



# CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA  
CROATIAN ACADEMIC AND RESEARCH NETWORK



## Cloud computing

NCERT-PUBDOC-2010-03-293

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

## **Nacionalni CERT**, [www.cert.hr](http://www.cert.hr)

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

## **LS&S**, [www.LSS.hr](http://www.LSS.hr)

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument je vlasništvo Nacionalnog CERT-a. Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u izvornom obliku, bez ikakvih izmjena, uz obavezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet-a, sukladno Zakonu o autorskim pravima. Počinitelj takve aktivnosti podliježe kaznenoj odgovornosti koja je regulirana Kaznenim zakonom RH.

## Sadržaj

<b>1. UVOD .....</b>	<b>4</b>
<b>2. CLOUD COMPUTING .....</b>	<b>6</b>
2.1. VIRTUALNI STROJEVI KAO STANDARDNI RAZVOJNI OBJEKT .....	8
2.2. PROGRAMIBILNOST INFRASTRUKTURE .....	8
2.3. OD ČEGA SE SASTOJI CLOUD COMPUTING? .....	9
2.3.1. Ključne karakteristike cloud computinga .....	9
2.3.2. Modeli pružanja usluge .....	11
2.3.3. Modeli izvedbe .....	12
2.4. EKONOMSKI ASPEKT .....	14
2.5. ARHITEKTURE U OBLAKU .....	14
2.6. SIGURNOSNI PROBLEMI I RIZICI .....	16
2.7. OBLACI „PROTIV“ OBLAKA .....	17
2.7.1. Amazon Elastic Compute Cloud .....	18
2.7.2. Google App Engine .....	19
2.7.3. GoGrid .....	19
2.7.4. AppNexus .....	19
2.7.5. Uvjeti i ugovori .....	20
<b>3. CLOUD SECURITY ALLIANCE .....</b>	<b>21</b>
3.1. POVIJEST ORGANIZACIJE .....	21
3.2. ŠTO, KADA I KAKO SPREMITI U OBLAK? .....	21
3.2.1. Identifikacija sredstava koja korisnik želi pohraniti u oblaku .....	22
3.2.2. Procjena važnosti sredstava .....	22
3.2.3. Odabir modela .....	22
3.2.4. Ocjenjivanje rizika .....	22
3.2.5. Skiciranje potencijalnog protoka podataka .....	22
3.3. GLAVNE PRIJETNJE SIGURNOSTI CLOUD COMPUTINGA .....	22
3.3.1. Zloupotreba cloud computinga .....	22
3.3.2. Nesigurna sučelja i API .....	23
3.3.3. Zlonamjerni korisnici koji napade izvode iznutra .....	23
3.3.4. Zajednički tehnološki problemi .....	24
3.3.5. Gubitak i neovlašteno otkrivanje podataka .....	24
3.3.6. Krađa korisničkih imena .....	25
3.3.7. Nepoznati profil rizika .....	25
<b>4. PROŠLOST, SADAŠNJOST I BUDUĆNOST .....</b>	<b>26</b>
<b>5. ZAKLJUČAK .....</b>	<b>27</b>
<b>6. REFERENCE .....</b>	<b>28</b>

## 1. Uvod

Razvojem informacijskih tehnologija na tržištu se neprekidno javlja potreba za inovacijama i unaprjeđenjem trenutnog stanja informacijskih sustava. Upravo ta težnja za inovacijama dovela je do nastanka *cloud computinga*. *Cloud computing* je nastao kao želja IT stručnjaka za povećanjem kapaciteta i dodavanjem novih mogućnosti na vlastite sustave bez investiranja u novu infrastrukturu i potrebe za osposobljavanjem novog osoblja i/ili kupnje novih licenciranih programa. Unatoč stvarno velikim kapacitetima koje nudi korisnicima, njegovi resursi ipak nisu beskonačni. *Cloud computing* obuhvaća svaku uslugu koja se temelji na ugovoru ili plaćanju po potrebi. Usluga pri tome mora biti obavljena u realnom vremenu. Pojava *cloud computinga* povećava mogućnosti IT-a. Njegovom pojavom povećavaju se dosadašnje mogućnosti IT-a (eng. *Information technology*), odnosno mogućnosti uporabe računala i programa. Napretkom računalnih i telekomunikacijskih tehnologija poboljšane su mogućnosti prijenosa, pohrane, zaštite, obrade i sigurnosti podataka. Analitičari te stručnjaci koji se bave sigurnošću i *cloud computingom* imaju i dalje različite načine shvaćanja i definiranja *njegovog definiranja*.

- Neki ga definiraju kao mogućnost iznajmljivanja jednog ili više poslužitelja te pokretanja različitih aplikacija na njima.
- Može se definirati i kao mogućnost iznajmljivanja virtualnog poslužitelja. Korisnici na virtualnom poslužitelju mogu pohranjivati podatke i po volji im pristupati.
- *Cloud computing* se može definirati i kao pohranjivanje i osiguravanje ogromnih količina podataka kojima mogu pristupiti samo ovlaštene aplikacije ili korisnici.
- *Cloud computing* može biti i mogućnost korištenja aplikacije koja se nalazi na Internetu i pohranjuje te štiti podatke za vrijeme pružanja usluge.
- On može koristiti virtualne poslužitelje za pohranu podataka kako bi se na njima čuvale aplikacije, poslovni i osobni podaci.
- Može se smatrati i kao mogućnost korištenja mnoštva *web* aplikacija kako bi se uz pomoć njih mogle integrirati fotografije, karte, GPS informacije i druge korisne stvari.

*Cloud computing* se može definirati i s obzirom na to koriste li ga stručnjaci ili obični korisnici. Obični korisnici će *cloud computing* definirati kao novi i jeftiniji način korištenja programskih rješenja koja će se unajmljivati prema potrebi. Informatički stručnjaci definirati će ga kao novi poslovni model ili novu tehnološku platformu za smještaj, pokretanje i korištenje informatičke programske podrške. Korištenjem *cloud computinga*, razvojni inženjeri i programeri se mogu koncentrirati na primjenu poslovne logike, umjesto na kupovanje novog sklopovlja za izvođenje i podršku rada aplikacija. Sistemskim inženjerima on smanjuje opseg posla pri održavanju platformi za izvođenje aplikacija. Postoje različiti oblici *cloud computinga* i različite aplikacije koje se mogu na njima izgraditi. *Cloud computing* povećava brzinu razvijanja aplikacija, pomažući tako u povećavanju broja inovacija koje se pojavljuju na tržištu. Kako je *cloud computing* poprilično nova stvar na IT tržištu, on još nije savršen. Postoje mnoge prednosti koje bi korisnike trebale privući korištenju *cloud computinga*, ali isto tako i problemi koje im korištenje može donijeti. Prije nego što se pojedini korisnik ili organizacija odluče na korištenje ove tehnološke platforme trebali bi se dobro informirati o mogućim nedostacima koje im ova tehnologija može donijeti. Korisnici bi prvo trebali proučiti koji se sve davatelji usluga mogu pronaći na tržištu i koje su njihove međusobne razlike. Zatim bi trebali odrediti koje podatke žele spremati, koliko su ti podatci osjetljivi, koje *cloud computing* usluge ili platforme im najbolje odgovaraju, koliko prostora je potrebno i slično. Uvođenje ove tehnologije sigurno nije jednostavna stvar za organizacije. Svaka organizacija prvo bi trebala procijeniti kolike će im financijske uštede donijeti korištenje ovog modela i kako će se one odraziti na sigurnost i konkurentnost organizacije. *Cloud computing* je još uvijek u razvoju i svakim danom se uvode nove promjene, pojavljuju novi poslužitelji, ali isto tako sve više korisnika pristupa ovome konceptu podjele programske podrške koji koristi Internet kao platformu te omogućuje pohranjivanje i čuvanje aplikacija. Aplikacije ili dokumenti mogu biti poslani iz bilo kojeg dijela svijeta.

Neke od prednosti korištenja *cloud computinga* su:

- niža cijena sklopovske podrške u smislu da korisnik ne mora kupovati novo sklopovlje, nego ga po potrebi iznajmljuje preko Interneta,
- korisniku je uvijek dostupna posljednja, najnovija inačica programske podrške,
- programska podrška i podaci su dostupni sa svakog računala s kojeg korisnik ima pristup Internetu,
- manji troškovi održavanja i nadogradnje programske podrške. Nema troškova izravno vezanih uz kupovinu sučelja, licenciranih programa, baze podataka, poslužitelja za elektroničku poštu, kao ni troškova vezanih za njihovu instalaciju i konfiguraciju te kasnije održavanje,
- u uslugu je uključena profesionalna antivirusna zaštita,

- dostupnost aplikacija,
- skalabilnost aplikacija - mogućnost opsluživanja velikog broja korisnika,
- fleksibilnost u izmjeni i prilagodbi aplikacija i
- stalno praćenje rada i održavanje infrastrukture.

Neki nedostaci *cloud computinga* su:

- problem dostupnosti,
- problem sigurnosti,
- problem ovisnosti o jednom pružatelju programske podrške,
- usvajanje novog načina razvoja aplikacija,
- nemogućnost jednostavnog premještanja postojećih aplikacija te
- nepostojanje standarda za povezivanje aplikacija različitih proizvođača, razmjenu podataka, premještanje podataka te programske podrške iz „oblaka jednog proizvođača“ u „oblak drugog“.

Stručnjaci koji se bave sigurnošću i *cloud computingom* intenzivno rade na smanjivanju nedostataka koji su se do sada pojavili pa analitičari smatraju da će najveći problemi biti riješeni u skoroj budućnosti. To će zasigurno pridonijeti još većoj uporabi *cloud computinga*.

## 2. Cloud computing

*Cloud* (hrv. oblak) je vrlo često korištena metafora za Internet. Ona potječe od načina na koji se Internet označava u raznim dijagramima, ali i od same infrastrukture Interneta. Kada se ona koristi zajedno s izrazom *computing* novi termin više nema isto značenje. Postoji mnoštvo različitih definicija *cloud computinga*. Neki analitičari definiraju *cloud computing* kao virtualne poslužitelje dostupne preko Interneta. Drugi smatraju da je sve što se nalazi iza vatrozida gledano sa stajališta korisnika lokalne mreže u „oblaku“. Možda bi najbolja definicija bila da je *cloud computing* koncept podjele programskog okruženja koji koristi Internet kao platformu te omogućuje da aplikacije i dokumenti poslani iz bilo kojeg dijela svijeta budu pohranjeni i čuvaju se na za to predviđenim poslužiteljima. Ova vrsta računala koja se zasnivaju na korištenju *weba*, smanjuju potrebu za kupnjom novog sklopovlja i programa te otvaraju nove oblike suradnje. Pristup „podacima u oblaku“ odvija se putem *web* preglednika ili specijaliziranih aplikacija.



**Slika 1. Cloud computing**  
Izvor: LCS

Organizacije koje pružaju usluge *cloud computinga* korisnicima omogućuju pristupanje aplikacijama i virtualnim poslužiteljima preko *web* preglednika. Korištenjem *cloud computing* tehnologije korisnici više nemaju potrebu za poznavanjem ili ispitivanjem tehnološke strukture „oblaka“.

IT (eng. *Information Technology*) uvijek teži povećanju kapaciteta ili novih mogućnosti bez investiranja u nove infrastrukture, obuku novog osoblja ili kupovinu novih licenciranih programa. *Cloud computing* također obuhvaća svaku uslugu koja se naplaćuje preko Interneta i povećava postojeće IT kapacitete.

*Cloud computing* je još uvijek u neprekidnom razvoju. Na njegovom razvoju radi mnogo različitih davatelja usluga koji svoju ponudu zasnivaju na „računarstvu u oblaku“ (razne aplikacije, usluge skladištenja i filtriranja nepoželjnih sadržaja).

„Oblak“ odvaja aplikacijske i informacijske resurse od infrastrukture koja leži u pozadini. Oblak odvaja i mehanizme kojima se ti resursi dostavljaju. Također, „oblak“ povećava suradnju, pokretljivost, skaliranje i dostupnost računalnih sustava te donosi nove mogućnosti konstrukcije uz pomoć optimalnog i učinkovitog upravljanja. *Cloud computing* objašnjava način uporabe više poslužitelja, aplikacija, informacija i infrastrukture koja se sastoji od mnoštva računalnih, mrežnih, informacijskih resursa te resursa za pohranu podataka i programa kako bi se smanjili financijski izdatci korisnika i omogućilo brže i jeftinije rješavanje problema. Ove komponente mogu biti brzo obrađene, interpretirane, primijenjene i skalirane pružajući tako model raspodjele i uporabe koji funkcionira na zahtjev korisnika.



