BEZBEDNOSNI ASPEKTI CLOUD COMPUTING OKRUŽENJA U MOGUĆIM VOJNIM PRIMENAMA

Andreja B. Samčović,
Univerzitet u Beogradu, Saobraćajni fakultet, Beograd

DOI: 10.5937/vojtehg61-2595
OBLAST: računarske nauke, telekomunikacije, informatika
VRSTA ČLANKA: stručni članak

Sažetak:

Evolucija cloud computing-a tokom poslednjih nekoliko godina potencijalno predstavlja jedan od najvećih napredaka u istoriji računarstva i telekomunikacija. Iako su prednosti usvajanja koncepta cloud computing-a brojne, postoje i neke značajne prepreke, od kojih je najbitnije pitanje bezbednosti. U ovom radu objašnjava se koncept cloud computing-a; daje se osvrt na tehnološke pokretače cloud computing-a; opisuju se modeli isporuke cloud servisa. Navedeni su postojeći modeli oblaka, kao i neka iskustva u stranim armijama. Osim toga, posebno je razmotrena bezbednost-kao-servis zbog svog značaja u vojnim primenama.

Ključne reči: clouds, computing, evolucija, telekomunikacije.

Uvod

Cloud computing (CC) predstavlja takvu kombinaciju računarskog hardvera, softvera, ekspertize i online usluga, koja podrazumeva više umreženih računara pod istim mrežnim operativnim sistemom, koji je dovoljno fleksibilan da mogu da mu se dodaju/menjaju/oduzimaju resursi bez prekida i koji te resurse može da dodeljuje jednostavnim, ali i kompleksnim aplikacijama (skalabilnost). Što je još bitnije, *cloud computing* je model korišćenja računarskih resursa (servera, diskova, operativnih sistema i aplikacija) na način da se ti resursi iznajmljuju, a ne kupuju.

Posledica takvog pristupa je da korisnik plaća samo onoliko resursa koliko zaista i koristi (*pay-as-you-go*), tako da više ne mora da vodi brigu oko nabavke hardvera i instalacije, kao i održavanja softvera (operativnog sistema i aplikacija) na tom hardveru. Zahvaljujući tome, naučne i vojne aplikacije trebalo bi da budu efikasnije, manevarski prostor veći, uz mogućnost da se uvek koristi najsavremeniji softver i to po povoljnijoj ceni (Mather et al., 2009).

Najveći deo arhitekture *cloud computing*-a koji se danas koristi obuhvata javne *cloud computing* mreže namenjene pružanju usluga putem in-

ZAHVALNICA: Ovaj rad je deo istraživanja na projektima pod brojevima 32025 i 32048, koje finansira Ministarstvo za prosvetu, nauku i tehnološki razvoj Republike Srbije.

andrej@sf.bg.ac.rs

terneta, kao što su *Google Search, Microsoft Hotmail* ili *Google Adsense* (Mather et al., 2009). Veliki provajderi usluga, zajedno sa tipičnim pionirima u prihvatanju novih tehnologija kao što su finansijske usluge i farmaceutske kompanije, takođe primenjuju arhitekturu CC prilikom implementacije privatnih *cloud* mreža zaštićenih *firewall*-om. Ovaj način korišćenja još uvek je u početnoj fazi i očekuje se da će ostvariti dalji rast na bazi korporativnih tehnologija virtuelizacije koje se već sada uvode.

Koncept *cloud computing*-a je proizišao iz ideje iznajmljivanja resursa informacione tehnologije (IT), npr. za procesiranje i skladištenje podataka kao usluge koja se plaća na osnovu korišćenja. Njegovi prethodnici su modeli distribuiranih usluga razvijeni tokom prošle decenije *(utility computing, grid computing, on-demand computing)*.

Sam termin 'oblak' se koristi kao metafora za internet, a potiče iz običaja da se središnja infrastruktura informacionih i komunikacionih usluga, od telefonije, preko serverskih farmi do interneta, crta kao oblak.

Upotreba *cloud computing*-a korisnike oslobađa od kapitalnih ulaganja u IT infrastrukturu, kao i sindroma viška hardvera i softvera *(overprovisioning)*, koji se javlja kada je potrebno da se vršna opterećenja *(peak demands)* pokriju vlastitom IT infrastrukturom.

Kada je potrebno korišćenje više računarskih resursa zbog pojave vršnog opterećenja, moguće je iznajmiti ih u oblaku, a kada potreba za njima nestane, otpustiti ih; samim tim, ne postoji briga oko toga da li skupo plaćena oprema skuplja prašinu ili troši električnu energiju.

Osim toga, možda je najbitnija prednost *cloud computing*-a to što se njime, pored računarskih resursa – hardvera i softvera – zapravo iznajmljuje i konfigurisana serverska farma u koju su ti resursi uklopljeni. Naime, umrežavanjem tako velikog broja računara širom sveta dobija se snaga super-računara i otvaraju novi horizonti za povećanje nivoa usluga i profita (Mather et al., 2009).

Google ovaj princip praktično primenjuje od svog nastanka – svoje usluge isporučuje uz pomoć farmi računara: pretragu interneta obavlja uz pomoć velikih gugIpleksa koji se sastoje od velikog broja običnih, personalnih računara *PC (Personal Computers)* koji nisu skupi, a uz to su lako zamenljivi; njihova procesorska moć se kombinuje tako da korisnicima omogućava da trenutno dođu do željenih informacija u beskrajnom rudniku interneta (Caceres et al., 2010).

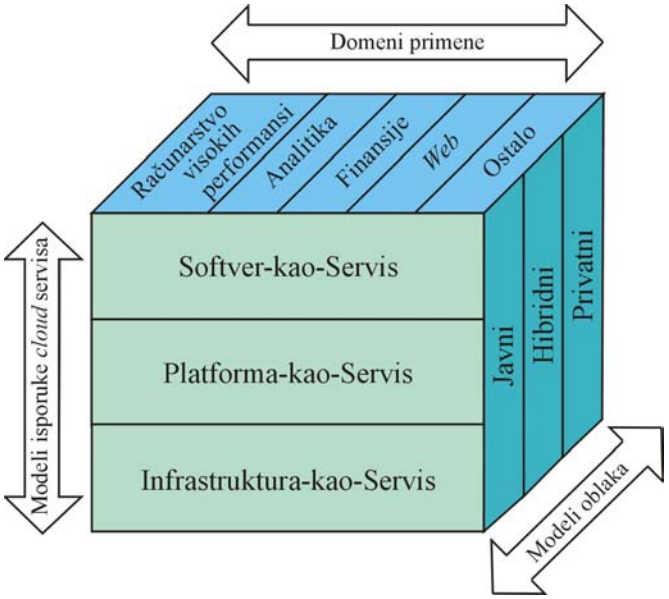
Snaga super-računara je do sada bila dostupna samo armijama, vladinim obaveštajnim službama, univerzitetima i velikim istraživačkim laboratorijama, i to za izvršavanje kompleksnih računanja za zadatke kao što su simulacija nuklearne eksplozije, predviđanje klimatskih promena, ili dizajniranje aviona. *Cloud computing* pruža ovakav tip moći, izvršenje desetina triliona računskih operacija u sekundi, za analiziranje rizika u finansijama, pružanje ličnih medicinskih usluga, čak i pokretanje veoma zahtevnih računarskih igara. Upravo to se postiže umrežavanjem velikih grupa, odnosno farmi servera, koji često koriste jeftinu potrošačku *PC* tehnologiju sa specijalizovanim konekcijama za širenje obrade podataka.

