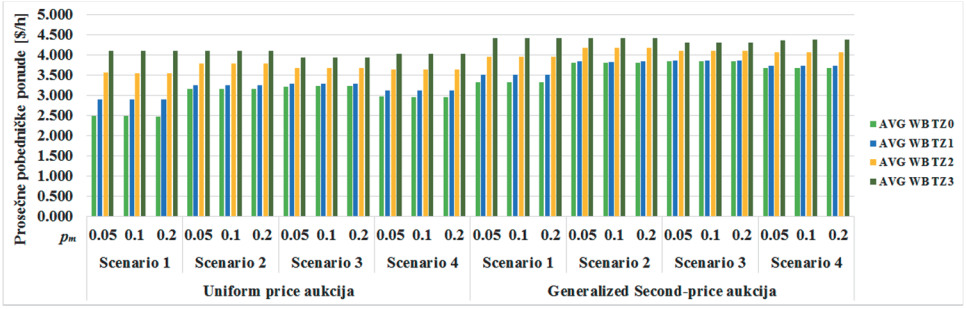
3. Evaluacija performansi

U cilju analize rezultata primene dva prethodno opisana mehanizma aukcija u *cloud* sistemu sa mogućnošću pojave napada, vršene su simulacije u *open source* programskom jeziku *Python 2.7*, u 50 iteracija. Simuliran je period od 30 dana. Svaki dan je podeljen u $N = 24$ vremenska intervala. Vremenski intervali 7-20 pripadaju periodu visokog opterećenja u mreži [3]. Broj korisnika koji iniciraju zahteve za obezbeđivanje *cloud* servisa mogu se modelovati primenom Poasonove raspodele sa parametrima $\lambda_h = 1,25$, i $\lambda_l = 0,75$, za periode visokog i niskog opterećenja u mreži, respektivno. U sistemu ima ukupno 40 VM koje su segmentirane u zone pouzdanosti, pri čemu svaka zona pouzdanosti sadrži 10 VM. Prosečan broj korisnika *cloud* servisa je 80. U slučaju pojave napada, pretpostavljene vrednosti za verovatnoću da će primenjeni mehanizam zaštite obezbediti raspoloživost VM u datoj zoni pouzdanosti su sledeće: $p_a^l = 0,66$, $p_a^m = 0,75$, $p_a^h = 0,84$, za mehanizme zaštite sa malim, srednjim i velikim intenzitetom, respektivno. Takođe, u slučaju napada na VM u zoni pouzdanosti TZ0, u kojoj nije implementiran mehanizam zaštite, verovatnoća da će data VM ostati raspoloživa je $p_a^0 = 0,5$. U radu su posmatrane situacije kada verovatnoća pojave napada na VM uzima sledeće vrednosti $\{0,05, 0,1, 0,2\}$. Inicijalna cena za zonu pouzdanosti TZ0 je izabrana na osnovu javno dostupnih podaka za Amazonove EC2 *spot* instancu *m5n.xlarge* za EU region (Frankfurt) i *Windows* operativni sistem [5] i jednaka je 2,256 $/h. Pretpostavljene

inicijalne cene za VM sa malim, srednjim i velikim nivoom zaštite su 2,820 $/h, 3,525 $/h i 4,406 $/h, respektivno.

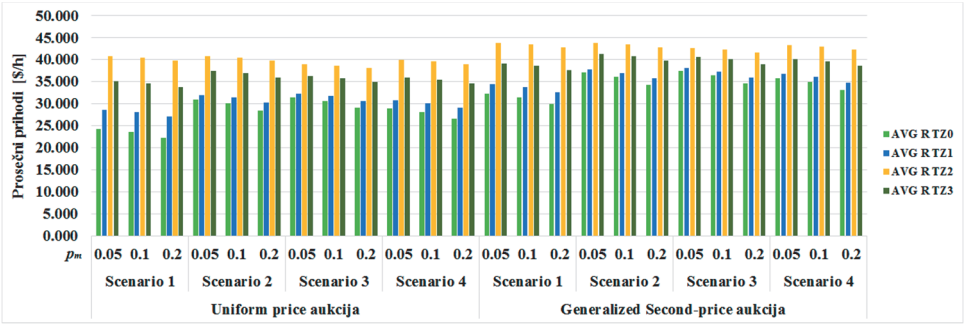
Analizirana su četiri moguća scenarija u zavisnosti od dominantno birane strategije za kreiranje ponuda. Scenariji 1, 2 i 3 predstavljaju slučajeve kada korisnici *cloud* servisa u najvećem broju biraju *task-related* strategiju kreiranja ponuda (q^I=0,50, q^{II}=0,30, q^{III}=0,20), *greedy* strategiju kreiranja ponuda (q^I=0,30, q^{II}=0,50, q^{III}=0,20) i *random* strategiju kreiranja ponuda (q^I=0,20, q^{II}=0,30, q^{III}=0,50), respektivno. Scenario 4 analizira slučaj kada je jednaka verovatnoća izbora svake strategije za kreiranje ponuda ($q^I=q^{II}=q^{III}$=0,33). Parametar koji oslikava odstupanje cene u odnosu na prethodni vremenski interval je $\delta = 0,2$. Zbog nedostatka prostora, svi rezultati u radu su prikazani samo za period visokog opterećenja u mreži. Iste zakonitosti važe i za period niskog opterećenja.