**Slika 2. Cloud computing**  
**Izvor: Nitesh Ambuj**

Na temelju mnogih istraživanja provedenih među analitičarima, proizvođačima i IT korisnicima ugrubo se može reći što je *cloud computing*:

- **SaaS** (eng. *Software as a Service*) - Oblik *cloud computinga* koji preko preglednika dostavlja jednu aplikaciju mnoštvu korisnika. Korištenjem ovog modela korisnici ne moraju investirati u nove poslužitelje i licencirane programe. Troškovi davatelja usluga su pri tome manji u odnosu na tradicionalnu uslugu čuvanja podataka na poslužitelju. Detaljniji opis SaaS usluge nalazi se u poglavlju o modelima pružanja usluga.
- **Uslužno računarstvo** (eng. *Utility computing*) - Uslužno računarstvo je relativno nova forma na tržištu informacijskih tehnologija. Koriste ju Amazon, Sun, IBM i drugi koji nude uslugu pohrane virtualnih poslužitelja kojima se pristupa na zahtjev korisnika. Pružatelj usluga osigurava računalne resurse i infrastrukturu korisniku prema potrebi. U budućnosti bi ovaj model mogao zamijeniti dio baza podataka jer korisnici uz pomoć *cloud computing* tehnologije mogu pohranjivati mnoštvo podataka na virtualnim poslužiteljima. Druge organizacije pružaju rješenja koja pomažu korisnicima u stvaranju virtualnih baza podataka.
- **Web usluge u oblaku** (eng. *Web services in the cloud*) - Web usluge su usko povezane sa SaaS modelom. Organizacije koje pružaju web usluge nude sučelja (eng. *application programming interface*) koja razvojnim inženjerima omogućuju iskorištavanje funkcionalnosti preko Interneta. Web usluge mogu imati veliki raspon, pa tako sežu od diskretnih poslovnih usluga (poput Strike Iron i Xignite), pa sve do jako dobro razvijenog sučelja, koje se može pronaći kod Google Mapsa, automatske obrade podataka nakon plaćanja te standardnih usluga obrade kreditnih kartica.
- **PaaS** (eng. *Platform as a service*) – PaaS je još jedna inačica SaaS modela. Ovaj model *cloud computinga* kao uslugu pruža razvojnu okolinu. Korisnik gradi vlastite aplikacije koje se pokreću na infrastrukturi davatelja usluge, te putem preglednika dostavljaju korisniku. Detaljniji opis nalazi se u poglavlju o modelima pružanja usluga.
- **MSP** (eng. *managed service providers*) – MSP je jedan od najstarijih oblika *cloud computinga*. Upravljana usluga je aplikacija namijenjena IT službi, a ne krajnjem korisniku. Primjer je usluga skeniranja zloćudnih programa koji se šire porukama elektroničke pošte ili usluge upravljanja aplikacijama (na primjer tu uslugu pruža Mercury).

[http://newsweaver.co.uk/mercury/e\\_article000347072.cfm?x=b11,0,w](http://newsweaver.co.uk/mercury/e_article000347072.cfm?x=b11,0,w)

U tu kategoriju se ubrajaju upravljani sigurnosni poslužitelji poput SecureWorksa, IBM-a i Verizona, kao i *cloud antispam* poslužitelji poput Postinia i Googlea. Druge ponude uključuju uslugu upravljanja radnom površinom. Takve usluge nude CenterBeam ili Everdream.

- **Usluge komercijalnih platformi** (eng. *Service commerce platforms*) - Ove su platforme hibrid SaaS i MSP modela. Usluga komercijalnih platformi nudi čvorište (eng. *hub*) s kojim korisnici komuniciraju. Najčešće se upotrebljava u web trgovinama, poput skupih upravljačkih sustava koji korisnicima



dozvoljavaju naručivanje mobilnih usluga zajedničkih platformi. Platforme tada koordiniraju pružanje usluga određivanjem cijene unutar specifikacija koje je postavio korisnik. Poznati primjeri davatelja ove usluge su Rearden Commerce i Ariba.

- **Integracija Interneta** (eng. *Internet integration*) - Danas je integracija *cloud computing* usluga i dalje u svojim ranim fazama. Način međusobnog povezivanja zasnovan na oblaku bi se možda trebao nazivati *sky computing* s mnoštvom izoliranih oblaka na koje se korisnici individualno moraju spajati. S druge strane kako sve više organizacija primjenjuje virtualizaciju i SOA arhitekturu (eng. *service-oriented architecture*), povećava se potreba za dobro povezanim uslugama koje se nalaze na Internetu. Ideja podesive infrastrukture ja da se jednog dana svakoj organizaciji napravi čvor u oblaku.

## 2.1. Virtualni strojevi kao standardni razvojni objekt

Posljednjih nekoliko godina virtualni strojevi postali su standardni razvojni objekt. Virtualizacija povećava prilagodljivost jer sklopovlje čini apstraktnim do točke da se programi mogu više puta raspoređivati bez izravne vezanosti za specifični fizički poslužitelj. Virtualizacija omogućuje postojanje dinamičkih baza podataka, gdje fizički poslužitelji osiguravaju mnoštvo resursa koji se po potrebi dohvaćaju. Odnos aplikacija za računanje, pohranu i mrežne resurse se dinamički mijenja kako bi se dostiglo zahtijevano radno opterećenje i djelotvornost. Implementacija aplikacija je odvojena od implementacije poslužitelja, pa se aplikacije mogu brzo raspoređivati i skalirati, bez potrebe za fizičkim poslužiteljima.

Virtualni strojevi postali su prevladavajuća apstrakcija i jedinica razvoja, jer su oni najmanje zajedničko sučelje koje odjeljuje davatelje usluga i razvojne organizacije. Korištenjem virtualnih strojeva kao razvojnih objekata zadovoljava se 80% korisničkih potreba, a i pomaže u zadovoljavanju potreba za brzim pregrupiranjem i skaliranjem aplikacija.

Oblaci za računanje su najčešće fizički povezani s oblacima za pohranu podataka. Oblaci za pohranu podataka pružaju virtualnu pohranu preko API-a koja olakšava virtualnim strojevima pohranu slika, datoteka ili komponenti poput *web* poslužitelja, aplikacijskih i poslovnih podataka.

Virtualne aplikacije i strojevi sadrže programe koji su u potpunosti ili djelomično programirani tako da izvode specifične zadatke. Oni mogu biti *web* poslužitelji ili poslužitelji baza podataka. Virtualni strojevi i aplikacije poboljšavaju sposobnosti brzog stvaranja i razvijanja aplikacija. Ključ daljnjeg razvoja *cloud computinga* je kombinirano korištenje virtualnih strojeva i aplikacija.

## 2.2. Programibilnost infrastrukture

Pomaci arhitekturalne odgovornosti imaju ozbiljne posljedice kod izgradnje poslužitelja i smještanja aplikacija. To bi moglo dovesti do smanjivanja kvalitete usluga, smanjene produktivnosti i preuzimanja odgovornosti za loše obavljen posao. U prošlosti su arhitekti određivali kako će različite komponente aplikacije biti raspoređene na skup poslužitelja, kako će biti povezane, osigurane, odabrane te kako će se njima upravljati. Danas, razvojni inženjeri mogu koristiti sučelja davatelja usluga ne samo da bi stvorili osnovnu kompoziciju na virtualnim strojevima, nego i kako bi odredili kako će se ona raspoređivati i razvijati da bi se prilagodila promjenama posla.

Povijesno su razvojni inženjeri koji su pisali programe koristeći programski jezik Javu određivali kada je prikladno izvođenje višestruke aktivnosti korištenjem paralelnog pristupa. Danas, razvojni inženjeri mogu pristupiti i razviti usluge s istim ciljem, dopuštajući im grananje aplikacije do te točke da se može uključiti tisuće virtualnih strojeva kako bi se mogli izvoditi neočekivano veliki zahtjevi.

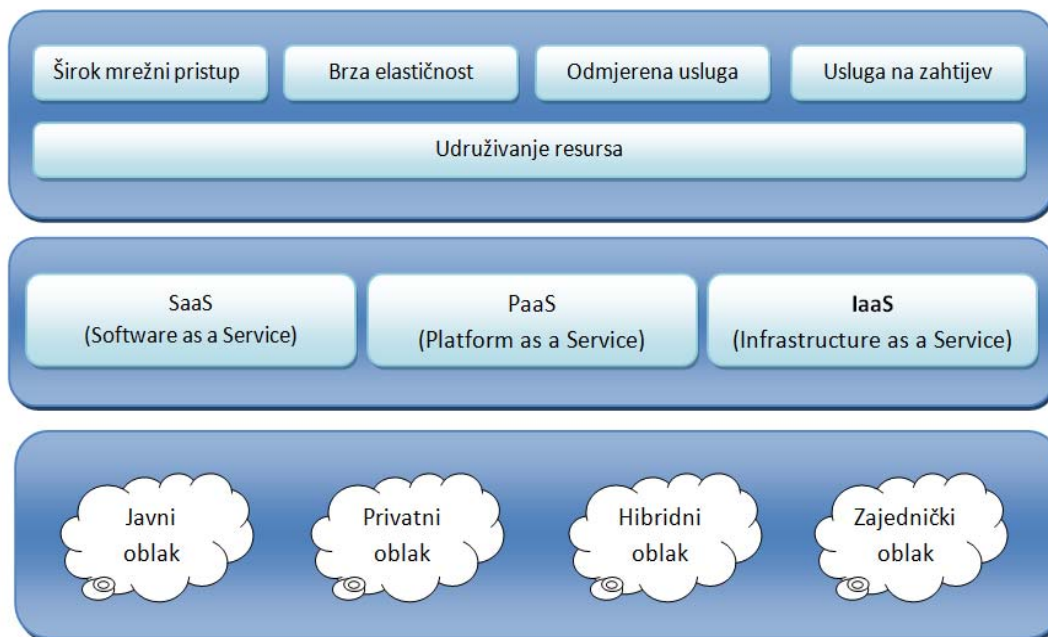
Mogućnost dinamičkog programiranja arhitekture aplikacije daje razvojnim inženjerima velike mogućnosti razvoja s proporcionalnim iznosom odgovornosti. Da bi se *cloud computing* što učinkovitije koristio, razvojni inženjeri moraju biti i arhitekti, a ti arhitekti moraju biti u mogućnosti razviti aplikacije s autokontrolom i mogućnošću automatskog širenja. Tako na primjer razvojni inženjer/arhitekt mora razumjeti kada je prikladno stvoriti dretvu, a kada novi virtualni stroj, zajedno s arhitektonskim nacrtima načina njihovog povezivanja.

Kada korisnici dobro razumiju navedene mogućnosti i iskoriste ih, rezultati mogu biti spektakularni. Primjer dobre uporabe je Animatev alat koji stvara video od skupa fotografija i glazbe. Aplikacija te organizacije se proširila s 50 do 3500 poslužitelja u samo tri dana zahvaljujući dijelu arhitekture koji dozvoljava lako dijeljenje. Da bi mogla raditi, aplikacija je morala imati izgrađen horizontalan pristup, tj. zauzimati ograničene dijelove poslužitelja i osiguravati si preko API-a vlastiti razmještaj.



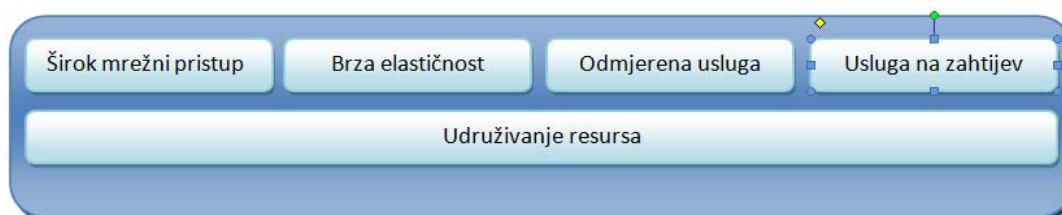
## 2.3. Od čega se sastoji Cloud computing?

Američka vladina organizacija koja se bavi standardima i tehnologijom - NIST (eng. *National Institute of Standards and Technology*) se među inim djelatnostima bavi i *cloud computingom*. Točnije, NIST se bavi valjanim definiranjem *cloud computinga* i podjelom na karakteristične modele. *Cloud* model promovira dostupnost i sastoji se od pet ključnih karakteristika, tri modela pružanja usluga te četiri modela implementacije koje su navedene na slici 3.



**Slika 3. Ključne karakteristike, modeli pružanja usluga, modeli implementacije**

### 2.3.1. Ključne karakteristike cloud computinga



**Slika 4. Ključne karakteristike cloud computinga**

Postoji pet ključnih karakteristika koje pokazuju odnos i razlike cloud computing sustava u odnosu na tradicionalni pristup u računarstvu. Tih pet ključnih karakteristika su:

- **Pružanje usluge na zahtjev korisnika** (eng. *On-demand self-service*) - Korisnik može samostalno odabrati i pokrenuti računalne resurse. Može birati vrijeme posluživanja i mrežni prostor za pohranu podataka bez potrebe za interakcijom s djelatnicima pojedinog davatelja usluge. U principu, danas većina poslužitelja svoje usluge temelji upravo na pristupu da korisnici plaćaju usluge u ovisnosti o vremenu i obujmu u kojem ih koriste.

Ovaj model *cloud computinga* pomaže u održavanju izvedbenih i kapacitivnih aspekata objekata koji ovise o razini usluge. *Self-service* priroda *cloud computinga* organizacijama omogućuje stvaranje elastične okoline koja se povećava i smanjuje ovisno o radnim uvjetima i ciljanim performansama. „Plati po korištenju“ priroda *cloud computinga* se može smatrati kao najam opreme koja se plaća ovisno o tome koliko je opreme, na koje vrijeme i s kojim uslugama iznajmljeno.

Virtualizacija je ključ ovoga modela. Organizacije koje koriste informacijske tehnologije shvaćaju da im virtualizacija omogućava brzo i jednostavno stvaranje kopija postojećih

okolina, ponekad uključujući više virtualnih strojeva kako bi podržala ispitivanja, razvoj i pohrana aktivnosti. Trošak ovih okolina je jako malen jer one mogu postojati na istom poslužitelju kao proizvodna okolina.