U *cloud computing* sistemu postoji značajni napredak u radu. Lokalni računari više ne moraju da izvršavaju teške poslove prilikom izvršavanja aplikacija. Mreža računara koja kreira oblak obavlja te poslove umesto lokalnih računara. Hardverski i softverski zahtevi na strani korisnika se smanjuju. Jedina stvar koju korisnik računara mora da ima da bi mogao da radi u *cloud computing* sistemu je softverski interfejs koji može biti obični pretraživač *(web browser)*, a CC mreža obavlja sve ostalo (Choo, 2010).

Posle uvodnog dela, u drugom delu rada razmotreni su modeli isporuke *cloud computing* servisa. U narednom poglavlju opisani su modeli oblaka: javni, privatni i hibridni. Zatim su data neka iskustva stranih armija u pogledu CC. Sledeća sekcija razmatra posebno Bezbednost-kao-Servis zbog svog značaja u vojnim primenama. Poslednje poglavlje obuhvata neka zaključna razmatranja.

Modeli isporuke cloud servisa

Framework koji se koristi za opisivanje *cloud computing* servisa poznat je pod akronimom SPI (*Softver Platforma Infrastruktura*) i označava tri najveća servisa koji se pružaju putem oblaka, a to su: Softver-kao-Servis (*SaaS, Software-as-a-Service*), Platforma-kao-Servis (*PaaS, Platform-as-a-Service*) i Infrastruktura-kao-Servis (*IaaS, Infrastructure-as-a-Service*) (Choo, 2010). Slika 1 ilustruje vezu između ovih servisa, njihove upotrebe i modela oblaka.



Slika 1 – SPI framework za cloud computing (Choo, 2010)
Figure 1 – SPI framework for cloud computing (Choo, 2010)

Tradicionalne metode kupovine softvera podrazumevaju da korisnik nadograđuje softver na hardver i da pri tome plaća troškove licence (što je kapitalni trošak). Korisniku je takođe bilo omogućeno da sklopi ugovor o održavanju i da, po određenoj ceni, dobija sigurnosne zakrpe i druge usluge za podršku softvera. Briga o kompatibilnosti operativnih sistema, instaliranju zakrpa i sl. padala bi na teret korisnika.

Softver-kao-Servis (SaaS, Software-as-a-Service)

U *SaaS* modelu korisnik ne kupuje softver, već ga iznajmljuje, tako što ili plaća pretplatu, ili plaća softver onoliko koliko ga koristi *(pay-per-use)*, što je operativni trošak. Uobičajeno je da je kupljeni servis, odnosno usluga, kompletna sa stanovišta hardvera, softvera i podrške. Korisnik pristupa servisu preko bilo kog uređaja za pristup.

Prednosti *SaaS* modela ogledaju se u sledećem:

SaaS omogućava organizacijama da izmeste hostovanje i upravljanje aplikacijama i prepuste ih trećoj strani (prodavcu softvera ili *cloud* servis provajderu) i da na taj način smanje troškove licenciranja softvera, aplikacija i druge infrastrukture, kao i osoblja potrebnog da hostuje te aplikacije unutar organizacija.

SaaS omogućava prodavcima softvera da kontrolišu i ograniče korišćenje, da zabranjuju umnožavanje i distribuiranje, i uopšte im olakšava kontrolisanje svih izvedenih verzija njihovog softvera. Ovakav vid centralizovane kontrole omogućuje prodavcima i distributerima softvera da uspostave stalni priliv prihoda od mnogobrojnih organizacija i pojedinačnih korisnika bez potrebe da učitaju softver kod svakog korisnika ili organizacija ponaosob.

Isporuka aplikacija upotrebom *SaaS* modela bazira se na *one-to-many* principu korišćenjem mreže *(web)* kao infrastrukture. Krajnji korisnik može pristupiti *SaaS* aplikaciji preko *web* pretraživača. Pojedini distributeri obezbeđuju svoj interfejs projektovan tako da podržava karakteristike jedinstvene za njihove aplikacije.

Korišćenje *SaaS* modela ne zahteva hardver; može se pokrenuti preko postojeće infrastrukture za pristup internetu. Ponekad su potrebna dodatna podešavanja zaštitnog zida (*firewall*). Ponuda *SaaS* modela se najčešće realizuje preko javne mreže, tako što se aplikacijama baziranim na ovom modelu pristupa preko interneta.

Najznačajnija razlika u arhitekturi između tradicionalnog modela softvera i *SaaS* modela ogleda se u broju zakupaca, odnosno korisnika koje aplikacija podržava, tj. opslužuje. Tradicionalni model softvera je izolovani model koji podrazumeva jednog korisnika, što znači da korisnik kupuje softversku aplikaciju i instalira je na serveru. *SaaS* je model čija arhitektura podržava veći broj korisnika, što znači da je fizička infrastruktura hardvera deljena među većim brojem korisnika, ali je logički jedinstvena za svakog korisnika ponaosob (Choo, 2010).

Posebnu pažnju treba posvetiti funkcijama provere autentičnosti i kontrole pristupa, koje nudi *cloud* servis provajder *SaaS* modela. To je najčešće jedini način kontrole bezbednosti koji je dostupan za upravljanje rizikom kome su informacije izložene.

Mnogi provajderi nude korisnički interfejs sa alatima za proveru autentičnosti i kontrolu pristupa aplikacijama. Pojedine *SaaS* aplikacije imaju ugrađene funkcije pomoću kojih korisnici mogu da dodele privilegije čitanja i pisanja drugim korisnicima. Međutim, upravljanje takvim privilegijama može imati slabe tačke zbog kojih njihovo korišćenje ne bi bilo u skladu sa standardima kontrole pristupa neke organizacije.

Platforma-kao-Servis (PaaS, Platform-as-a-Service)

U slučaju *PaaS* modela, provajder nudi razvojno okruženje programerima koji razvijaju aplikacije i nude svoje usluge preko platforme provajdera. Uobičajeno je da *cloud* servis provajder nudi alate i standarde za razvoj, kao i kanale za distribuciju i plaćanje tih usluga. Takođe je uobičajeno da provajder naplaćuje pružanje platforme i usluge prodaje i distribucije servisa. To omogućava brzo širenje softverskih aplikacija, s obzirom na nisku cenu pristupanja kanalima koji korisnicima stoje na raspolaganju.