Slika 2 prikazuje prosečne vrednosti pobedničkih ponuda za sve posmatrane strategije kreiranja ponuda u slučaju primene *Uniform price* i *Generalized Second-price* aukcije. AWG WB TZ0, AWG WB TZ1, AWG WB TZ2 i AWG WB TZ3 na Slici 2 označavaju prosečne pobedničke ponude za VM po zonama pouzdanosti TZ0, TZ1, TZ2 i TZ3, respektivno. Rezultati ukazuju na to da *Generalized Second-price* aukcija dovodi do većih prosečnih vrednosti za pobedničke ponude, i to za sve posmatrane scenarije. Iz tog aspekta, *Uniform price* aukcija daje pogodnija rešenja za korisnike *cloud* servisa. Može se uočiti i da Scenario 1 daje najmanje prosečne vrednosti za pobedničke ponude. Dominantan izbor *greedy* strategije kreiranja ponuda (Scenario 2), kao ni dominantan izbor *random* strategije (Scenario 3), nije preporučljiv jer generiše povećanje prosečnih vrednosti pobedničkih ponuda, a samim tim i veće troškove za korisnike *cloud* servisa. Scenario 4 često daje bolje rezultate od Scenarija 2 i 3, ali lošije od Scenarija 1. Kada raste verovatnoća napada na VM, prosečne vrednosti pobedničkih ponuda se razlikuju zbog manjeg broja raspoloživih VM.



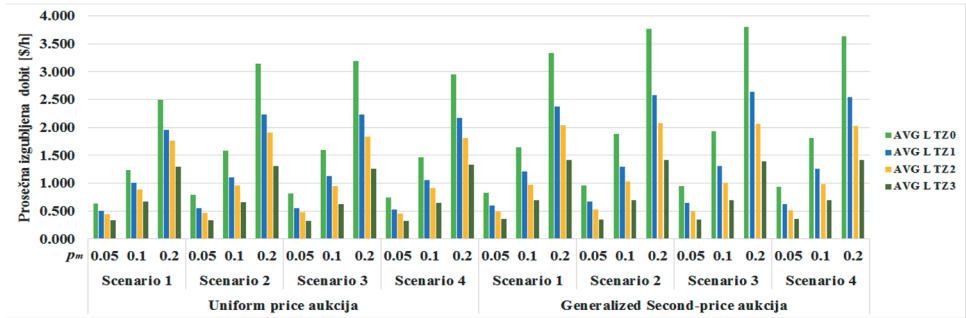
Slika 2. Vrednosti pobedničkih ponuda za period visokog opterećenja u mreži

Slika 3 predstavlja prosečne prihode *cloud* provajdera. AWG R TZ0, AWG R TZ1, AWG R TZ2 i AWG R TZ3 na Slici 3 označavaju prosečne prihode *cloud* provajdera za zone pouzdanosti TZ0, TZ1, TZ2 i TZ3, respektivno. Prihodi neznatno opadaju sa povećanjem verovatnoće napada u svim posmatranim scenarijima. Scenario 3 obezbeđuje najviše prihode za obe aukcije i nezavisno od opterećenja u mreži. Može se uočiti i da *Generalized Second-price* aukcija generiše najviše prihode za sve posmatrane scenarije i za sve vrednosti parametara.