Isto tako, nove aplikacije se mogu razvijati i rasprostirati u novim virtualnim strojevima na postojećim fizičkim poslužiteljima, otvorenima za uporabu preko Interneta. Aplikacije mogu biti skalirane, ako su uspješne na tržištu.

Mogućnost korištenja i plaćanja samo onih resursa koji su korišteni prebacuje rizik koliko infrastrukture zauzeti od organizacije koja razvija aplikaciju na davatelja usluga *cloud computinga*. Također pomiče i odgovornost za arhitekturne odluke s arhitekata aplikacije na razvojne inženjere. Ovi pomaci odgovornosti mogu povećati rizike.

- **Širok mrežni pristup** (eng. *Broad network access*) - Mogućnosti su dostupne putem mreže i njima se pristupa koristeći standardne mehanizme koji promoviraju heterogenu uporabu „tankih“ i/ili „bogatijih“ klijentskih platformi (na primjer, mobilni uređaji, laptopi te PDA uređaji) kao i tradicionalnih programskih usluga temeljenih na „oblaku“. Ovo je vrlo blisko Microsoftovoj P+U/program+usluga (eng. S+S / softwafe+service) strategiji (ideja je da se bilo koji uređaj može spojiti na sustav od bilo kuda).
- **Udruživanje resursa** (eng. *Resource pooling*) - Računalni resursi pružatelja usluga spajaju se kako bi poslužili sve korisnike koristeći model više zakupljenih jedinica (eng. *Multi-Tenant model*), s različitim fizičkim i virtualnim resursima, koji se dinamički dodjeljuju i uklanjaju prema zahtjevima korisnika. Korisnik uobičajeno nema nadzor i znanje o točnom mjestu uporabljenih resursa, ali ipak ga može odrediti na većoj razini apstrakcije (na primjer na razini države). Primjeri resursa uključuju mrežni prostor, procesore, memoriju, mrežnu propusnost te virtualne strojeve.
- **Brza elastičnost** (eng. *Rapid elasticity*) - Mogućnosti koje korisnicima nudi *cloud computing* mogu biti ubrzano i elastično pokrenute, u nekim slučajevima i automatski, kako bi se po potrebi ostvarilo proporcionalno povećanje ili smanjenje mogućnosti kada one više nisu potrebne. Krajnjem korisniku mogućnosti koje koristi mogu izgledati kao da nemaju ograničenja i mogu se kupiti u bilo kojoj količini u bilo koje vrijeme (na primjer Amazon EC2).
- **Odmjerena usluga** (eng. *Measured service*) - Sustavi koji koriste *cloud computing* automatski provjeravaju i optimiraju uporabu resursa. Uporaba resursa se optimira utjecajem na mjerenje sposobnosti apstrakcije prikladne potrebnom tipu usluge (na primjer pohrana podataka, širina pojasa, aktivni korisnički račun). Uporaba resursa se može pratiti, provjeravati i o njoj se mogu raditi izvješća pružajući tako transparentan uvid davateljima usluge i korisnicima. Važno je primijetiti da se *cloud computing* poslužitelji često (ali ne uvijek) koriste zajedno s virtualizacijskim tehnologijama. Međutim, ne postoje zahtjevi koji usko povezuju apstrakciju sredstava i virtualizacijske tehnologije pa se u mnogim ponudama virtualizacija operacijskih sustava ipak ne koristi.

### 2.3.2. Modeli pružanja usluge



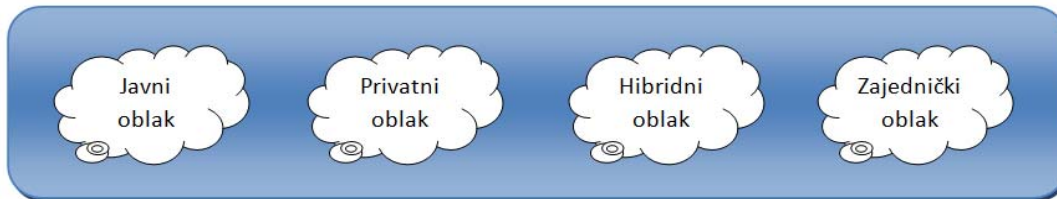
**Slika 5. Modeli pružanja usluge**

Isporuka *cloud computing* usluge podijeljena je na tri arhitekturna modela i različite izvedene kombinacije. Tri osnovne klasifikacije često se nazivaju SPI model, pri čemu SPI označava program, platformu ili infrastrukturu (eng. *Software, Platform, Infrastructure*). Mogući modeli pružanja usluge su:

- **SaaS** (eng. *Cloud Software as a Service*) - Korisniku je pružena mogućnost uporabe dostupnih aplikacija koje se nalaze u infrastrukturi oblaka. Aplikacije su dostupne s različitih klijentskih uređaja uz pomoć klijentskog sučelja (na primjer *web* preglednika). Pri tome korisnik ne provjerava pozadinsku infrastrukturu, uključujući mrežu, servise, operacijske sustave, pohranu podataka ili čak individualne aplikacijske mogućnosti. Jedina moguća iznimka su specifične korisničke konfiguracijske postavke. Odnosno, SaaS je tehnološka platforma koja omogućuje dostupnost aplikacija putem Interneta u obliku usluga koje se unajmljuju prema potrebi, umjesto da se kupuju kao zasebni program koji treba instalirati na kućnim (odnosno uredskim) računalima. Ubrzan je trend prijelaza na taj poslovni model, koji tvrtkama omogućuje najam tekstualnih, tabličnih, kalendarskih ili drugih programa prema potrebi, čime se izbjegava trošak kupovine, instalacije, nadgradnje i održavanja programa na uredskim računalima. Ovaj model *cloud computinga* dostavlja jednu aplikaciju preko korisničkog preglednika tisućama korisnika koji koriste arhitekturu predviđenu za mnoštvo zakupa. S korisničke strane to znači da nema dodatnog ulaganja u poslužitelje ili programske licence, a davateljima usluga troškovi su mali u odnosu na tradicionalnu uslugu držanja datoteka na poslužitelju. Primjeri SaaS-a su Google Apps i Zoho Office.
- **PaaS** (eng. *Cloud Platform as a Service*) – varijacija SaaS strukture koja kao uslugu donosi razvojnu okolinu. Korisnik sam gradi vlastite aplikacije koje se pokreću na infrastrukturi davatelja usluge. Aplikacije se korisnicima dostavljaju preko sučelja poslužitelja dohvatljivog putem Interneta. Navedeni poslužitelji su u vlasništvu davatelja usluga. Ove usluge su ograničene dizajnom i mogućnostima isporučitelja tako da korisnik nema potpunu slobodu. Korisnik ne može provjeravati strukturu oblaka niti mrežu, sustave pohrane, operacijske sustave i poslužitelje, ali ipak ima nadzor nad razvijenim aplikacijama. Ponekada ima čak i mogućnost nadzora okolinske konfiguracije. Neki od primjera su Salesforce.com, Force.com, Coghead i Google App Engine.
- **IaaS** (eng. *Cloud Infrastructure as a Service*) – Korisniku je kao usluga pružena mogućnost korištenja računalne infrastrukture (uglavnom virtualne platforme). Korisnici ne kupuju poslužitelje, programe, prostore za pohranu podataka ili mrežnu opremu, već kupuju navedene resurse kao vanjsku uslugu. Korisniku je pružena mogućnost upravljanja obradom, pohranom, umrežavanjem i drugim osnovnim računalnim resursima. Korisnik može pokrenuti različite vrste programske podrške, od operacijskog sustava do aplikacija. Korisnik nema nadzor nad infrastrukturom oblaka, ali ima nadzor nad operacijskim sustavima, pohranom podataka i razvojem aplikacija. Korisnik može imati i ograničeni nadzor nad odabranim komponentama umrežavanja.

Neprekidne inovacije dovode do brzog razvoja različitih novih rješenja. Razvojem sučelja korisnici i davatelji usluga moći će uživati u različitim metodama interakcije s *cloud computing* uslugama, što će dovesti do porasta važnosti takozvane usluge konzultanata u *cloud computingu*. Konzultanti će za dobrobit korisnika sumirati eventualno nepouzdanu mogućnost i sučelja. Tako će se ubrzati dolazak do zajedničkih, otvorenih i standardiziranih načina rješavanja problema *cloud computinga*. Na temelju tih rezultata korisnici će biti u mogućnosti izabrati model koji najbolje odgovara njihovim specifičnim potrebama.

### 2.3.3. Modeli izvedbe



**Slika 6. Modeli izvedbe cloud computinga**

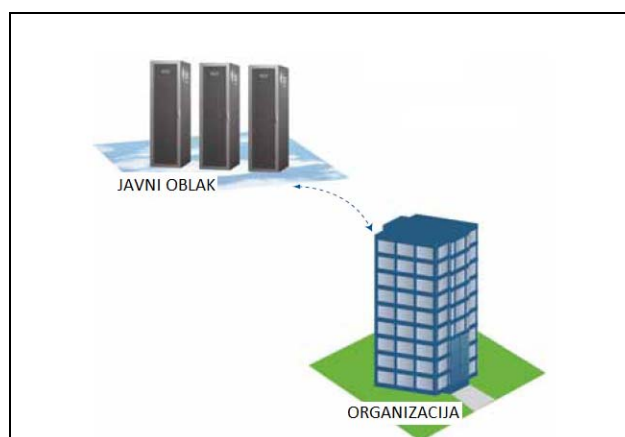
Neovisno o modelima pružanja usluga (SaaS, PaaS ili IaaS) postoje četiri različita modela provođenja *cloud computing* usluga. Ta četiri modela su izvedena na četiri različita načina, ovisno o specifičnim potrebama. Oblici su opisani u nastavku.

- **Javni oblak** (eng. *Public Cloud*) - *cloud computing* platforma dostupna i otvorena za javnost, neovisno o tome radi li se o pojedincima ili organizacijama. U vlasništvu je tvrtke koja prodaje *cloud computing* usluge. U slučaju javnih platformi postavlja se pitanje sigurnosti vlastitih podataka.

Aplikacije različitih korisnika često se nalaze na istim poslužiteljima, sustavima za pohranjivanje i mrežama. Javni oblaci smanjuju sigurnosne rizike i troškove pružanjem promjenjive infrastrukture. Oni čine privremeno zakupljenu infrastrukturu organizacija.

Ako je javni oblak realiziran s pažnjom usmjerenom na izvedbu, sigurnost i položaj podataka druge aplikacije pokrenute na oblaku ne bi trebalo stvarati probleme prema arhitekturi oblaka i krajnjim korisnicima. Jedna od prednosti javnih oblaka je da oni mogu biti puno veći nego što mogu biti privatni oblaci. Javni oblaci nude mogućnost povećavanja ili smanjivanja zakupljenog dijela oblaka i prebacivanje odgovornosti, ako se pojave neplanirani rizici, s organizacija na davatelja usluga.

Dijelovi javnog oblaka mogu biti i pod isključivom uporabom samo jednog korisnika, čineći tako privatni podatkovni centar (eng. *datacenter*). Zauzimanje tzv. slika virtualnih strojeva (eng. *virtual machine images*) u javnom oblaku ne daje korisnicima potpuni uvid u infrastrukturu oblaka, dok zakupljivanje podatkovnih centara daje korisnicima veći uvid u samu infrastrukturu. Tada korisnici mogu upravljati ne samo sa slikama virtualnih strojeva, nego i poslužiteljima, sustavima pohrane, mrežnim uređajima i mrežnim topologijama. Stvaranje privatnog virtualnog podatkovnog centra s komponentama koje se nalaze u istom objektu smanjuje problem postojanja mnoštva različitih lokacija podataka zato što je brzina prijenosa puno veća pri povezivanju objekata unutar istog oblaka.

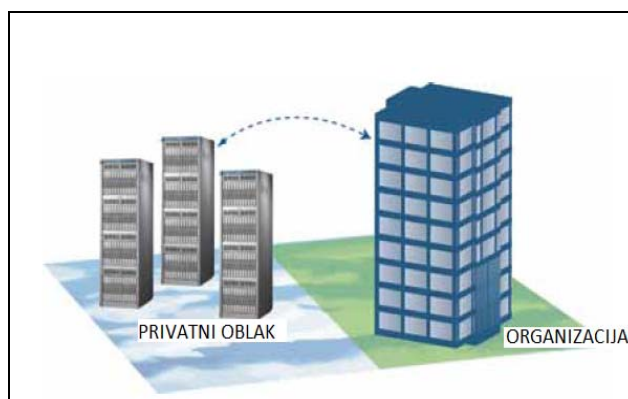


**Slika 7. Javni oblak**  
**Izvor: SUN**

- **Privatni oblak** (eng. *Private Cloud*) – *Cloud computing* infrastruktura dostupna je isključivo jednoj organizaciji. Njome može upravljati sama organizacija ili netko drugi. Organizacije koriste privatne oblake kada trebaju ili žele veći nadzor nad podacima nego što ga mogu imati korištenjem javnog oblaka.

Privatni oblaci su napravljeni isključivo za uporabu jednog klijenta, pružajući mu najveći nadzor nad podacima i najveću sigurnost imovine pohranjene na oblaku. Organizacija posjeduje infrastrukturu i ima nadzor nad raspodjelom aplikacija na vlastitoj infrastrukturi. Privatni oblaci mogu biti raspoređeni i unutar organizacijskog podatkovnog centra.