PaaS predstavlja varijaciju *SaaS* modela, pri čemu se razvojno okruženje nudi kao servis. Programeri koriste gradivne blokove (unapred definisane i određene blokove koda) razvojnog okruženja za kreiranje sopstvenih aplikacija. Takođe, sami alati za razvoj aplikacija su hostovani u oblaku i pristupa im se preko pretraživača; na taj način je programerima omogućeno da kreiraju aplikacije bez prethodnog instaliranja alata.

PaaS model je naročito koristan zato što omogućuje malim i novim kompanijama da razviju i koriste aplikacije bez troškova kupovine servera i bez potrebe za njihovim podešavanjem (Choo, 2010).

Uopšteno govoreći, *cloud* servis provajderi *PaaS* modela su odgovorni za obezbeđivanje platforme na kojoj se pokreću korisničke aplikacije. Aplikacije *PaaS* modela mogu da koriste komponente ili *web* servise koje pruža treća strana, tj. provajder aplikacija, pa je u tom slučaju provajder odgovoran za bezbednost svojih usluga. Dakle, korisnici bi trebalo da razumeju zavisnost njihovih aplikacija od svih usluga i procene rizike koji se odnose na pružanje usluga od strane trećeg provajdera. Sve do sada, *cloud* servis provajderi nisu bili voljni da otkrivaju informacije koje se tiču bezbednosti platforme, koristeći kao argument da bi takve informacije hakeri mogli da upotrebe u svoju korist. Ipak, korisnici bi trebalo da zahtevaju transparentnost od *cloud* servis provajdera i da traže pristup informacijama neophodnim za procenjivanje rizika i upravljanje bezbednošću.

U slučaju *PaaS* modela isporuke servisa, osnovni principi bezbednosti su čuvanje i izolacija aplikacija jednih korisnika od aplikacija drugih korisnika. *Cloud* servis provajder je odgovoran za praćenje novih grešaka i ranjivosti koje mogu biti iskorišćene za eksploataciju *PaaS* platforme. Takva situa-

cija predstavlja najgori scenario za *PaaS* usluge; implikacije vezane za privatnost osetljivih korisničkih informacija su nepoželjne i mogu da nanesu veliku štetu u radu. Stoga bi korisnici trebalo da budu upoznati sa načinom na koji *cloud* servis provajderi upravljaju platformama (Carlin and Curan, 2011).

Infrastruktura-kao-Servis (IaaS, Infrastructure-as-a-Service)

IaaS model je sličan modelu računarstva u vidu usluge *(utility computing)* koji se zasniva na ideji da se računarske usluge nude na isti način kao komunalne usluge *(utilities)*. To znači da korisnik plaća usluge koje zaista i koristi, kao što su: utrošena procesorska snaga, prostor za skladištenje na disku, fizički računarski resursi, lokacija, *backup*, i dr.

IaaS je model koji se najčešće povezuje sa pojmom *cloud computing*-a i odnosi se na *online* servise koji korisnika oslobađaju brige o detaljima o infrastrukturi. U slučaju CC, provajder u potpunosti ima kontrolu nad infrastrukturom. S druge strane, korisnici računarstva u vidu usluge sami traže servis koji će im omogućiti da upravljaju *online* uslugama; pri tome koriste i plaćaju resurse *cloud* servis provajdera.

Bitna karakteristika *IaaS* modela, pored već pomenutih, kao što su skalabilnost i plaćanje na bazi ostvarene potrošnje, je najbolje-od-tehnologije i resursa *(best-of-breed technology and resources)*, što korisnicima omogućava pristup najboljim tehnološkim rešenjima za deo ukupne cene koštanja (Choo, 2010).

Među velikim brojem tehnologija koje pokreću *cloud computing*, najvažnija je virtuelizacija, kao osnova za *IaaS*. Virtuelizacija je omogućila odvajanje aplikacija od servera, njihovu mobilnost i fleksibilnost u alociranju resursa. Drugim rečima, korišćenjem virtuelizacije, aplikacije se ne vezuju za hardver i mogu se slobodnije prenositi sa servera na server i iz jednog centra za obradu podataka u drugi.

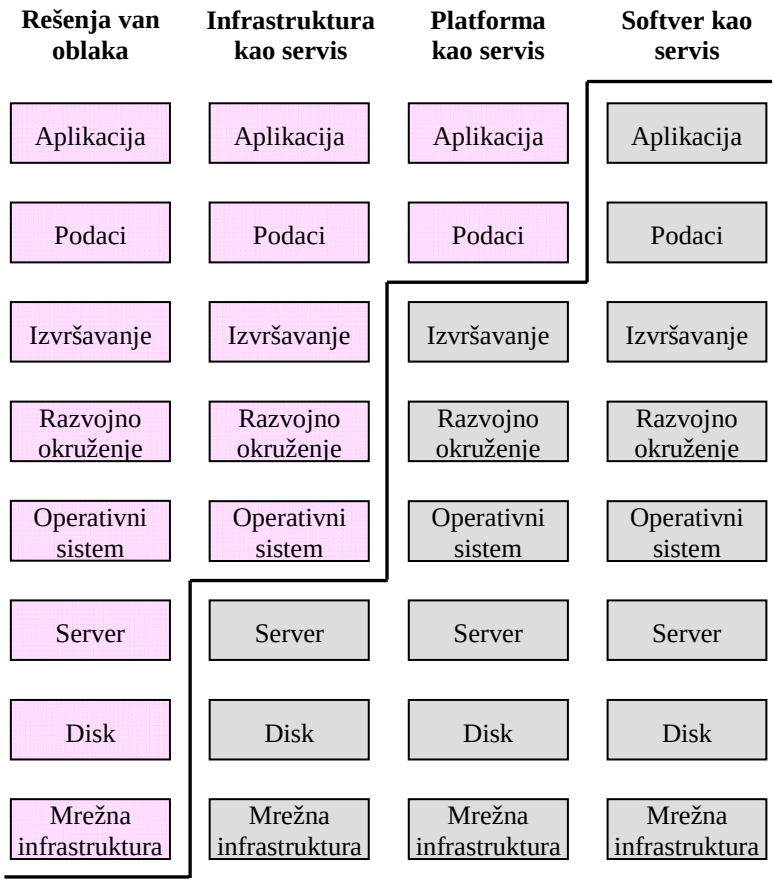
Danas postoje različite forme virtuelizacije, uključujući virtuelizaciju operativnog sistema *(VMware, Xen)*, virtuelizaciju skladištenja *(NAS – Network Attached Storage, SAN – Storage Area Network)* i virtuelizaciju aplikacija ili softvera *(Apache Tomcat, JBoss, Oracle App Server, WebSphere)* (Mather et al., 2009).