Slika 3. Prihodi cloud provajdera za period visokog opterećenja u mreži

Na Slici 4 su prikazane prosečne vrednosti izgubljene dobiti *cloud* provajdera usled neraspoloživosti nekih VM za sve analizirane strategije kreiranja ponuda, sve scenarije i obe aukcije. AWG L TZ0, AWG L TZ1, AWG L TZ2 i AWG L TZ3 na Slici 4 označavaju prosečnu izgubljenu dobit *cloud* provajdera za zone pouzdanosti TZ0, TZ1, TZ2 i TZ3, respektivno. Pokazuje se da se izgubljena dobit *cloud* provajdera udvostručava sa porastom verovatnoće napada nezavisno od posmatranog scenarija. Viši intenzitet zaštite i primena *Uniform price* aukcije obezbeđuju manje vrednosti za izgubljenu dobit.



Slika 4. Izgubljena dobit cloud provajdera za period visokog opterećenja u mreži

4. Zaključak

U ovom radu analizirana je primena dva mehanizma za tarifiranje i alokaciju *cloud* resursa koji se zasnivaju na *Uniform price* aukciji i *Generalized Second-price* aukciji. Intenzitet mehanizma zaštite je uveden kao relevantan parametar koji oslikava nivo bezbednosti VM. Prilikom kreiranja zahteva za iniciranje željene VM, korisnici *cloud* servisa biraju jednu od tri moguće strategije kreiranja ponuda. U zavisnosti od dominantno izabrane strategije za kreiranje ponuda, posmatrano je nekoliko scenarija. Analizirane su prosečne vrednosti probedničkih ponuda, prihoda i izgubljene dobiti *cloud* provajdera. Rezultati pokazuju da *Generalized Second-price* aukcija ostvaruje veće prihode, nezavisno od izabrane strategije kreiranja ponuda i perioda opterećenja u mreži, dok je *Uniform price* aukcija pogodnija iz aspekta korisnika *cloud* servisa. Takođe, *task-related* strategija kreiranja ponuda se pokazala kao najpogodnija, s obzirom na to da zahteva najmanje prosečne pobedničke ponude u većini slučajeva. Veći intenzitet mehanizma zaštite

obezbeđuje i veće prihode usled većih inicijalnih cena i smanjuje izgubljenu dobit *cloud* provajdera. Međutim, veći intenzitet mehanizma zaštite zahteva više računarskih resursa i povećava troškove *cloud* provajdera. Ovo takođe utiče i na performanse *cloud* sistema, što zahteva sveobuhvatnu analizu i predstavlja predmet budućih istraživanja.

Zahvalnica

Rad je finansiran od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije.

Literatura

[1] B. Mikavica, A. Kostić-Ljubisavljević, D. Popović, "A Security-Driven Approach to the Auction-Based Cloud Service Pricing", *International Journal for Traffic and Transport Engineering*, vol. 11, no. 2, pp. 213-228, 2021. DOI: 10.7708/ijtte.2021.11(2).03

[2] M. A. Khan, "A Survey of Security Issues for Cloud Computing", *Journal of Network and Computer Applications*, vol. 71, pp. 11-29, 2016. DOI: 10.1016/j.jnca.2016.05.010

[3] B. Mikavica, A. Kostić-Ljubisavljević, "Pricing and Bidding Strategies for Cloud Spot Block Instances", *Proc. of the 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) 2018*, Opatija, Croatia, 2018, pp. 419-424. DOI: 10.23919/MIPRO.2018.8400073

[4] H. Xu, X. Qiu, Y. Sheng, L.Luo, Y. Xiang, "A QoS-Driven Approach to the Cloud Service Addressing Attributes of Security", *IEEE Access*, vol. 6, pp. 34477-34487, 2018. DOI: 10.1109/ACCESS.2018.2849594

[5] Amazon EC2 Spot Instances Pricing. (2021). [Online]. Available at: https://aws.amazon.com/ec2/spot/pricing/

Abstract: *Cloud resources are organized into virtual machines (VMs) with corresponding computational and storage capacities. Security and pricing are considered important issues from both cloud provider and cloud customers' perspectives. In terms of security, VMs are one of the most vulnerable segments in the cloud environment. Auction-based mechanisms for pricing and cloud resource allocation are often suggested as a promising solution since they support revenue maximization and fair resource allocation to customers that value them the most. In this paper, the VMs security modelling is introduced to assess the security level of VMs. Various bidding strategies and various security levels provided are analysed under two auction-based mechanisms, Uniform price auction and Generalized Second-price auction. Comparison of these security-driven auction-based pricing mechanisms is provided based on the winning bids, cloud provider's revenues and possible losses due to VMs unavailability.*

Keywords: *cloud virtual machines, auction, bidding, pricing, security*

AUCTION-BASED SECURITY MODELLING AND RESOURCE ALLOCATION IN CLOUD ENVIRONMENT

Branka Mikavica, Dražen Popović