IT službe kompanija ili davatelji usluga grade privatne oblake i upravljaju njima. Organizacije koje posjeduju privatni oblak na njemu mogu instalirati programe, aplikacije, pohranjivati podatke i upravljati strukturom oblaka. Također, privatni oblaci pružaju kompanijama visoku razinu nadzora nad korištenjem resursa oblaka jer korištenjem privatnog oblaka organizacije imaju potrebne vještine i mogućnosti za uspostavljanje i upravljanje okolinom.



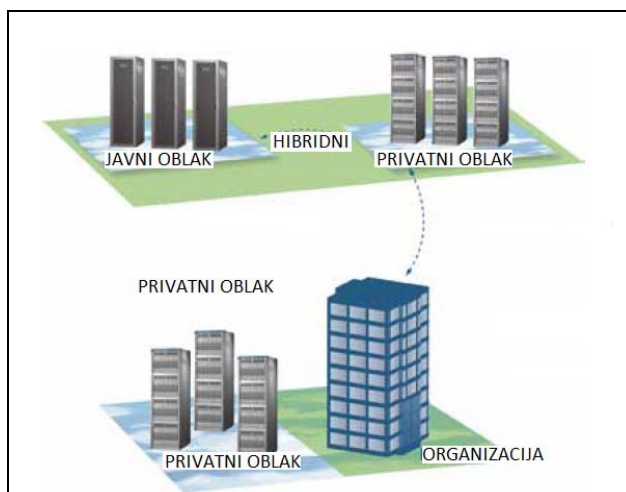
**Slika 8. Privatni oblak**  
Izvor: SUN

- **Zajednički oblak** (eng. *Community Cloud*) - Nekoliko organizacija dijeli strukturu oblaka. Infrastruktura podržava posebne zajednice koje imaju zajedničke potrebe, misije, zahtjeve sigurnosti i slično. Njima mogu upravljati same organizacije ili netko drugi (pružatelj usluga *cloud computinga*).
- **Hibridni oblak** (eng. *Hybrid Cloud*) Strukturu oblaka čine dva ili više različitih oblaka (privatni, zajednički ili javni) koji ostaju jedinstveni entiteti, ali su međusobno povezani standardiziranim ili prikladnim tehnologijama koje omogućavaju efikasan prijenos podataka ili aplikacija.

Hibridni oblaci povezuju javne i privatne modele oblaka. Mogućnost proširivanja privatnog oblaka s resursima javnog oblaka može se koristiti za održavanje uslužnih razina kako bi se lakše izdržala velika opterećenja. To se najčešće može vidjeti kod uporabe oblaka za pohranu podataka kako bi podržali *Web 2.0* aplikacije. Hibridni oblak se također može koristiti za upravljanje planiranim velikim opterećenjima. Privatni oblaci mogu se koristiti za izvođenje periodičkih zadataka koji se jednostavno raspoređuju na javne oblake.

Hibridni oblaci susreću se sa složenosti određivanja kako raspodijeliti aplikacije po javnom i privatnom oblaku. Pokraj ovog problema u obzir se mora uzeti i odnos između podataka i obrade resursa. Ako su podaci mali ili aplikacije ne pamte stanja, hibridni oblak može biti bolje rješenje od prepisivanja velike količine podataka u javni oblak (u kojem se izvodi jednostavna obrada).





**Slika 9. Hibridni oblak**  
Izvor: SUN

Uslijed povećavanja zahtjeva korisnika i prilika na tržištu pojavljuje se potreba za uvođenjem novih *cloud computing* modela. Primjer toga je i nedavno pojavljivanje privatnog oblaka (eng. *Private colud*) – načina upotrebljavanja infrastrukture javnog oblaka za privatne ili poluprivatne potrebe i povezivanje tih resursa s unutarnjim resursima korisničke baze podataka. Uobičajeno se to postiže povezivanjem korisnika u privatnu virtualnu mrežu (eng. *virtual private network*).

Kod dizajniranja oblaka dizajneri trebaju paziti na arhitekturno razmještanje podataka. Način razmještaja podataka ima velik utjecaj na buduću prilagodljivost, sigurnost i mobilnost rezultirajućeg rješenja.

## 2.4. Ekonomski aspekt

Korištenjem *cloud computinga* moguće je izbjeći velike troškove kupnje skupih sklopovlja, programa i usluga. Korisnici *cloud computing* usluga plaćaju samo ono što koriste. Uglavnom ne postoje zahtjevi za plaćanje unaprijed, a troškovi su jako mali u odnosu na korištenje vlastite IT infrastrukture. Ovaj pristup organizaciji IT rješenja korisnicima nudi jednostavan pristup podacima i mnoštvu različitih aplikacija. Druge prednosti ovoga pristupa su podijeljena infrastruktura i niski troškovi nadzora.

Općenito, korisnici uvijek mogu raskinuti ugovor gdje su usluge često pokrivenne sporazumima o razmjeni usluga s financijskim kaznama.

Korištenjem *cloud computinga* organizacije mogu uštedjeti na kapitalnim troškovima, ali s druge strane pri korištenju *cloud computinga* organizacije moraju biti jako oprezne. Ovisno o potrebama organizacije, troškovi usluge mogu biti i jako skupi, pa korištenje *cloud computinga* ne mora dovesti do velikih financijskih ušteda. U situacijama kada bi glavni troškovi bili relativno mali, ili kada organizacija ima veću fleksibilnost u svom osnovnom proračunu nego u operacijskom proračunu *cloud* model i nema nekog velikog financijskog smisla. Drugi faktori koji utječu na bilo koje druge potencijalne uštede uključuju učinkovitost organizacije baze podataka pojedine organizacije u usporedbi s oblakom nekog dobavljača, postojeće troškove organizacije, razinu prihvaćanja *cloud computinga* i tip funkcionalnosti koju oblak posjeduje.

## 2.5. Arhitekture u oblaku

Arhitektura programskih sustava uključenih u *cloud computing* tipično uključuje višestruku međusobnu komunikaciju komponenata oblaka. Komunikacija se obavlja preko aplikacijskog programskog sučelja, uobičajeno preko *web* poslužitelja. Ovo približno sliči tzv. Unix filozofiji posjedovanja više programa od kojih svaki dobro radi jednu stvar, a zajedno rade povezani preko univerzalnih sučelja.

*Cloud* arhitekture rješavaju nekoliko ključnih problema koji su bitni za obradu velike količine podataka. U tradicionalnoj obradi podataka teško je dobiti toliko računala koliko je pojedinoj aplikaciji potrebno. Također, teško je dobiti potrebna računala u trenutku kada su potrebni. Pojavljuju se mnoge poteškoće u raspodjeli i koordiniranju mnoštva poslova na različitim sustavima, pokretanju procesa na njima i osiguravanju alternativnih rješenja (npr. rezervno računalo) u slučaju da jedan od korištenih zakaže. Teško je automatski procijeniti poraste i padove dinamičkog opterećenja. Nakon obavljenog posla treba

se „riješiti“ svih tih korištenih strojeva. *Cloud* arhitektura rješava sve te probleme. Aplikacije izgrađene na *cloud* arhitekturi pokreću se u oblaku gdje fizičko mjesto infrastrukture određuje davatelj usluge. Oni iskorištavaju jednostavna programska sučelja (eng. *application programming interface*) dostupnih usluga na Internetu. Raspoređivanje se izvodi na zahtjev, a logika raspodjele i pouzdana logika usluga ostaje implementirana i skrivena u oblaku. Korištenje resursa u *cloud* arhitekturi je, po potrebi, ponekada kratkotrajno, a ponekada se javlja više puta, ali s određenim razmacima. Zbog toga je ova arhitektura jako iskoristiva i optimalna.

Kako bi razvojni inženjeri iskoristili što više prednosti *cloud computinga* moraju biti u mogućnosti reorganizirati aplikacije. Aplikacije se reorganiziraju tako da najbolje iskoriste arhitekturne i razvojne paradigme koje *cloud computing* podržava. Prednosti iskorištavanja aplikacija korištenjem *cloud computing* arhitekture uključuju smanjivanje vremena odziva, minimalizaciju rizika, smanjivanje troškova pristupa, povećavanje brzine inovacija i mnoge druge.

Prednosti gradnje aplikacija uz pomoć *cloud* arhitekture su:

- **Smanjivanje vremena izvođenja i vremena odziva.** Aplikacijama koje u suštini koriste oblake za izvršavanje mnoštva različitih poslova *cloud computing* omogućuje izvođenje na mnoštvu različitih poslužitelja. Na primjer, izvođenje se može omogućiti na 1000 poslužitelja i tako ubrzavati obavljanje posla. Obrada na takav način može biti gotova za 1/1000 vremena koje bi bilo potrebno jednom poslužitelju. Neki korisnici na vlastitom CPU (eng. *Central Processing Unit*) ne mogu izvršiti određene zadatke, pa se tada odlučuju za korištenje *cloud computinga*. Korištenjem *cloud computinga* korisnici imaju pristup aplikacijama koje im mogu ponuditi brzo vrijeme odziva, jer se korisnički zahtjev obrađuje na mnoštvu virtualnih strojeva. Izvođenje zadatka na virtualnom stroju može optimirati vrijeme odziva raspodjelom poslova na zahtjev korisnika.
- **Gotovo ne postoji plaćanje infrastrukture unaprijed.** Ako korisnik mora izgraditi veliki sustav, a želi ga izgraditi u potpunosti u svojem vlasništvu, to ga može jako puno koštati u startu. Korisnik bi tada morao investirati u sklopovlje (sklopovi, napajanja, usmjernici i dr.), upravljanje sklopovljem (upravljanje napajanjem, hlađenjem) i u operacijsko osoblje. Zbog velikih troškova organizacija bi trebala nekoliko odobrenja od uprave prije nego što bi projekt mogao započeti. Korištenjem uslužnog računarstva stvari se mijenjaju. Više ne postoje fiksni ili početni troškovi.
- **Smanjivanje rizika.** IT organizacije koriste oblake za smanjivanje sigurnosnih rizika kojima su podložni poslužitelji. Zakupljivanjem aplikacije u oblaku, glavni problemi davatelja usluga postaju raspodjela i rizik zakupljivanja premalo ili previše infrastrukture. U sve većem broju slučajeva davatelji *cloud* usluga imaju veliku infrastrukturu koja može podnijeti rast zakupljenog prostora i rad individualnog korisnika, smanjujući tako financijske rizike kojima korisnici mogu biti podložni.
- **Infrastruktura koja funkcionira točno na vrijeme** (eng. *just in time infrastructure*). Pri zakupljivanju aplikacija u oblaku programeri u početku možda i ne znaju kolike kapacitete moraju točno zakupiti, pa može doći do zakupljivanja prevelikog ili premalog dijela oblaka. Rješenja imaju mali rizik jer programeri mogu zakupljivati nove kapacitete kako im rastu potrebe, a ako u početku zakupe previše prostora *cloud* arhitekture isto tako mogu i osloboditi infrastrukturu jednako brzo kako su ju i zakupili.
- **Mali početni troškovi.** Postoje mnoga svojstva *cloud computinga* koja pomažu u reduciranju početnih troškova. Korištenjem ove tehnologije korisnici iznajmljuju infrastrukturu (dakle oni ju ne kupuju) pa troškovi nisu veliki, a kapitalne investicije mogu čak biti jednake nuli. Danas postoji mnoštvo različitih organizacija koje nude usluge *cloud computinga*. Zahvaljujući tome, kupci imaju veće mogućnosti izbora, a organizacije kako bi ostale konkurentne, smanjuju troškove kupnje ciklusa obrade i pohrane, što pomaže u daljnjem reduciranju početnih troškova korištenja *cloud computinga*.

Aplikacije se jako brzo razvijaju, čime se smanjuje vrijeme potrebno za njihov izlazak na tržište. Brzim izlaskom na tržište organizacije koje su napravile aplikaciju mogu dobiti veliku početnu prednost u odnosu na konkurenciju. Nudeći nešto novo one mogu diktirati cijenu i zarađivati više, sve dok neka konkurentna organizacija ne napravi neku sličnu, ali jeftiniju aplikaciju. Nakon toga organizacije se počinju boriti za prevlast na tržištu, a to čine kvalitetom i cijenom.

- **Povećan tempo inovacija.** *Cloud computing* povećava tempo inovacija. Niski početni troškovi pri ulasku na nova tržišta dovode izjednačavanju uvjeta na tržištu. Novim korisnicima niski početni troškovi omogućuju brz razvoj novih proizvoda po nižim cijenama, što im omogućuje ravnomjernije natjecanje s već dobro uhodanim organizacijama, čiji razvojni procesi mogu biti značajno veći. Veća razina nadmetanja povećava stupanj i tempo inovacija. Cijela industrija



profitira postojanjem mnogo inovatora koji koriste programe otvorenog koda i tako povećavaju broj inovacija.