Za primer se može uzeti virtuelizacija operativnog sistema. Savremena virtuelizacija dozvoljava pokretanje više instanci operativnih sistema na jednom računaru. Ovi operativni sistemi dele resurse zajedničkog hardvera. Kontrola nad hardverom je prepuštena softveru koji se bavi pristupima procesoru, memoriji, ulazno-izlaznim operacijama, hard diskovima i mrežnim hardverom.

Virtuelizacija je tako, na sebi svojstven način, pomirila dve krajnosti u pogledu organizacije IT sistema – centralizovan sistem naspram decentralizovanog. Umesto da se nabavljaju novi računari sa savremenim perifernim uređajima, korišćenjem virtuelizacije u upotrebu se stavlja centralni hardver na sloju

ispod virtuelnih mašina i na taj način se obavlja centralizacija čitavog sistema. Osnovna korist od ovoga jeste to što takva celina sada može mnogo lakše da se održava. Potrebno je samo na jednom računaru instalirati sigurnosne zakrpe, nove verzije aplikacija ili dodatne alate i svi korisnici sistema preko virtuelnih mašina imaće iste uslove za rad (Đekić, 2008).

Jednostavno rečeno, sistem za virtuelizaciju jedan računar pretvara u višestruki računar na kome se istovremeno izvršava više operativnih sistema. Na taj način se korisniku čini da se svaki od tih operativnih sistema i programa na njima izvršava na nezavisnom računaru. Upravo to omogućuje oblaku opsluživanje više korisnika istovremeno. Naravno, svakom od tih operativnih sistema, odnosno njihovim korisnicima, čini se da je računar samo njihov, tj. nisu svesni ostalih operativnih sistema (Nick et al., 2010). Slika 2 pokazuje nadležnosti provajdera i korisnika kod različitih vrsta servisa u oblaku.



Slika 2 – Nadležnosti provajdera i korisnika kod različitih vrsta servisa u oblaku
Figure 2 – Competences of providers and users for different services in the cloud

Hardverske platforme sa tehnikom *load balancing* se često koriste za sprovođenje nastavka servisa nakon ispada jedne ili više komponenti. Komponente se prate kontinuirano i kada nema odziva neke komponente onda se o tome obaveštava *load balancer* i više se ne šalje saobraćaj ka toj komponenti. Očuvanje energije i resursa nisu uvek centralno mesto kada se govori o CC, ali sa pravilnim balansom opterećenja potrošnja resursa može da bude svedena na minimum. Ovaj postupak ne služi samo da održi troškove nižim i organizacije više „zelenim“, već i za to da komponente platforme budu dugotrajnije. Tehnika *load balancing* takođe omogućuje i druge važne funkcije kao što je skalabilnost.

U slučaju *IaaS* modela, korisničke aplikacije i platforma na kojoj se pokreću rade na virtuelnim korisničkim serverima; instaliraju ih i njima upravljaju sami korisnici. To znači da korisnici snose punu odgovornost za bezbednost aplikacija smeštenih u oblaku, pa ne bi trebalo da očekuju pomoć u obezbeđivanju aplikacija od strane *cloud* servis provajdera, osim dobijanja osnovnih smernica i upoznavanja sa karakteristikama zaštitnog zida koje mogu da utiču na komunikaciju korisničkih aplikacija sa drugim aplikacijama, korisnicima i uslugama, u okviru ili izvan oblaka.

Web aplikacije moraju biti projektovane tako da poseduju standardne bezbednosne mere protiv uobičajenih pretnji koje sa sobom nosi korišćenje interneta. Korisnici su isključivo odgovorni za čuvanje svojih aplikacija, postavljanje sigurnosnih mera i zaštitu sistema od malicioznih programa i hakera koji pokušavaju da neovlašćeno pristupe njihovim podacima smeštenim u oblaku (Mather et al., 2009).

Modeli oblaka

Kao što je ranije napomenuto, termin ’oblak’ je metafora za internet i predstavlja pojednostavljeni prikaz složenih, međusobno povezanih uređaja i veza koje čine internet. Javni i privatni (drugi naziv: eksterni i interni) oblaci su delovi interneta i definišu se (ili, bolje rečeno, razlikuju se) na osnovu veze koju formiraju sa nekom organizacijom.

Javni oblaci

Javni (eksterni) oblaci opisuju se na tradicionalni način, što podrazumeva samoposluživanje resursima preko interneta, pomoću web aplikacija ili web servisa, a koje pruža i naplaćuje treća strana, odnosno *cloud* servis provajder.

Javni oblak hostuje treća strana, tj. *cloud* servis provajder; on takođe rukovodi i upravlja oblakom. Usluge oblaka su dostupne brojnim korisnicima preko zajedničke infrastrukture.

U slučaju javnog oblaka, upravljanje bezbednošću je prepušteno trećem licu, tj. *cloud* servis provajderu, koji je odgovoran za ponudu servisa u javnom oblaku. Samim tim, korisnici servisa javnog oblaka imaju niži stepen kontrole i nadzora nad fizičkim i logičkim bezbednosnim aspektima javnog oblaka (Choo, 2010).

Privatni oblaci

Privatni (interni) oblaci predstavljaju verziju *cloud computing*-a na privatnim mrežama; donose izvesne prednosti CC bez klopki, kapitalizacije bezbednosti podataka i briga oko pouzdanosti uopšte (Nick et al., 2010).

Organizacije na početku moraju da kupe, izgrade i upravljaju oblacima, pa stoga ne dolazi do smanjenja početnih kapitalnih troškova i potrebnih obučenih kadrova. Vlasnik privatnog oblaka (institucija, kompanija) čiji su korisnici npr. zaposleni je odgovaran za upravljanje oblakom.

Privatni oblaci se razlikuju od javnih po tome što se mrežna i računarska infrastruktura dodeljuju samo jednoj organizaciji – nije deljena među većim brojem organizacija (postoji samo jedan korisnik oblaka).

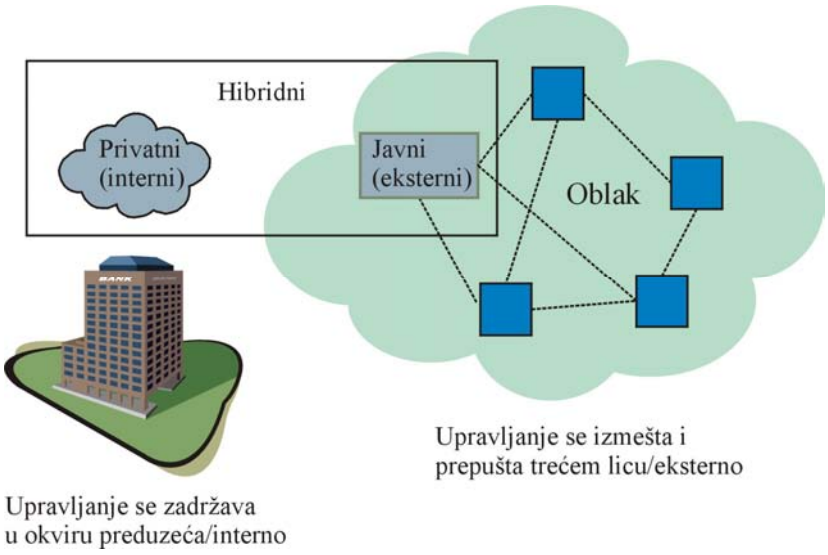
U slučaju privatnog oblaka, upravljanje bezbednošću je posao internog IT odeljenja organizacije. To znači da korisnici privatnog oblaka imaju visoki stepen kontrole i nadzora nad fizičkim i logičkim bezbednosnim aspektima infrastrukture privatnog oblaka. Sa tako visokim stepenom kontrole i transparentnosti, korisnicima je lakše da rade u skladu sa ustanovljenim korporativnim bezbednosnim i regulatornim standardima (Sangroya, 2010).