- **Učinkovitije korištenje resursa.** Administratori sustava uglavnom se brinu oko nabavke sklopovlja kako ne bi ostali bez potrebnih kapaciteta, i oko boljeg iskorištavanja infrastrukture (kada imaju dovoljna sredstva i idealne količine kapaciteta). Korištenjem *cloud* arhitekture oni mogu bolje i učinkovitije upravljati resursima. Učinkovitije upravljaju resursima jer imaju mogućnost pristupa aplikacijama samo kada su im one potrebne, a nakon toga ih jednostavno mogu prestati koristiti.
- **Troškovi na temelju uporabe.** Stil naplaćivanja troškova po uporabi omogućuje naplaćivanje samo onih infrastrukture koje su korištene. Korisnik nije odgovoran za cijelu infrastrukturu oblaka. Ovo je ključna razlika između aplikacija koje se nalaze na samom računalu korisnika i *web* aplikacija. Aplikacije na radnoj površini ili tradicionalne klijent/poslužitelj aplikacije izvode se na korisnikovoj vlastitoj infrastrukturi (PC-u ili poslužitelju), dok kod aplikacija s *cloud* arhitekturom korisnik ne koristi vlastitu infrastrukturu i naplaćuje mu se samo dio infrastrukture koji je koristio.
- **Potencijal smanjivanja vremena obrade.** Paralelizacija je jedan od izvrsnih načina ubrzanja obrade. Ako jedan računski zahtjevan ili osjetljiv posao pokrenemo na jednom stroju i za njegovo izvršavanje je potrebno 500 sati, s *cloud* arhitekturom bilo bi moguće razdijeliti posao na 500 slučajeva i obaviti ga u jednom satu. Dostupnost elastične infrastrukture aplikacijama pruža mogućnost iskorištavanja paralelizacije, što je financijski jako pogodno i smanjuje potrebno vrijeme obrade.

## 2.6. Sigurnosni problemi i rizici

Neki analitičari smatraju da *cloud computing* obiluje sigurnosnim rizicima. Prije odabira organizacije čiju uslugu *cloud computinga* će koristiti, pametni korisnik bi prvo trebao obaviti procjene sigurnosti korištenja ove tehnologije. Provjeru sigurnosti najbolje može obaviti netko nepristran (npr. stručni konzultant).

*Cloud computing* ima jedinstvena obilježja koja zahtijevaju procjenu rizika u područjima poput integriteta, oporavka i privatnosti. *Cloud computing* zahtjeva i procjenu pravnih problema u područjima poput inovacija, nadzorne usklađenosti i revizija.

Amazonov EC2 i Google App Engine su primjeri *cloud computinga* koje analitičari opisuju kao tipove *cloud computinga* u kojima su masivno razdijeljene IT sposobnosti dostavljene kao usluga vanjskim korisnicima putem Interneta.

Korisnici moraju zahtijevati transparentnost i izbjegavati davatelje usluga koji odbijaju pružiti detaljne informacije o sigurnosnim problemima. Korisnici se moraju raspitati o sposobnosti onih koji vode politiku organizacije, arhitektima, programerima i operaterima, procesima nadzora rizika i tehničkih mehanizama, nivou testiranja koje je provedeno da bi se potvrdilo da procesi nadzora i usluge rade na planirani način te o tome jesu li davatelji usluga u sposobnosti identificirati neočekivane ranjivosti.

U nastavku su navedeni neki od specifičnih sigurnosnih rizika:

- **Privilegirani korisnički pristup.** Obrada osjetljivih podataka izvan organizacije donosi određenu razinu rizika. Vanjske usluge zaobilaze fizičke i logičke provjere kao i nadzor osoblja. Korisnici bi trebali prikupiti što više informacija o ljudima koji upravljaju podacima. Trebali bi od davatelja usluga zatražiti informacije o zapošljavanju i nadzoru privilegiranih administratora i provjerama ovlasti njihovih pristupa.
- **Nadzorna usklađenost.** Korisnici su odgovorni za sigurnost i integritet vlastitih podataka čak i kada su oni pohranjeni kod pružatelja usluga. Zato, prije nego što odaberu kojeg davatelja usluga žele izabrati moraju se o njemu dobro informirati. Tradicionalni pružatelji usluga se podvrgavaju vanjskim revizijama i sigurnosnom certificiranju, na taj način dokazujući korisnicima svoje vrijednosti i prednosti pred drugima. Davatelji usluga koji odbijaju pristupiti ovim ispitivanjima pokazuju da ih korisnici mogu angažirati samo za najjednostavnije usluge.
- **Adresa podataka.** Korisnik nema točan uvid gdje su njegovi podaci u oblaku pohranjeni. On ne mora znati čak ni državu u kojoj će biti pohranjeni. Korisnik može od davatelja usluge zatražiti pohranjivanje podataka na točno određenim adresama i davanje ugovorne obveze o poštivanju zahtjeva privatnosti u interesu korisnika.
- **Odvajanje podataka.** Podaci se u oblaku uobičajeno nalaze u zajedničkoj okolini s podacima drugih korisnika. Zaštitno kodiranje pri tome može biti korisno, ali ne rješava sve probleme. Korisnik prije odabira organizacije mora saznati što je učinjeno za odvajanje podataka. Davatelji

usluga trebali bi pružiti dokaze da su napravljene sheme zaštitnog kriptiranja ispitane. Pogreške u zaštitnom kriptiranju podatke mogu učiniti potpuno neupotrebljivim.

- **Oporavljanje.** Iako korisnik ne zna gdje su njegovi podaci spremljeni, davatelj *cloud* usluga bi trebao reći korisniku što će se dogoditi s podacima u slučaju neplaniranih nesreća. Svaka ponuda poslužitelja koja ne nudi dupliciranje podataka i aplikacija na više različitih mjesta je ranjiva i podložna totalnom gubitku podataka.
- **Podrška istraživanja.** Korištenjem *cloud computinga* istraživanja neprikladnih ili ilegalnih aktivnosti mogu biti nemoguća ili jako složena. *Cloud* poslužitelji su jako teški za istraživanje zbog potrebe za autentikacijom i zbog toga što se na jednom oblaku spremaju podaci mnogih korisnika, a podaci jednog korisnika mogu biti podijeljeni i na više različitih *datacentara* i poslužitelja. Ako korisnik ne može dobiti pismenu potvrdu da *cloud* podržava određene oblike istraživanja tada se može zaključiti da zahtjevi za istraživanjem i otkrivanjem neće biti mogući. Pismena potvrda davatelja usluge bi trebala sadržavati podatke kojima davatelj usluge potvrđuje da je već uspješno provodio takve aktivnosti.

Uobičajeni zahtjevi sigurnosti su:

CILJ	OPIS
<b>Povjerljivost</b>	Osiguravanje da se informacije ne otkriju ljudima koji nemaju prava pristupa.
<b>Integritet</b>	Osiguravanje da je informacija koja se čuva na sustavu prava reprezentacija informacije koja se trebala čuvati na poslužitelju i da nije modificirana od strane neovlaštene osobe.
<b>Dostupnost</b>	Osiguravanje da resursi za obradu informacije nisu nedostupni zbog utjecaja zlonamjernih korisnika.
<b>Nepriznavanje</b>	Osiguravanje da se može dokazati da su dogovori postignuti zaista napravljeni.

**Tablica 1. Uobičajeni zahtjevi sigurnosti**

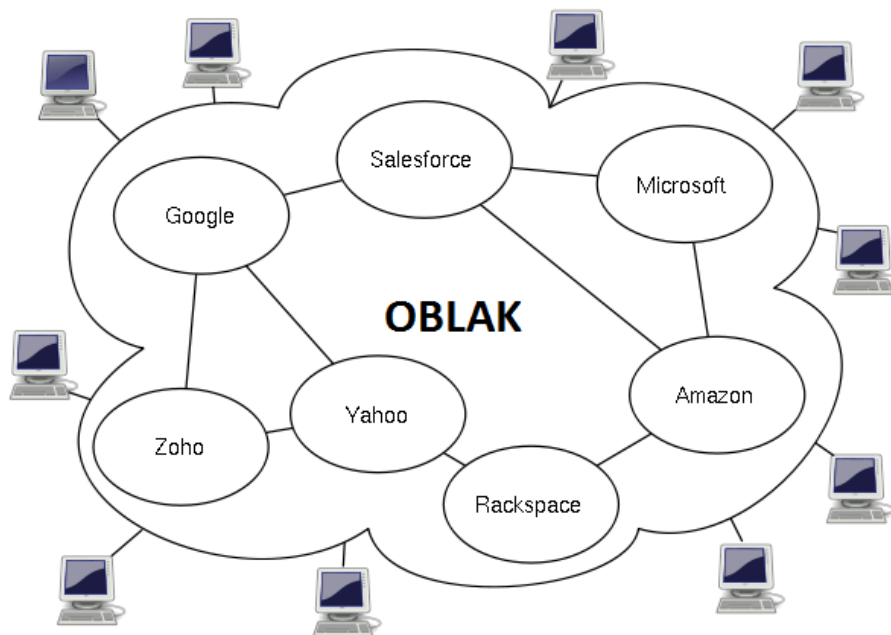
## 2.7. Oblaci „protiv“ oblaka

Od trenutka pojave *cloud computinga*, na tržištu se pojavilo mnoštvo novih davatelja usluga, a taj trend se i dalje odražava. Svaki od njih ima neke prednosti i nedostatke. Korisnici se odlučuju za one pružatelje usluga koji najbolje zadovoljavaju njihove potrebe. Kako svaki korisnik ima drugačije potrebe i drugačije stvari su mu bitne, dobra je činjenica da svaki davatelj usluga ima drugačije osobine. Isto tako je dobro to što se na tržištu trenutno nalazi mnoštvo različitih davatelja usluga, jer se time stvara pozitivna konkurencija na tržištu. Konkurencija prisiljava davatelje usluga na neprekidnu potrebu za usavršavanjem i na snižavanje cijena. Organizacije koje nude usluge *cloud computinga* moraju to raditi da bi bile u stanju zadržati svoje korisnike i uspješno konkurirati na tržištu.

Ispitivanje, koje je proveo Peter Wayner izvedeno je na nekoliko poznatih poslužitelja i nekoliko novih koji ovu uslugu tek počinju nuditi. Originalni članak o istraživanju moguće je pročitati na adresi:

<http://www.infoworld.com/d/cloud-computing/cloud-versus-cloud-guided-tour-amazon-google-appnexus-and-gogrid-122>

Najvažniji rezultati opisani su u nastavku teksta. Na temelju usporedbe svaki korisnik će moći izabrati onog davatelja usluga koji najbolje zadovoljava njegove potrebe.



**Slika 10. Poslužitelji cloud computinga**  
Izvor:Wikipedia

Iznenadujuće je da su davatelji usluga dosta međusobno različiti. Dok su mnogi dijelovi usluge *web hostinga* prilično standardni (pohrana podataka, obrada velike količine podataka, pristup različitim aplikacijama, nije potrebno kupovati sklopovlje), definicija *cloud computinga* jako varira. Amazonov Elastic Compute Cloud nudi Linux strojeve s administratorskim pristupom i mogućnost pokretanja bilo koje aplikacije. Googlov App Engine također dopušta i pokretanje bilo kojeg programa napisanog u Pythonu koji koristi Googleovu bazu podataka.

Poslužitelji nude različite mogućnosti spremanja podataka. Svaka osobina *cloud computinga* koja pojednostavljuje rad čini to uklanjanjem pojedinih sklopki (eng. *switch*) iz doseg korisnika, tako ga prisiljavajući na korištenje skupa rutina koje su možda, ali ne i nužno, ono što bi pružatelj usluga želio.

Oblaci su više manje zajednički poslužitelji. *Cloud computing* omogućava korištenje više procesora kad god se za to pojavi zahtjev, ali oni ne mogu riješiti probleme ravnomjernog raspoređivanja i spremanja podataka. Mnogi veliki izazovi se pojavljuju na arhitekturalnoj razini i jednostavno pokretanje više procesora neće riješiti osnovne pogreške u dizajnu.

Oblaci su jedna od mogućnosti spremanja podataka koja ima mnogo potencijala, ali tradicionalni *web hosting* i dalje ima značajne prednosti nad njima. Korištenje oblaka pojednostavljuje neke stvari, ali i dalje ne zadovoljava u potpunosti želje korisnika.

### 2.7.1. Amazon Elastic Compute Cloud

Amazon je bio jedna od prvih organizacija koja je lansirala rješenje namijenjeno široj javnosti, koji i dalje ima jedan od najprofinitijih i razrađenijih kompleta mogućnosti. Ako korisnik treba više procesora, korisnik može ubrzati virtualne strojeve s EC2 (eng. *Elastic Compute Cloud*) *web* uslugom. Ako korisnik želi pohraniti podatke, on može pohraniti do 5 GB podataka u S3 sustav (eng. *Simple Storage Service*). Amazon je izgradio i novi sustav korištenja baze podataka, ali ona je još u testnoj inačici. Da bi što prije obavili posao, korisnikova računala mogu direktno komunicirati a Amazonovom SQS-om uslugom (eng. *Simple Queue Service*) i API-em (eng. *application programming interface*) za slanje poruka.

Korištenjem sigurnosnih alata i upisivanjem naredbi u linije za upisivanje podataka korisnik šalje naredbe vlastitom setu poslužitelja „ u oblaku“. Svi virtualni poslužitelji koriste neki od Linux operacijskih sustava. Korisnik izabire vlastiti virtualni poslužitelj na koji želi instalirati vlastite programe i korisničke instalacije. Ako korisnik rezervira dovoljno mjesta na oblaku, učitavanje operacijskog sustava zajedno sa željenim aplikacijama se odvija jako brzo.

### 2.7.2. Google App Engine

Google App Engine nudi potpuno druge stvari u odnosu na Amazon. Dok kod Amazona korisnik dobiva administratorske ovlasti, na App Enginu ne može zapisati datoteku ni u svom vlastitom direktoriju. Google je iz sigurnosnih razloga zabranio korisniku zapisivanje podataka izvan Googleove baze podataka. Ako korisnik želi spremati podatke mora koristiti Googleovu bazu podataka.