Tehnički standardi za povezivanje različitih računarskih sistema i delova softvera potrebnih za rad CC još uvek nisu u potpunosti definisani, što može usporiti razvoj novih usluga. Za probojem širokopojasnog pristupa internetu u Sjedinjenim Američkim Državama zaostaju mnoge zemlje u Evropi i Aziji, a bez brzih konekcija, posebno bežičnih, *cloud computing* neće biti široko dostupan.

Primer za privatni oblak bi bio *Amazonov* servis *Elastic Compute Cloud (EC2). EC2* je web servis koji omogućuje skalabilnu realizaciju aplikacija obezbeđivanjem interfejsa preko kojeg korisnici mogu da kreiraju virtuelne mašine tj. instance servera, i na njih postave bilo koji softver. Korisnici mogu da kreiraju, pokreću i terminiraju instance servera prema potrebi, plaćajući po satu za aktivne servere. Jednostavnije rečeno, korisnici plaćaju pristup virtuelnim računarima. Na primer, korisnik može iznajmiti virtuelni računar s operativnim sistemom *Windows* i udaljeno se spajati na njega pomoću protokola poput *SSH (Secure Shell)*. Pri tome, korisnik ima opciju određivanja početnih resursa za virtuelni računar i može ih menjati po potrebi. Osim toga, *EC2* može da sarađuje sa *Amazonovim* web servisima koji pružaju dodatni memorijski prostor i relacijske baze podataka.

Hibridni oblaci

Hibridno okruženje čini više javnih i/ili privatnih oblaka. Hibridni oblaci su projektovani tako da zadovolje specifične poslovne i tehnološke zahteve, pomažući optimizaciju bezbednosti i privatnosti uz smanjene IT investicije. Hibridni oblak organizacijama pruža mogućnost da manje osetljive (*non-core*) aplikacije pokreću unutar javnog oblaka, a da osetljive (*core*) aplikacije i podatke zadrže unutar privatnog oblaka (Choo, 2010), što je pokazano na Slici 3.



Slika 3 – Hibridni oblak (Choo, 2010)
Figure 3 – Hybrid cloud (Choo, 2010)

Budući da hibridni oblak predstavlja kombinaciju javnih i privatnih oblaka, kod njega se pokušava da se izbegnu ograničenja oba pristupa. Kod hibridnog oblaka deo infrastrukture servisa se nalazi u privatnom oblaku, a deo u javnom oblaku. Hibridni oblaci pružaju veću fleksibilnost nego privatni i javni oblaci ponaosob. Obezbeđuju bolju kontrolu i bezbednost aplikacija u poređenju sa javnim oblacima, zadržavajući pri tome mogućnost ekspanzije i kontrakcije servisa na zahtev. Sa druge strane, projektovanje hibridnog oblaka zahteva pažljivi kompromis između komponenata privatnog i javnog oblaka.

Primer za hibridnu mrežu bi bila platforma *Aneka* za razvoj distribuiranih aplikacija u oblaku, kroz implementaciju *PaaS* modela (Vecchiola et al, 2009). Ključna osobina *Aneka* sistema je servisno orijentisano okruženje koje koristi i fizičku i virtuelnu infrastrukturu i omogućava izvršenje aplikacija razvijenih u različitim modelima. Administratori sistema mogu da pristupe kolekciji alata koja se nalazi u javnom oblaku dostupnom preko interneta, ili u privatnim oblacima koji čine niz čvorova sa ograničenim pristupom u okvi-

ru intraneta neke organizacije. Imajući to u vidu, sa istog računara se može pristupati spoljnjim i unutrašnjim resursima. Navedene osobine *Aneka* sistema čine ga interesantnim za obrazovne, akademske i vojne primene.

Pregled postojećih vojnih primena cloud computing-a

Cloud computing okruženje može biti iskorišćeno u vojnim primenama. NATO (*North Atlantic Treaty Organization*) pakt je razvio *PaaS* platformu pod imenom *Snow Leopard Cloud* za razne vojne vežbe, kao i mirovne misije (Cayirci et al, 2009). Navedena platforma koristi web 2.0 aplikacije, videokonferenciju, govor preko internet protokola (*Voice over IP*), kao i upravljanje na daljinu preko ručnih uređaja i terminala. Oblak *Snow Leopard* je usmeren prema vojnim primenama i zbog toga ima višenivovsku bezbednost, kao i kriptovanu infrastrukturu mreže. Visoka privatnost i bezbednosni standardi se primenjuju koristeći pristup *single-sign-on*, gde korisnici moraju da se uloguju da bi pristupili različitim servisima.

Druga vojna primena CC bila bi u oblasti regrutacije. Američka armija je počela da koristi CC da bi poboljšala proces regrutacije novih kadeta (Wyld, 2009). Pri tome se kombinuju *cloud computing* rešenja sa društvenim mrežama preko mobilnih uređaja, kako bi se izašlo u susret novim generacijama. Osim toga, CC pristup se upotrebljava i kako bi se javnost što bolje informisala o armiji. Korišćenje *SaaS* modela je omogućilo američkoj armiji da radikalno izmeni svoj pristup naporima pri regrutaciji na efikasan način, koji uz to i umanjuje troškove. Aplikacija u oblaku je dramatično smanjila troškove hardvera. Procenjuje se da je korišćenje *SaaS* modela znatno jevtinije od izgradnje nove platforme u tu svrhu i da okvirno iznosi 54.000$ godišnje. Nasuprot tome, izgradnja tradicionalnog sistema bi koštala desetak puta više. *SaaS* model je pokazao dobre performanse u pogledu skalabilnosti, kao i znatno kraćeg vremena potrebnog za poboljšanje sistema. Sa novim CC sistemom, regrutima je omogućeno da budu dinamički povezani sa ostalim učesnicima bilo gde i bilo kada koristeći pri tome savremene mobilne uređaje.