Rezultat svih tih ograničenja nije nužno loša stvar. *Web* aplikacije su ogoljene do samog osnovnog skupa osobina i sagrađeno je prilično dobro okruženje za njihovu dostavu. Google nudi neke dobre alate za traženje pogrešaka u aplikacijama na korisnikovom stroju, ali inzistira i na povezivanju korisnikovog broja mobitela i Gmail korisničkog imena.

Najbolji korisnici App Enginea su grupe ili individualni korisnici koji u Pythonu žele napisati dio sučelja, koje se nalazi između korisnika i baze podataka. API je podešen za ovu vrstu posla.

### 2.7.3. GoGrid

GoGrid se sam smatra prvim svjetskim upravljačkim sustavom s više poslužitelja. Ono što GoGrid nudi nije funkcionalno jako različito od Amazonovog EC2, ali korištenje termina kontrolni okvir čini se ipak boljim opisom onoga što se događa nego što se to vidi korištenjem termina oblak. Korisnik započinje i prekida učitavanje podataka na isti način na koji relativno stari alati poput Pleska i cPanela dodaju i oduzimaju usluge.

GoGrid nudi mnoge iste usluge kao i Amazon EC2. Njegov *web control panel* korisnicima je ipak mnogo lakši za uporabu od EC2-ove naredbene linije, u koju korisnici Amazona upisuju naredbe za upravljanje vlastitim virtualnim strojevima. Nema potrebe za izrezivanjem i kopiranjem (eng. *cut and copy*) informacije jer mali *pop-up* prozori olakšavaju korisnicima rad s poslužiteljem. Nije potrebno upisivanje nikakvih naredbi u naredbene linije već se sve akcije odrađuju kroz jednostavno grafičko sučelje. Za vrijeme korištenja poslužitelja korisnici cijelo vrijeme imaju uvid u dosadašnje troškove (što je jako korisno za praćenje materijalnih troškova vezanih uz usluge koje se koriste).

GoGrid nudi mnoštvo pripremljenih operacijskih sustava spremnih za uporabu. Postoji uobičajena zbirka CentOS/Fedora i LAMP rješenja. Ako je korisniku potreban neki od Windows operacijskih sustava, uz adekvatnu naknadu, omogućeno mu je korištenje Windows Server 2003 operacijskog sustava s opcionalnim IIS 6.0 i Microsoft SQL Server paketima. Također, postoje i pripremljeni operacijski sustavi s instaliranim Ruby on Rails, PostgreSQL i Facebook aplikacijskim poslužiteljem. GoGrid ima mnoge slične značajke kao i Amazonov EC2. SimpleDB ipak nudi više *cloud* usluga za zajedničko spremanje informacija. Nedostatak usluga za zajedničko spremanje informacija otežava pokretanje i gašenje poslužitelja. Još jedan problem korisniku stvara nemogućnost prestanka plaćanja usluge. Jedini način prestanka plaćanja poslužitelja je njegovo brisanje, a to znači potpuni gubitak podataka koji se u tom trenutku na njemu nalaze.

### 2.7.4. AppNexus

AppNexus poslužitelj je dobar izbor za korisnike kojima se sviđa ideja *cloud computinga*, ali nisu sigurni žele li napustiti korištenje jezgre Unix operacijskog sustava te nekih administratorskih alata. Organizacija u čijem je vlasništvu AppNexus je uzela veliki poslužitelj industrijske veličine s najboljim alatima za zajedničko učitavanje i pohranu podataka te pronašla način prodavanja malih dijelova poslužitelja korisnicima. AppNexus pruža nekoliko apstraktnih naredbenih linija kojima korisnici dobivaju mogućnost uključivanja i isključivanja poslužitelja te pristup datotečnom sustavu.

Osnovne funkcionalnosti AppNexus oblaka su slične Amazonovom EC2. Korisnik se prijavljuje preko naredbene linije i pokrene pripremljenu distribuciju operacijskog sustava Linux. Ako se pojavi potreba, AppNexus može ponovo inicijalizirati virtualni poslužitelj i s drugih izvora (poput Amazonovog EC2). Pri takvoj izgradnji dolazi do zamjenjivanja jezgre s inačicom koja je pogodnija za virtualno okruženje. Korisnici na jednostavan način mogu pratiti pohranu i dijeljenje podataka unutar mreže (eng. *cluster*) poslužitelja.

Ipak, bolje rješenje je korištenje CDN (eng. *Content Delivery Network*) sustava. Mreža poslužitelja za pohranu podataka koji imaju ugrađen vlastiti skup HTTP poslužitelja. Korisnik može odmah započeti sa spremanjem statičkih podataka iz vlastitih datoteka. Podaci postaju dostupni odmah nakon njihovog zapisivanja u „/cdn“ mapu, a AppNexus raspodjeljuje podatke „u oblaku“ za pohranu podataka kako bi stvorio više neovisnih podatkovnih centara.

### 2.7.5. Uvjeti i ugovori

Kada korisnik želi koristiti usluge *cloud computinga* on mora s davateljima usluge sklopiti ugovore. Ugovori su specifični i jasni. U njima su navedeni uvjeti koje korisnik mora poštovati i mogućnosti koje potpisivanjem dobiva davatelj usluge.

GoGrid u ugovoru navodi brojčane pragove za standardne vrijednosti poput vremena čekanja, mijenjanja faze signala, gubitka paketa i dr. Ako sustav ne zadovoljava navedene vrijednosti GoGrid obećava davanje svojih usluga u iznosu 100 puta većem od izgubljenog iznosa.

Nakon što korisnik potpiše ugovor s Amazonom o korištenju usluge *cloud computinga*, Amazon ima pravo ukinuti korisnički račun i obrisati spremljene podatke. Amazon pri tome ne mora korisnicima navesti nikakav valjani razlog brisanja korisničkih podataka.

Google korisnicima ipak nudi malo bolje uvjete vezane za pravo brisanja korisničkih podataka. Google će ukinuti korisnički račun samo ako korisnik ne poštuje uvjete ugovora ili učini nešto ilegalno. Potpisivanjem ugovora između Googla i korisnika, Google dobiva pravo skeniranja, pregledavanja, obilježavanja, filtriranja, mijenjanja, odbijanja i/ili uklanjanja bilo kojeg dijela ili cijelog sadržaja s poslužitelja.

Poslužitelji *cloud computinga* su jako prilagodljivi pri izgradnji mreže uređaja, ali su i dalje daleko od savršenih. Veliki problem je mogućnost rušenja poslužitelja ili gubitka podataka s diska za vrijeme obavljanja određenog posla.

Ako korisnik želi da na sigurnost podataka ne utječe problem s bilo kojim poslužiteljem unutar oblaka, mora ih pohraniti u tzv. „podatkovnu memoriju oblaka“, ali to je jako skupo. Cijena je pri tome mnogo viša od uobičajene jer je razina usluge viša.

Svaka od organizacija ima drugačije načine naplaćivanja svoje usluge. GoGrid ima Intel Xeon poslužitelje, kojeg smatraju jačim nego što su poslužitelji drugih organizacija, pa zbog toga GoGrid povećava cijenu svoje usluge. Google ni ne naplaćuje svoju uslugu po vremenu trajanja usluge, već po broju ciklusa CPU-a. Amazon EC2 ima strojeve uobičajene veličine, ali i one koji imaju veći kapacitet od uobičajenih, pa ih zato i više naplaćuje. Kada se troškovi mijenjaju, organizacije često smanjuju cijene, ali ih isto tako i povećavaju kada se ispostavi da je cijena usluge bila viša od očekivane. U nastavku su dane neke okvirne cijene navedenih usluga.

Resurs	Jedinica	Cijena u \$
Premještanje podataka na poslužitelj	GB	0.12
Premještanje podataka s poslužitelja	GB	0.10
Vrijeme CPU	sati rada CPU	0.10
Pohrana podataka	GB mjesečno	0.15

**Tablica 2. Cijene Googlovih cloud computing usluga**

Resurs	Jedinica	Cijena u \$
Premještanje podataka na poslužitelj	GB	0.10
Premještanje podataka s poslužitelja	GB	0.15
Vrijeme CPU	sati rada CPU	0.12
Pohrana podataka	GB mjesečno	0.15
Prijenosi pohranjenih podataka	10K aplikacijskih zahtjeva	0.01

**Tablica 3. Cijene Amazonovih cloud computing usluga**

Resurs	Jedinica	Cijena u \$
Premještanje podataka na poslužitelj	GB	0.10
Premještanje podataka s poslužitelja	GB	0.14
Vrijeme CPU	sati rada CPU	0.125
Pohrana podataka	GB mjesečno	0.15

**Tablica 4. Cijene Microsoftovih cloud computing usluga**



### 3. Cloud Security Alliance

Cloud Security Alliance je neprofitna organizacija osnovana kako bi promicala uporabu najboljih načina na koje se korištenje *cloud computinga* može učiniti što sigurnijim. Cloud Security Alliance se bavi educiranjem korisnika o načinima uporabe *cloud computinga* i na taj način pomaže u osiguravanju svih drugih oblika računarstva (mobilnog računarstva, *grid* računarstva, mrežnog računarstva, klijentsko-poslužiteljskog računarstva, *peer-to-peer* računarstva i mnogih drugih).

Cloud Security Alliance čini mnoštvo stručnjaka iz različitih disciplina ujedinenih kako bi:

- promicali međusobno razumijevanje između korisnika i pružatelja usluga *cloud computinga* vezano za potrebne sigurnosne zahtjeve i potvrde osiguranja,
- promicali nezavisna istraživanja u područjima *cloud computing* sigurnosti,
- pokretali kampanje za podizanje svijesti i edukacijske programe o prikladnom korištenju *cloud computinga* i sigurnosnim rješenjima te
- stvarali liste problema i smjernica za povećanje sigurnosti *cloud computinga*.

#### 3.1. Povijest organizacije

2008. godine u sigurnosnoj zajednici postavljalo se sve više pitanja vezanih uz mogućnosti i sigurnosne probleme *cloud computinga*. Od te godine počinju sve veća ulaganja u istraživanja o sigurnosti ove tehnologije. Na konferenciji ISSA CISO Forum održanoj 20. kolovoza 2008. u Las Vegasu stvoren je osnovni koncept Cloud Security Alliancea. Na toj je konferenciji Jim Reavis održao predavanje o nadolazećim trendova zbog kojih se moraju početi poduzimati značajne akcije vezane uz sigurnost *cloud computinga*. Reavis i Nils Puhlmann su nakon toga odredili početne misije i strategije Cloud Security Alliance organizacije. U prosincu 2008. godine održano je mnoštvo sastanaka o problemima sigurnosti *cloud computinga*. Na tim sastancima prisustvovali su Reavis, Puhlmann i drugi važni ljudi iz različitih organizacija poput Suna, Qualysa, PGP, HP, RSA Securitya i mnogih drugih. Na njima je formalno osnovan Cloud Security Alliance. U radu Cloud Security Alliancea od trenutka osnivanja sudjeluju deseci stručnjaka iz različitih područja. Ti stručnjaci bavili su se istraživanjima, pisanjem i uređivanjem prvog vodiča za najbolje načine uporabe *cloud computing* tehnologije. On je objavljen 2009. godine na RSA konferenciji. Individualci koji su sudjelovali u nastanku prvoga vodiča smatraju se osnivačima Cloud Security Alliance organizacije. Ova organizacija i dalje rado prima sve stručnjake koji se žele baviti sigurnošću *cloud computinga*.

Cloud Security Alliance je izdao novu inačicu dokumenta "*Security Guidance for Critical Areas of Focus in Cloud Computing*" koji bi korisnicima trebao poslužiti kao vodič i inspiracija pri upravljanju rizicima pri korištenju *cloud computing* tehnologija koji su se pojavile nakon izdavanja prve inačice.

Zahvaljujući Cloud Security Allianceu danas se neprekidno pojavljuju nova rješenja za uklanjanje sigurnosnih problema *cloud computinga*. Organizacije koriste ovaj vodič kako bi si olakšale korištenje *cloud computinga*, a i sve se više priča o sigurnosnim problemima koji se javljaju diljem svijeta. Najvažnije dostignuće je to da se stručnjaci više bave sigurnosnim problemima budućnosti, a ne samo sadašnjosti.

#### 3.2. Što, kada i kako spremi u oblak?

Početak korištenja *cloud computinga* je složena odluka za svaku organizaciju, koja prvo mora odvagati sve prednosti i nedostatke koje joj to donosi.

*Cloud computing* nije nužno više ili manje siguran od uobičajenog načina spremanja podataka na poslužitelje i druge korisničke sustave. Kao i sa svakom drugom novom tehnologijom, i ovo rješenje otvara nove rizike ali i nove mogućnosti. U nekim slučajevima pohranjivanje podataka na oblak pruža mogućnost izmjene arhitekture starih aplikacija i infrastruktura kako bi zadovoljile sigurnosne zahtjeve korisnika. Cilj ovoga vodiča nije da korisnicima kaže što, gdje i kako pomaknuti u oblak, nego da im pruži praktične preporuke i odgovore na ključna pitanja kako bi rad s *cloud computingom* bio što sigurniji.