Bezbednost-kao-Servis

U ovom poglavlju biće reči o bezbednosti koja se pruža u vidu usluge, tj. kao jedan od modela isporuke *cloud* servisa. Slično kao Softver-kao-Servis, i model isporuke *cloud* servisa Bezbednost-kao-Servis (*Security-as-a-Service, BkS*) se dostavlja korisnicima na bazi pretplate.

Postoje tri podsticaja za razvoj Bezbednosti-kao-Servisa. Najraniji pokretač je, sada već više od decenije star, *spam*, tj. neželjena pošta. Još

1999. godine kompanija *Postini* ponudila je uslugu filtriranja *e-mail*-ova, koju danas nude brojne kompanije i internet servis provajderi (http://googleblog.blogspot.com/2007/09/weve-officially-acquired-postini.html).

Drugog pokretača za razvoj Bezbednosti-kao-Servisa predstavljaju servisi za upravljanje bezbednošću *(MSS, Managed Security Services)*. Podsticaj za korišćenje *MSS*-a bio je (i još uvek je) isti kao i za upotrebu CC: sniženi troškovi u odnosu na kućna rešenja, usled korišćenja zajedničkih resursa. Takođe, *MSS* model je probio neformalnu, ali snažnu barijeru izmeštanja *(outsourcing)* delova informaciono-bezbednosnog programa neke organizacije. U ovom slučaju, izmeštanje podrazumeva upravljanje uređajima izvan same organizacije *(off-premises)*. Treba napomenuti da, iako izmeštanje informacione bezbednosti često postoji kao opcija, u početku se koristilo samo izmeštanje u okviru organizacije *(outsourcing on-premises)*, tj. izmeštanje u drugu prostoriju u okviru istog objekta, za razliku od izmeštanja van samog objekta *(off-premises)*.

Iako je upravljanje bezbednošću izmešteno u *MSS* modelu, odgovornost za bezbednost ostaje na strani korisnika. Korisnik je taj koji je odgovoran za upravljanje i nadgledanje *MSS*-a; korisnik takođe određuje koji će propisi biti sprovedeni. Provajder *MSS*-a nadgleda i upravlja uređajima (npr. *firewall* – zaštitnim zidom) i protokom podataka (npr. filtriranjem *e-mail*-ova); međutim, ti uređaji pripadaju korisniku. Kao rezultat toga, uštede i efikasnost se mogu povećati samo do određene granice. Iako je *MSS* servis na bazi pretplate (što je operativni trošak), korisnik nije oslobođen kapitalnog troška kupovine hardvera. U slučaju *cloud computing*-a, kapitalni trošak je još više umanjen zato što je posedovanje najvećeg broja uređaja, njihovo nadgledanje i upravljanje odgovornost *BkS* provajdera.

Treći pokretač za razvoj Bezbednosti-kao-Servisa predstavlja opadanje organizacione efikasnosti u pokušaju pružanja bezbednosti direktno na krajnjim tačkama *(endpoints)*. Ne samo da dolazi do umnožavanja ovih tačaka, već imaju veliki broj konfiguracijskih promenljivih, pa IT odeljenja ne uspevaju da njima efikasno upravljaju. Pored toga, mnoge od ovih krajnjih tačaka su mobilne, što rešavanje problema konfiguracije i ažuriranja bezbednosnog softvera čini obimnim i teškim zadatkom (Benoit, 2009).

Zbog svega navedenog, kao i zbog eksplozivnog rasta malicioznih programa, zaštita krajnjih tačaka na krajnjim tačkama *(endpoints on the endpoints)* predstavlja rastući problem. Na primer, *Symantec* je 2008. godine otkrio 1.656.277 malicioznih pretnji (CloudAV, 2009). Ovo je dovelo do promene u razmišljanju o tome kako zaštititi krajnje tačke. Umesto nadgledanja i upravljanja samim krajnjim tačkama, čišćenje saobraćaja se može obaviti u oblastima od oblaka do krajnjih tačaka i obrnuto.

Pokazalo se da antivirus baziran na oblaku *(cloud-based antivirus)* pruža 35% bolju detekciju pretnji od antivirusa baziranog na krajnjim tačkama, kao i ukupnu stopu otkrivanja od 98%, što su značajno bolji rezultati (Mather et al, 2009).

Usluge za poboljšanje bezbednosti informacija

Današnja ponuda u *BkS* segmentu uključuje više usluga za poboljšanje informacione bezbednosti: filtriranje *e-mail*-ova (uključujući *backup* i arhiviranje), filtriranje *web* sadržaja i upravljanje ranjivošću *(vulnerability management)*.

Filtriranje e-mail-ova

Ova usluga pre svega podrazumeva čišćenje neželjene pošte, *phishing e-mail*-ova i malicioznih kodova; pri tome se *anti-malware* pokreće u oblaku a ne direktno na krajnjim tačkama. Ovaj servis čišćenja-u-oblaku *(cleansing-in-the-cloud service)* za posledicu ima brojne prednosti: smanjeno opterećenje *e-mail* servera i poboljšanje efikasnosti *anti-malware* softvera.

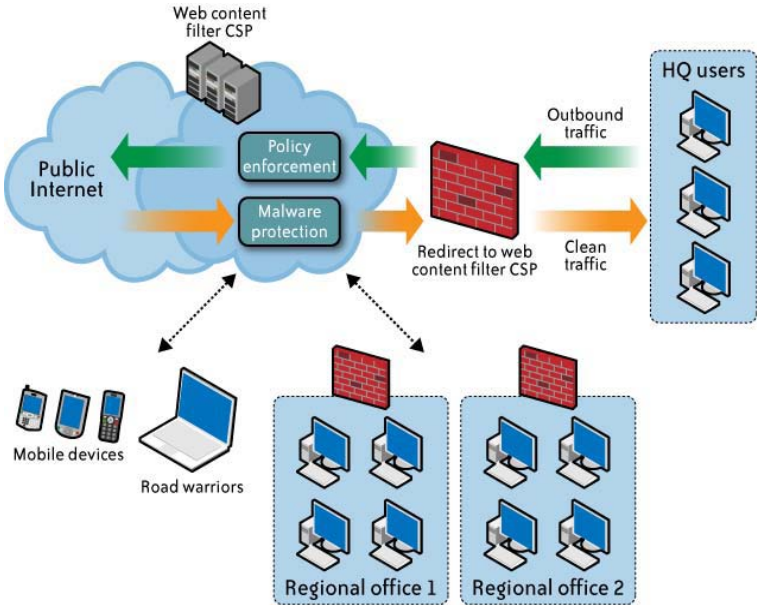
Iako je najviše pažnje usmereno na dolazne *e-mail*-ove, ova usluga se koristi i za filtriranje odlazne pošte. Mnoge organizacije žele da se osiguraju od nenamernog slanja zaraženih *e-mail*-ova, pa čišćenje odlazne pošte predstavlja dobar način za sprečavanje takvih problema i nelagodnosti koje nose sa sobom.

Filtriranje *e-mail*-ova uključuje *backup* i arhiviranje, što podrazumeva skladištenje i indeksiranje pošte koja se smešta u centralnu bazu. To dalje organizaciji omogućava pretraživanje po brojnim parametrima, kao što su datum, primalac, pošiljalac, tema i sadržaj (Mather et al, 2009).

Filtriranje web sadržaja

Dok krajnje tačke organizacije pokušavaju da preuzmu saobraćaj, taj saobraćaj se preusmerava ka *BkS* provajderu koji traži i uklanja maliciozne pretnje i osigurava da se samo čist saobraćaj isporučuje krajnjim korisnicima. Organizacije takođe imaju mogućnost da regulišu *web* sadržaj dopuštanjem ili blokiranjem određenih sadržaja. Zbog velikog broja sajtova dostupnih danas, ranija rešenja zasnovana na *URL (Uniform Resource Locator)* filtriranju postala su krajnje neefikasna. *BkS* provajderi dopunjuju *URL* filtriranje ispitivanjem *HTTP* zaglavlja informacija, sadržaja stranica i ugrađenih veza *(embedded links)* radi boljeg razumevanja *web* sadržaja.

Filtriranje *web* sadržaja uključuje i pretraživanje odlaznog saobraćaja radi otkrivanja osetljivih informacija, kao što su informacije o kreditnim karticama ili intelektualnoj svojini, koje korisnici mogu da pošalju bez odgovarajuće autorizacije (zaštita od curenja podataka) (Mather et al, 2009). Slika 4 ilustruje filtriranje *web* sadržaja.



Slika 4 – Filtriranje web sadržaja u BkS modelu (Mather et al, 2009)
Figure 4 – Filtering of the web content in the BkS model (Mather et al, 2009)

Upravljanje ranjivošću sistema

Sa porastom kompleksnosti organizacije i njihovim povećanim prisustvom na internetu, osiguravanje bezbednih konfiguracija i funkcionisanja sistema koje obuhvataju, postalo je teže i značajnije. Postoje *BkS* provajderi koji otkrivaju, određuju prioritet i procenjuju ranjivost sistema, a potom izveštavaju o tim ranjivostima, uklanjaju ih i vrše sigurnosnu proveru sistema.

Današnja ponuda Bezbednosti-kao-Servisa ne samo da je održiva, već je u velikoj meri razvijena. Usluge filtriranja *e-mail*-ova i *web* sadržaja postoje već nekoliko godina i metode za pružanje tih usluga su razvijene, a i novije usluge se unapređuju. Ipak, nijedan *cloud* servis provajder još uvek nije uvrstio Bezbednost-kao-Servis u ponudu svojih usluga; provajderi ga još uvek isporučuju putem oblaka specijalizovanih samo za pružanje bezbednosti.

Verovatno je da će u budućnosti doći do značajnog rasta Bezbednosti-kao-Servisa iz dva razloga. Prvo, trend izmeštanja informacione bezbednosti će se najverovatnije nastaviti. Ono što je počelo sa filtriranjem *e-mail*-ova i upravljanjem bezbednosnim servisima će se proširiti, jer će organizacije nastaviti da traže načine smanjenja kapitalnih troškova i sve će se više koncentrisati na svoju osnovnu delatnost. Drugo, postoje i drugi bezbednosni zahtevi, čije će se potrebe i složenost razvijati sa usvajanjem koncepta *cloud computing*-a. Ta dodatna složenost će u još većoj meri podsticati razvoj Bezbednosti-kao-Servisa.

Konkretno, te dodatne bezbednosne zahteve predstavljaju dva proaktivna i dva reaktivna načina zaštite. Proaktivni načini zaštite bitni za razvoj CC su upravljanje identitetom i upravljanje ključevima (prilikom kriptovanja). Za *cloud computing* je potreban značajni napredak na oba ova polja, što će potencijalna rešenja učiniti veoma dragocenim. Reaktivni načini zaštite bili bi skalabilni i efektivni sistem za upravljanje sigurnosnim incidentima i događajima *(Security Incident and Event Management, SIEM)* i prevencija odliva podataka *(Data Loss Prevention, DLP)*. Realizacija ovih rešenja će biti teška i zahtevaće složenost koja će morati da bude skalabilna a ipak jednostavna za upotrebu. S druge strane, sve ove potrebe predstavljaju značajne mogućnosti za proizvođače, kao i za usvajanje i razvoj CC (Urošević, 2011).

Zaključak

Treba imati na umu da *cloud computing* menja postojeće modele poslovanja. Posmatrano iz perspektive informacione bezbednosti, najveća promena koju donosi CC je prikupljanje zajedničkih resursa više korisnika na centralizovanoj lokaciji. Ta promena za posledicu ima pomeranje granica poverenja; gde se tačno te granice nalaze još uvek nije jasno. Granice poverenja su različite za svaki od *SPI* modela (Softver-kao-Servis, Platforma-kao-Servis i Infrastruktura-kao-Servis); pa čak i u okviru svakog od tih modela granice se razlikuju u zavisnosti od *cloud* servis provajdera.

Nivo bezbednosti koji pruža *cloud* servis provajder zavisi i od perspektive iz koje se posmatra. Na primer, profesionalcima IT sektora jedne velike i razvijene organizacije nivo bezbednosti u CC može biti neprihvatljiv u poređenju sa trenutnim položajem. S druge strane, nivo bezbednosti koji pruža *cloud computing* maloj ili srednjoj organizaciji ili njenom delu može biti prihvatljiv, pa čak i veći u odnosu na trenutno stanje.

Za dalji razvoj CC potreban je veći uvid u rad *cloud* servis provajdera, odnosno transparentnost u vezi načina na koji se brinu o bezbednosti. Ipak, to samo po sebi nije dovoljno za povećanje nivoa bezbednosti; potrebna su i značajna poboljšanja tehnologije bezbednosti u vidu proaktivne i reaktivne zaštite.

Moguće vojne primene CC bile bi u vojnim vežbama, mirovnim misijama, upravljanju na daljinu, kao i oblasti regrutacije kadeta.

Što se tiče nadgledanja bezbednosti, tehnologije sistema za upravljanje sigurnosnim incidentima i događajima su jedva u stanju da zadovolje današnje potrebe velikih organizacija. Naprosto nije realno očekivati da će postojeća rešenja biti u stanju da zadovolje potrebe oblaka. Korisnici već sada zahtevaju prenosivost, a uskoro će zahtevati upotrebu više oblaka istovremeno. Ta potražnja za simultanim korišćenjem većeg broja oblaka će u potpunosti promeniti današnji pristup nadgledanju bezbednosti.

Sa porastom količine podataka uskladištenih u javnim oblacima, korisnici će zahtevati veće angažovanje *cloud* servis provajdera u cilju zaštite tih poda-

taka. Velike organizacije će ulagati sopstvene napore u osiguravanje prevencije odliva podataka i zahtevaće to isto od *cloud* servis provajdera. Doći će do obimnijih transfera podataka i povećanja obima kriptovanog saobraćaja; veliko je pitanje da li će se današnja rešenja pokazati delotvornim u CC okruženju.