*Security Guidance*, kojeg je objavio Cloud Security Alliance, trebao bi pomoći korisnicima u odabiru te im dati trenutne preporuke na što treba obratiti pažnju i što treba izbjegavati. Cloud Security Alliance u dokumentu „*Security Guidance*“ fokusira se na 15 poglavlja (novija inačica na 13), koja korisnicima olakšavaju specifikaciju vlastitih potreba i sigurnosnih odluka. Domene su podijeljene u tri osnovne skupine:

- arhitektura oblaka (jedno poglavlje),

- upravljanje oblakom (pet poglavlja) i
- operacije u oblaku (sedam poglavlja).

Kroz vodič su dane iscrpne preporuke kako reducirati rizike prihvaćanjem *cloud computinga*, ali praćenje svih preporuka nije nužno. Ni jedan vodič ni lista za korisnike *cloud computinga* ne mogu dati potpune upute i preporuke. *Cloud computing* nudi mnoštvo različitih modela, pa je nemoguće predvidjeti sve mogućnosti.

Jednostavni okvir koji pomaže korisnicima u određivanju početnih rizika *cloud computinga* i obavještava ih o sigurnosnim odlukama sastoji se od stavki navedenih u sljedećim potpoglavljima.

### 3.2.1. Identifikacija sredstava koja korisnik želi pohraniti u oblaku

Prvi korak u procjeni rizika *cloud computinga* je određivanje što točno korisnici žele pohraniti. Sredstva koja se mogu pohraniti u oblaku mogu se podijeliti u dvije skupine:

1. podaci,
2. aplikacije, funkcije i/ili procesi.

Korištenjem *cloud computinga* podaci i aplikacije ne moraju biti pohranjene na istim adresama. Korisnik čak može premješati samo dijelove funkcija na oblake.

### 3.2.2. Procjena važnosti sredstava

Idući korak je određivanje važnosti podataka ili funkcija za pojedinu organizaciju. Korisnici ipak trebaju barem grubu procjenu osjetljivosti imovine i važnosti aplikacija, funkcija i procesa. U suštini *Guidance* se bavi procjenom povjerljivosti, integriteta i zahtjeva povjerljivosti te kako na njih utječe pohranjivanje dijela ili svih sredstava na oblak.

### 3.2.3. Odabir modela

Korisnici moraju znati kolika je važnost sredstava. Sljedeći korak je odabir modela *cloud computing* arhitekture koji je pogodan za određenog korisnika. Prije nego što se korisnik odluči za pojedinog davatelja usluge on mora znati može li podnijeti rizike vezane za različite izvedbene modele.

### 3.2.4. Ocjenjivanje rizika

U ovom koraku korisnici se usmjeravaju na određivanje stupnja provjere. Ako korisnik već ima određene zahtjeve može ih uključiti u ocjenjivanje, a ako razmatra točno određenu ponudu može koristiti potpunije procjene rizika.

### 3.2.5. Skiciranje potencijalnog protoka podataka

Ako korisnik razmatra specifičnu razvojnu mogućnost, trebao bi napraviti potpuni plan protoka podataka između vlastite organizacije, pružatelja usluge i svakog drugog čvora.

## 3.3. Glavne prijetnje sigurnosti cloud computinga

CSA (eng. Cloud Security Alliance) je u travnju 2009. godine razvio vodič za korisnike pod imenom: „*Security Guidance for Critical Areas in Cloud Computing*“. Ovaj vodič je brzo postao industrijski vodič za sigurnost ove tehnologije. Mnoštvo organizacija diljem svijeta koriste ovaj vodič kako bi upravljale svojim *cloud computing* resursima.

Nakon toga CSA (eng. Cloud Security Alliance) je objavio dokument „*Top Threats to Cloud Computing*“ kako bi pružio potrebnu pomoć organizacijama pri donošenju odluka o upravljanju rizikom. Ovaj dokument korisnicima služi kao dodatak ranijem dokumentu: „*Security Guidance for Critical Areas in Cloud Computing*“. Kako se svakodnevno pojavljuju različite nove prijetnje sigurnosti kao i novi rizici, navedeni dokument se stalno nadograđuje. U njemu su se stručnjaci usmjerili na jedinstvene ili jako raširene probleme *cloud computinga*. U nastavku je opisano sedam osnovni prijetnji *cloud computing* arhitekturi.

### 3.3.1. Zloupotreba cloud computinga

Korisnici *cloud computinga* često imaju privid neograničenih mogućnosti uporabe, što naravno nije utemeljena činjenica. Možda najveći takav privid imaju korisnici IaaS sustava. Navedeni model korisnicima daje neograničene mogućnosti uporabe mrežnih resursa i pohrane podataka. Neki



davatelji usluga nude i besplatnu, ali ograničenu, uporabu usluga *cloud computinga* u određenom probnom periodu. Sve navedeno smanjuje stupanj sigurnosti korištenja *cloud computinga*.

Zlonamjerni korisnici relativno jednostavno i nekažnjeno iskorištavaju sigurnosne propuste tako da razvijaju tehnologije koje će im omogućiti učinkovitiji pristup i iskorištavanje podataka drugih korisnika, a pri tome neće ugroziti vlastiti identitet. Davatelji *cloud computing* usluga su neprekidna meta zlonamjernih korisnika, djelomično zbog relativno slabih autentikacijskih sustava, a djelomično zbog izostanka svijesti o sigurnosnim rizicima krajnjih korisnika sustava.

Najviše napada preživjeli su davatelji PaaS modela *cloud computinga*, ali u zadnje vrijeme istraživanja pokazuju sve veću učestalost napada i na IaaS model pružanja usluge. U budućnosti će davatelji usluga veću pažnju morati posvetiti sprječavanju probijanja lozinki i ključeva, DDoS napadima (eng. *Distributed Denial of Service*), pokušaju izvođenja dinamičkih napada i sličnim napadačkim tehnikama.

Da bi se korisnici i davatelji usluga zaštitili od napada trebali bi:

- uvesti složeniju početnu registraciju i provjeru procesa,
- poboljšati praćenje i koordinaciju prijevera koje se izvode preko kreditnih kartica,
- uvesti cjelokupno provjeravanje mrežnog prometa korisnika te
- ugraditi nadzor javnih crnih lista na kojima su navedeni zlonamjerni korisnici (tj. adrese s kojih se korisnici prijavljuju) kako bi se zaštitili vlastiti sustavi.

### 3.3.2. Nesigurna sučelja i API

Davatelji *cloud computing* usluga otkivaju dio programskih sučelja ili API-a (eng. *application programming interface*) koje korisnici koriste za upravljanje *cloud* uslugama. Korištenjem ovih sučelja korisnici mogu izvoditi raspodjelu, upravljanje, nadzor i sinkronizaciju. Sigurnost i dostupnost osnovnih *cloud computing* usluga ovisi o dostupnosti i sigurnosti API-a. Ova sučelja moraju osigurati zaštitu korisnika od zlonamjernih napada. Mnoge organizacije na ta sučelja nadograđuju dodatne usluge, koje još više otežavaju sprječavanje različitih zlonamjernih napada. Na taj način organizacije dobivaju nova (složenija) sučelja, koja su zbog svoje složenosti više izložena riziku. Većina davatelja usluga teži osiguravanju vlastitih modela, ali i korisnici pri uporabi moraju razumjeti sigurnosne probleme povezane s uporabom, upravljanjem, sinkronizacijom i praćenjem *cloud* usluga. Ako se organizacija prepusti korištenju slabe skupine sučelja, ona se tako izlaže različitim oblicima rizika povezanih sa sigurnošću, integritetom, dostupnošću i odgovornošću.

Zlonamjerni korisnici za izvršavanje zlonamjernih napada na korisnike često iskorištavaju to što se korisnici često susreću s anonimnim pristupom i/ili potrebom za ponovnom uporabom lozinki, prijavom bez upisivanja teksta ili prijenos sadržaja, nefleksibilnom provjerom pristupa ili nevaljalom autentifikacijom, ograničenim praćenjem i bilježenjem sposobnosti, nepoznatim uslugama ili zavisnosti sučelja.

Prijetnja se pojavljuje na svim modelima pružanja usluge - IaaS, SaaS i PaaS.

Da bi se korisnici i davatelji usluga zaštitili od napada potrebno je:

- analizirati sigurnosne modele sučelja davatelja *cloud computing* usluga,
- prenositi šifrirani signal i osigurati odgovarajuću *autentikaciju* i provjeru pristupa te
- razumjeti da se preko sučelja povezuju na druge sustave koji mogu biti sigurnosno ugroženi (pa se tako mogu neplanirano i neoprezno i sami izložiti riziku).

### 3.3.3. Zlonamjerni korisnici koji napade izvode iznutra

Većina organizacija je jako dobro upoznata s opasnostima koje im mogu donijeti dobro upućeni zlonamjerni korisnici. Ova prijetnja predstavlja još veći problem korisnicima *cloud* usluga. Prijetnja predstavlja problem pogotovo kada se u obzir uzme osnovni nedostatak transparentnosti procesa i procedura davatelja usluga.

Na primjer, davatelji usluga ne otkrivaju način na koji svojim korisnicima daju pristup fizičkim i virtualnim sredstvima, niti način na koji prate korisnike, analiziraju i izvještavaju o suradnji. Ova situacija stvara privlačnu mogućnost iskorištavanja, koju zlonamjerni korisnici rado iskorištavaju. Razina odobrenog pristupa oblaku omogućuje iskorištavanje povjerljivih podataka ili dobivanje potpunog nadzora nad uslugom s jako malom mogućnošću otkrivanja identiteta napadača. Utjecaj koji zlonamjerni korisnici „iznutra“ mogu imati na organizaciju definitivno se ne smije zanemariti,

pogotovo kada se u obzir uzme njihova razina pristupa i mogućnost prodiranja u organizacije. Neki od načina na koji zlonamjerni korisnici mogu utjecati na organizaciju su povreda ugleda, financijski utjecaj i gubitak produktivnosti. Kada organizacija prihvati *cloud* poslužitelje ljudski utjecaj postaje još veći. Jako je važno upoznati korisnike *cloud computinga* s postupcima koje poduzima davatelj usluga da bi spriječio napade iznutra.

Da bi se korisnici i davatelji usluga zaštitili od napada trebaju:

- provoditi strogi nadzor nad lancem nabave i provoditi cjelokupne procjene isporučitelja,
- odrediti zahtjeve za ljudskim resursima kao dio pravnog ugovora,
- zahtijevati transparentnost u informacijskoj sigurnosti i praksi upravljanja, kao i usklađenost izvještavanja i
- odrediti proces obavještanja o sigurnosnim problemima.

### 3.3.4. Zajednički tehnološki problemi

IaaS model pružanja usluge se temelji na dijeljenju infrastrukture. Često komponente koje čine infrastrukturu nude jaka izolacijska svojstva za arhitekturu podijeljenu na više korisnika. Da bi se riješio ovaj nedostatak potreban je veći nadzor međusobnog posredovanja operacijskih sustava korisnika i fizičkih računalnih resursa. Unatoč povećanom nadzoru zlonamjerni korisnici ipak pronadu način dobivanja neprikladne razine nadzora ili utjecaja na platformu. Obrana od tih prijetnji bi trebala uključiti povećano praćenje korisničkih aktivnosti, akcija čitanja/pohrane podataka i nadzor aktivnosti na mreži.

Zlonamjerni korisnici su u posljednjih nekoliko godina uspjeli zloupotrijebiti zajedničku imovinu korisnika koja se nalazi „u oblaku“. Dijelovi diska, predmemorija procesora, GPU i drugi zajednički elementi nikada nisu bili namijenjeni snažnoj podjeli. Kao rezultat toga zlonamjerni korisnici se usmjeravaju na izvođenje operacija na prostorima drugim korisnicima i tako dobivaju neovlašteni pristup podacima.

Prijetnja se pojavljuje na IaaS modelima pružanja usluge.

Da bi se korisnici i davatelji usluga zaštitili od napada potrebno je:

- implementirati najbolje sigurnosne postupke za instalaciju / konfiguraciju,
- proučavati okolinu da bi se uočile neovlaštene promjene / aktivnosti,
- promicati jake autentikacijske mehanizme i nadzor pristupa za administrativne radnje i
- promicati ugovore o razini usluge kako bi se smanjio utjecaj ranjivosti.

### 3.3.5. Gubitak i neovlašteno otkrivanje podataka

Postoje brojni načini na koje zlonamjerni korisnici mogu ugroziti važne podatke organizacije. Primjer toga je brisanje ili promjena podataka bez kopije originalnog sadržaja. Raskidanje veze između dijela podataka pohranjenog na nekom drugom dijelu poslužitelja i cjelokupnog izvornog podatka može podatak učiniti nepovratnim (jednako kao što to može učiniti pohrana podataka na nesiguran medij za pohranu). Gubitak ključa za kodiranje može dovesti do uništavanja bitnih podataka. Neovlaštenim stranama mora biti zabranjen pristup osjetljivim podacima. U oblaku raste prijetnja ugrožavanja podataka zbog mnoštva različitih međudjelovanja između rizika i izazova koji su jedinstveni za oblak ili, još opasnije, zbog arhitekturnih ili operacijskih svojstava oblaka.