Nedostaci postojeće tehnologije informacione bezbednosti ukazuju na verovatnoću da će veliki broj korisnika biti nezadovoljan naporima koje *cloud* servis provajderi ulažu u osiguravanje bezbednosti, ali istovremeno označavaju priliku za razvoj novih tehnologija i rešenja.

Cloud computing predstavlja novi model, još uvek uglavnom nepoznat i mali broj korisnika ga razume u dovoljnoj meri za donošenje odgovarajuće procene. Realna pitanja bezbednosti postoje, bez ikakve sumnje. Ipak, bolje razumevanje, veća transparentnost i poboljšanje tehnologija dovešće do toga da brige oko bezbednosti u CC izblede i postanu deo prošlosti.

Literatura

Benoit, April 2009, *Trends for 2008*, Symantec's Global Internet Security Threat Report*,* Vol. XIV, p.10.

Caceres, J., Vaquero, L., Polo, A., 2010, Service Scalability over the Cloud', *Handbook of Cloud Computing*, Springer, USA, pp. 357–377.

Carlin, S., Curran, K., January-March 2011, Cloud Computing Security, *International Journal of Ambient Computing and Intelligence*, UK, pp.14–19.

Cayirci, E. et al., 2009, Snow leopard cloud: a multi-national education training and experimentation cloud and its security challenges, *Cloud Computing*, pp. 57–68.

CloudAV: N-Version Antivirus in the Network Cloud, USENIX Conference, San Jose, California, July 2008.

Choo, K. K.R., 2010, Cloud computing: Challenges and future directions, *Trends&issues in crime and criminal justice*, No.400, Australian Institute of Criminology, Australia, pp.1–6.

Đekić, M., Za bolje iskorišćenje, *Svet kompjutera*, dostupno na:
http://www.sk.rs/2008/04/skse01.html.

Mather, T., Kumaraswamy, S., Latif, S., 2009, *Cloud Security and Privacy*, *First edition*, O'Reilly, USA.

Nick, J., Cohen, D., Kaliski, B., 2010, Key enabling Technologies for Virtual Private Clouds, *Handbook of Cloud Computing*, Springer, USA, pp. 47–63.

Sangroya, A., 2010, Towards Analyzing Data Security Risks in Cloud Computing Environments, pp. 255–265, *ICISTM 2010*, Germany.

Urošević, V., 2011, Visokotehnološki kriminal u cloud computing okruženju – rizici i pretnje, str. 8–13, *Konferencija o bezbednosti informacija BISEC 2011*, Beograd, Srbija, juni 2011.

Vecchiola, C., Xingchen C., Rajkumar, B., 2009, Aneka: a software platform for. NET-based cloud computing, *High Speed and Large Scale Scientific Computing*, pp. 267–295.

Wyld, D., 2009, *Moving to the cloud: an introduction to cloud computing in government*, IBM Center for the business of government.

http://googleblog.blogspot.com/2007/09/weve-officially-acquired-postini.html, preuzeto: 14. 09. 2012.

SECURITY ISSUES OF CLOUD COMPUTING ENVIRONMENT IN POSSIBLE MILITARY APPLICATIONS

FIELD: Computer Sciences, Telecommunications, Information Technology
ARTICLE TYPE: Professional Paper

Summary:

The evolution of cloud computing over the past few years is potentially one of major advances in the history of computing and telecommunications. Although there are many benefits of adopting cloud computing, there are also some significant barriers to adoption, security issues being the most important of them. This paper introduces the concept of cloud computing; looks at relevant technologies in cloud computing; takes into account cloud deployment models and some military applications. Additionally, Security-as-a-Service is specially considered because of its importance in the military applications.

Cloud computing (CC) is such a combination of computer hardware, software, online services and expertise networked by high-speed Internet connections. What is more, cloud computing is a model of using computing resources (servers, disks, operating systems and applications) where these resources are rented and not bought. The consequence of this approach is that users pay only as many resources as they actually have used (pay-as-you-go), so they do not need to take care about either hardware procurement and its installation, or software (operating system and applications) maintenance.

Most of the cloud computing architecture used nowadays includes public cloud computing networks for providing services through the Internet, such as Google Search, Microsoft Hotmail or Google Adsense. Large service providers, together with typical pioneers in adopting new technologies such as financial services and pharmaceutical companies, also apply the architecture of CC in the implementation of private cloud networks protected by firewalls. This mode of use is still in its early stages and is expected to achieve further growth in the corporate database virtualization technologies that are now being introduced.

The framework used to describe cloud computing services is known as the acronym SPI (Software Platform Infrastructure) and marks the three major services provided through the clouds: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). Traditional methods of purchasing software involve software upgrading onto hardware with paying license fees (which is capital expenditure). The user is also able to enter into any contract for maintenance and to get security patches and other services for software support at a certain price. The compatibility of operating systems and the installation of patches is the responsibility of the user.

Being a simplified representation of complex, interconnected devices and connections that form the Internet, the term 'cloud' is a metap-

hor for the Internet. Public and private (external and internal) clouds are the parts of the Internet and are defined (or, rather, they differ) based on the connections formed by institutions.

Similar to SaaS, the Security-as-a-Service cloud service model is delivered to customers on a subscription basis. In addition, SaaS is also applied in the Security-as-a-Service. There are three incentives for the development of Security-as-a-Service. The earliest driver is spam which is now more than a decade old. Another driver for the development of Security-as-a-Service is a service for managing safety (MSS, Managed Security Services). The impetus for the use of MSS was (and still is) the same as for the use of CC: reduced cost compared to home solutions due to the use of shared resources. Also, the MSS model breaks the informal but powerful barrier of displacement (outsourcing) of the parts of the information security program of an institution. In this case, displacement implies control devices outside the institution (off-premises). It should be noted that, although outsourcing IT security is often an option, initially it can only be used in the relocation of the facility (outsourcing on-premises), ie. to be moved into another room within the same building, as opposed to the relocation outside the building.

It should be taken into account that cloud computing changes the existing business models. From the perspective of information security, the biggest change brought by cloud computing is collecting shared resources of multiple users at a centralized location. This change results in a shift of confidence limits; exactly where these limits are is not clear yet. Confidence limits are different for each model of SPI (Software-as-a-Service, Platform-as-a-Service and Infrastructure-as-a-Service), even when limits vary within each of these models depending on the cloud service provider.

Keywords: *clouds, computing, evolution, telecommunications.*

Datum prijema članka/Paper received on: 19. 09. 2012.
Datum dostavljanja ispravki rukopisa/
Manuscript corrections submitted on: 05. 12. 2012.
Datum konačnog prihvatanja članka za objavljivanje/ Paper accepted for publishing on: 08. 12. 2012.