Gubitak ili neovlašteno otkrivanje podataka mogu imati poguban utjecaj na poslovanje. Mogu ugroziti ugled i reputaciju organizacije, dovesti do prekida poslovne suradnje s organizacijama koje koriste oblak, poslovnim partnerima ili gubitka povjerenja korisnika. Gubitak ključnog intelektualnog vlasništva može imati natjecateljske i financijske utjecaje, jer će mnoge druge organizacije ili zlonamjerni korisnici pokušati doći do tih podataka i iskoristiti ih za vlastitu dobrobit. Ovisno o podacima koji su izgubljeni ili su djelomično procurili na tržište može doći do kršenja ljudskih prava (npr. objavljivanja inkriminirajućih podataka o nekome pojedincu, iskorištavanje dobivenih informacija u želji da se smanji financijska moć ili ugled pojedinca) i pravnih posljedica (npr. pokretanje sudskih postupaka protiv pojedinca ili organizacije zbog sadržaja pronađenih podataka). Do iskorištavanja podataka organizacija ili pojedinačnih korisnika može doći zbog nedovoljne autentikacije, autorizacije i provjere kontrole, zatim nepravilnog korištenja šifri i programskih ključeva, operacijskih neuspjeha, pouzdanosti podatkovnih centara i dr.

Prijetnja se pojavljuje na svim modelima pružanja usluge. Da bi se korisnici i davatelji usluga zaštitili od napada potrebno je:

- implementirati sučelje s dobrom kontrolom pristupa,
- kriptirati podatke i zaštititi njihov integritet podataka,
- analizirati zaštitu podataka za vrijeme dizajna i izvođenja te
- nakon što korisnici oduče za prestanak korištenja poslužitelja, davatelji usluga bi trebali trajno ukloniti korisničke podatke sa poslužitelja. Korisnici bi trebali sklopiti ugovor s davateljima usluge koji sadrži detalje oko postojanja sigurnosnih mjera i strategije pridržavanja.

### 3.3.6. Krađa korisničkih imena

Krađom korisničkog imena napadači mogu iskorištavati usluge koje plaćaju korisnici. Zlonamjerni korisnici napadima poput krađe identiteta, prijevare i iskorištavanja programskih ranjivosti još uvijek postižu uspjehe u narušavanju sigurnosti korisnika. Korisnici često koriste iste vjerodajnice i lozinke, što povećava broj ovakvih napada. Korištenjem *cloud computinga* pojavljuju se nove prijetnje. Ako napadač dobije pristup vjerodajnicama, on može promatrati aktivnosti i transakcije, upravljati podacima te usmjeravati korisnike na zlonamjerne stranice. Korisnički računi ili usluge postaju napadačima nova meta s kojom mogu iskorištavati korisnikov identitet za izvođenje daljnjih napada.

Krađa korisničkih imena, obično u obliku krađe vjerodajnica (eng. *credentials*), korisnicima predstavlja jednu od najvećih prijetnji. S ukradenim vjerodajnicama zlonamjerni napadači mogu pristupiti kritičnim podacima *cloud computing* usluga, i tako ugroziti povjerljivost, integritet i dostupnost tih usluga. Organizacije bi trebale biti svjesne ovih tehnika kao i uobičajenih načina zaštite od istih.

Prijetnja se pojavljuje na svim modelima pružanja usluge *cloud computinga*.

Da bi se korisnici i davatelji usluga zaštitili od napada potrebno je:

- zabraniti dijeljenje pristupnih vjerodajnica između korisnika i poslužitelja,
- gdje god je moguće koristiti snažne dvofaktorske autentikacijske tehnike,
- izvoditi proaktivno praćenje za otkrivanje neovlaštenih aktivnosti i
- razumijevati sigurnosne politike i SLA (eng. *service level agreement*) davatelja *cloud computing* usluga.

### 3.3.7. Nepoznati profil rizika

Jedna od karakteristika *cloud computinga* je smanjivanje vlasništva nad sklopovljem i programima te omogućavanje organizacijama da se usmjere na njihove osnovne poslovne strategije. To dovodi do finansijskih i operacijskih prednosti koje se moraju pažljivo odvagati s kontradiktornim sigurnosnim problemima. Inačice programa, dopune koda, sigurnosne prakse, profil ranjivosti kao i pokušaji neovlaštenih pristupa su jako važni faktori za procjenu rizika organizacije. Za procjenu rizika organizacijama su jako važne i informacije o tome tko sve dijeli zajedničku infrastrukturu. Sigurnost skrivanjem podataka (eng. *security by obscurity*) može se jednostavno postići, ali može rezultirati nepoznatom izloženošću. Ona također može utjecati i na dubinske analize koje zahtijevaju visok stupanj nadzora ili regulirana operacijska područja.

Da bi se korisnici i davatelji usluga zaštitili od napada trebali bi se usmjeriti na:

- razotkrivanje primjenjivih zapisa i podataka,
- djelomično i/ili puno otkrivanje detalja infrastrukture i
- praćenje i upozoravanje na potrebne informacije kojima korisnici mogu smanjiti izloženost riziku.

## 4. Prošlost, sadašnjost i budućnost

*Cloud computing* je prošao kroz mnoštvo razvojnih faza koje uključuju *grid* i *utility computing*, APS (eng. *application service provision*) i SaaS (eng. *Software as a Service*). Kao počeci *cloud computinga* smatraju se 1960.-te godine.

Sve je počelo s idejom J.C.R. Licklidera o kompjuterskoj mreži koja povezuje cijeli svijet. On je, među ostalim, odgovoran za omogućavanje razvoja ARPANET-a (eng. *Advanced Research Projects Agency Network*) 1969. godine. Njegova vizija bila je da svi na Zemlji budu međusobno povezani i imaju pristup programima i podacima na svakoj *web* stranici s bilo koje lokacije na svijetu. To je ideja koja uvelike sličí današnjem *cloud computingu*.

Neki stručnjaci pripisuju zasluge stvaranja koncepta *cloud computinga* drugome znanstveniku - Johnu McCarthyju. On je predložio ideju o javno dostupnom računarstvu (eng. *utility computing*). Zaista, *cloud computing* ima slične karakteristike kakve su imale organizacije koje su u šezdesetim godinama prošlog stoljeća pružale usluge obrade podataka na udaljenim poslužiteljima.

Termin oblak posuđen je iz telefonije i telekomunikacija, koje su do 1990.-ih primarno nudile točno usmjereni prijenos podataka, a tada su počele nuditi i usluge VPN-a (eng. *Virtual Private Network*) s usporednom kvalitetom usluge, ali puno nižim troškovima. Prospajanjem prometa, kako bi uravnotežili iskorištavanje, bili su u mogućnosti iskoristiti cjelokupnu propusnost mreže. Simbol oblaka se koristio za označavanje točke grananja poslužitelja od jednog do drugog korisnika.

*Cloud computing* širi te granice da bi u potpunosti obuhvatio poslužitelje i infrastrukturu mreže. Od šezdesetih godina *cloud computing* se razvijao u mnogo smjerova (*Web 2.0* je primjer najnovije inovacije). Međutim, Internet se tek u devedesetim godinama počeo masovnije primjenjivati i imati značajniju propusnost. Jedna od značajnijih prekretnica u *cloud computingu* bio je nastanak Salesforce.coma 1999. godine. Salesforce.com je bio pionir u konceptu dostavljanja aplikacija preko jednostavnih *web* stranica. Njihovi poslužitelji su popločali put specijaliziranim programskim organizacijama za dostavljanje aplikacija preko Interneta.

Amazon je odigrao ključnu ulogu u razvoju *cloud computinga* moderniziranjem svojih podatkovnih centara. Nova arhitektura oblaka rezultirala je značajnim i učinkovitim unutrašnjim poboljšanjima koja omogućuju malim organizacijama lakše i brže dodavanje novih podataka u oblake. Prva njegova značajna inovacija bio je Amazon *Web Service* (objavljen 2002. godine), koji je pružio *cloud computing* usluge koje uključuju pohranu i obradu, pa čak i ljudsku inteligenciju preko Amazon Mechanical Turka. Amazon je na osnovama *utility computinga* 2005. godine počeo osiguravati pristup svojim sustavima preko *web* poslužitelja. Ova osobina razvoja Amazon *web* poslužitelja ocijenjena je kao izuzetno pojednostavljeno dotadašnjih tehnoloških dostignuća na ovome području. 2006. godine Amazon je objavio EC2 (eng. *Elastic Compute cloud*) kao komercijalni *web* poslužitelj koji malim organizacijama i individualnim korisnicima omogućuje iznajmljivanje kompjutera na kojima mogu pokretati vlastite aplikacije. Amazon EC2/S3 je bio prvi komercijalni *cloud computing* poslužitelj.

Google, IBM i nekolicina sveučilišta uključila su se 2007. godine u veliki istraživački projekt daljnjeg razvoja *cloud computinga*. To je rezultiralo novim inovacijama na ovom području.

Značajna prekretnica pojavila se 2009. godine. Bio je to *Web 2.0*, koji je tada započeo svoj proboj na tržište. Google i druge organizacije tada su isto počele nuditi aplikacije zasnovane na preglednicima. Tako je nastao Google Apps.

Najvažniji doprinos razvoju *cloud computinga* bilo je pojavljivanje uspješnih novih aplikacija objavljenih od strane Microsofta i Googlea. Te dvije organizacije pružale su usluge koje su pouzdane i lake za korištenje, pa su odmah prihvaćene na tržištu. Drugi ključni faktori koji su omogućili razvoj ove tehnologije uključuju razvijanje virtualizacijske tehnologije, razvoj univerzalnih brzih propusnica i univerzalnih programskih standarda.

Mnoge organizacije danas prepoznaju prednosti koje im nudi *cloud computing*. On im omogućuje povećanje mogućnosti pohrane podataka, prilagodljivost i smanjenje troškova. Ali korisnici su i dalje zabrinuti za sigurnost vlastitih podataka pohranjenih u oblaku.

*Cloud computing* će doživjeti pravi procvat u praksi tek kada se riješe sigurnosni problemi koje trenutno posjeduje. Analitičari smatraju da će ti sigurnosni problemi uskoro biti riješeni. Kada se riješe sigurnosni problemi, poslužitelji *cloud computinga* omogućiti će korisnicima širenje vlastitih infrastruktura, dodavanje kapaciteta na zahtjev korisnika, povećavanje prilagodljivosti, a u ponudi će biti i sve više različitih resursa (pa će time doći i do značajnih financijskih ušteda).

Organizacije će u budućnosti vjerojatno sve više koristiti *cloud computing*. To će se dogoditi kada se na Internetu počne povećavati broj usluga koje se mogu koristiti za obradu i pohranu zahtjevnijih aplikacija. *Cloud computing* donijeti će velike prednosti IT korisnicima.

## 5. Zaključak

*Cloud computing* je nova i nadasve obećavajuća paradigma pružanja IT usluga. Ovaj oblik računarstva danas još definitivno nije na svome vrhuncu, iako na tržištu već postoje nekolicina komercijalnih pružatelja ovih usluga. *Cloud computing* i dalje nije zastupljen na tržištu u mjeri kojoj bi mogao biti, tako da će stručnjaci morati i dalje raditi na njegovom razvoju i stvaranju novih inovacija, u hoda vanju postojećih rješenja pazeći pri tome da sigurnost cijelog sustava (p)ostane dovoljno dobra. *Cloud computing* će dosegnuti svoj potpuni razvojni potencijal tek kada se uklone dosadašnji problemi poput problema sigurnosti, dostupnosti, teškog prebacivanja podataka, ovisnosti o jednom poslužitelju i dr. Tek po nestanku tih problema značajno će se povećati broj korisnika. *Cloud computing* ima svijetlu budućnost zato što teži povećavanju kapaciteta ili novih mogućnosti bez investiranja u nove infrastrukture, obuku novog osoblja ili kupovanje novih licenciranih programa. Sve su to velike prednosti *cloud computinga* u odnosu da dosadašnje načine pohranjivanja podataka, koje će organizacijama donijeti velike financijske uštede te im pružiti mogućnost bržeg i većeg razvoja, investiranja u nova istraživanja i nove projekte, pa tako i daljnji razvoj IT sektora.

## 6. Reference

- [1] Infoworld, Seven cloud-computing security risks,  
<http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0>
- [2] Infoworld, What cloud computing really means,  
<http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031>
- [3] Infoworld, Cloud versus cloud,  
<http://www.infoworld.com/d/cloud-computing/cloud-versus-cloud-guided-tour-amazon-google-appexus-and-gogrid-122>
- [4] Infoworld, Early experiments in cloud computing,  
<http://www.infoworld.com/d/cloud-computing/early-experiments-in-cloud-computing-020>
- [5] Global Security Challenge,  
[http://www.globalsecuritychallenge.com/gsc\\_competitions.php#cloud](http://www.globalsecuritychallenge.com/gsc_competitions.php#cloud)
- [6] Cloud Security Alliance, History  
<http://www.cloudsecurityalliance.org/About.html>
- [7] Cloud Security Alliance,  
<http://www.cloudsecurityalliance.org/>
- [8] Cloud Security, Cloud Security Threats Survey,  
<http://cloudsecurity.org/>
- [9] Wikipedia, Cloud\_Computing\_Security,  
[http://en.wikipedia.org/wiki/Cloud\\_computing\\_security](http://en.wikipedia.org/wiki/Cloud_computing_security)
- [10] SNS, Cloud Computing,  
[http://csrc.nist.gov/groups/SNS/cloud-computing/Computer Weekly. A History of Cloud Computing.](http://csrc.nist.gov/groups/SNS/cloud-computing/Computer_Weekly_A_History_of_Cloud_Computing)  
<http://www.computerweekly.com/Articles/2009/06/10/235429/A-history-of-cloud-computing.htm>
- [11] Cloud Security Alliance, Topthreats,  
<http://www.cloudsecurityalliance.org/topthreats.html>