Sigurnosni i pravni aspekt zaštite podataka u cloud okruženju

Sunić, Eugen

Master's thesis / Diplomski rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:545531

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository







SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Eugen Sunić

SIGURNOSNI I PRAVNI ASPEKT ZAŠTITE PODATAKA U *CLOUD* OKRUŽENJU

DIPLOMSKI RAD

Zagreb, 2016.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 19. travnja 2016.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Telekomunikacijska legislativa i standardizacija**

DIPLOMSKI ZADATAK br. 3523

Pristupnik: **Eugen Sunić (0135216922)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Sigurnosni i pravni aspekt zaštite podataka u cloud okruženju**

Opis zadatka:

U diplomskom radu treba najprije definirati pojam cloud okruženja te ukratko opisati povijest nastanka clouda. Zatim ukratko navode temeljne karakteristika clouda kao i servisni modeli: SaaS, IaaS, PaaS te što svaki od tih modela nudi. Srž rada je u analizi i istraživanju implementacije različitih standarda unutar računalnog clouda. To zahtjeva temeljni opis relevantnih standarda i njegovu primjenu. Rad će opisati rješenja koja nudi Europska unija te rješenja od strane Sjedinjenih Država. Isto tako napravit će istraživanje o europsko-američkome sporu sigurne luke (eng. safe harbour) koji ukazuje na neusuglašenost pravnih pravila te probleme koji onemogućuju interoperabilnost između američkih i europskih organizacija. Rad će se dotaknuti direktive Europske unije za zaštitu podataka te istražiti što ona nudi u pogledu zaštite korisnika u cloud okruženju.

Zadatak uručen pristupniku: 15. ožujka 2016.

Mentor:

doc. dr. sc. Goran Vojković

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

SIGURNOSNI I PRAVNI ASPEKT ZAŠTITE PODATAKA U *CLOUD* OKRUŽENJU

SECURITY AND LEGAL ASPECTS OF DATA PROTECTION INSIDE THE CLOUD ENVIRONMENT

Mentor: doc. dr. sc. Goran Vojković

Student: Eugen Sunić, 0135216922

Zagreb, rujan 2016.

SIGURNOSNI I PRAVNI ASPEKT ZAŠTITE PODATAKA U *CLOUD* OKRUŽENJU

SAŽETAK

Cloud computing predstavlja novu paradigmu u informacijsko-komunikacijskim uslugama. Međutim, prije uvođenja *cloud* okruženja, potrebno je ispitati financijsku isplativost prelaska s tradicionalnog načina na *cloud*. Za razliku od tradicionalnog načina, spremanje podataka i procesorska snaga seli se s osobnih računala, na *cloudu*. Tamo se datoteke obrađuju i spremaju, što znači da se podaci spremaju na fizički udaljene poslužitelje. U tim podacima mogu postojati i osobni podaci. Prema trenutnoj europskoj i hrvatskoj zakonodavnoj regulativi s osobnim podacima se mora pažljivo postupati, pravno i tehnički. Zbog toga se u ovom diplomskog radu daje pregled sigurnosnih i pravnih aspekata zaštite podataka u *cloud* okruženju.

KLJUČNE RIJEČI: *cloud* okruženje; osobni podaci; zaštita osobnih podataka; sigurnosni aspekt zaštite osobnih podataka; pravni aspekt zaštite osobnih podataka

SECURITY AND LEGAL ASPECTS OF DATA PROTECTION INSIDE THE *CLOUD* ENVIRONMENT

SUMMARY

Cloud computing represents a new paradigm in information and communication services. However, before the introduction of *cloud* environments, it is necessary to examine the financial feasibility of switching from the traditional way of the *cloud*. Unlike the traditional way, data storage and processing power moved from the personal computer to the *cloud*. Files are processed and stored on the *cloud,* which means that data is stored on remote servers physically. In these data there may be personal data. According to the current European and Croatian legal regulations, personal data must be handled with care, legally and in a technically correct way. Therefore, this diploma work gives an overview of the security and legal aspects of data protection in the *cloud* environment.

KEY WORDS: *cloud* environment; personal information; protection of personal data; security aspect of personal data protection; legal aspects of the protection of personal data

SADRŽAJ

1 UVOD 1

2 POVIJEST RAZVOJA RAČUNALNOG *CLOUDA* 2

2.1 Pregled računalnog *clouda* u 20. stoljeću 2

2.2 Pregled računalnog *clouda* u 20. stoljeću 3

3 OSNOVNE KARAKTERISTIKE *CLOUD* OKRUŽENJA 5

3.1 Pet ključnih karakteristika *cloud* okruženja 5

3.1.1 Široki mrežni pristup 5

3.1.2 Brza elastičnost 6

3.1.3 Odmjerena usluga 6

3.1.4 Usluga na zahtjev 7

3.1.5 Udruživanje resursa 8

3.2 Izvedbe *cloud* okruženja 8

3.2.1 Javni oblak 9

3.2.2 Privatni oblak 10

3.2.3 Zajednički oblak 10

3.2.4 Hibridni oblak 11

4 SERVISNI MODELI U RAČUNALNOM *CLOUDU* 13

4.1 Servisni model: Infrastruktura kao usluga 13

4.2 Servisni model: Platforma kao usluga 15

4.3 Servisni model: Softver kao usluga 16

5 ULOGA STANDARDIZACIJE U *CLOUD* OKRUŽENJU 18

5.1 *Cloud* standardi 19

5.2 Certificiranje 20

5.3 *Cloud Security Standards Guidance* 21

5.3.1 Provjera djelotvornog upravljanja, postojanje rizika i sukladnost procesa 21

5.3.2 Operativna revizija i poslovni procesi 23
6 REGULATORNE I STANDARDIZACIJSKE ORGANIZACIJE KAO DONOSITELJI PROPISA U *CLOUDU* 25
6.1 ISACA 25
6.2 *Cloud Security Alliance* 25
6.3 *Distributed Management Task Force* 26
6.4 *Open Commons Consortium* 26
6.5 *Open Grid Forum* 27
6.6 *The Object Management Group* i *The Cloud Standards Customer Council* 27
7 USVAJANJE ISO STANDARDA I PREPORUKA U *CLOUD* POSLOVANJU 29
8 EUROPSKI ZAKON O ZAŠTITI PODATAKA NA *CLOUDU* 31
8.1 Europske Direktive 31
8.2 Uredba Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka 33
8.3 Hrvatsko zakonodavstvo 35
9 „*SAFE HARBOR*“ SIGURNOSNA NAČELA KAO DOGOVOR IZMEĐU EUROPSKE UNIJE I SJEDINJENIH AMERIČKIH DRŽAVA 39
9.1 Odluka Suda Europske unije 40
9.2 Donošenje novog sporazuma između Europske unije i Sjedinjenih Američkih Država 41
10 SIGURNOSNI RIZICI I OPASNOST U *CLOUDU* 42
10.1 Korisnički sadržaj pohranjen i procesiran u *cloudu* 42
10.2 Vlasništvo nad podacima generiranim izvan *clouda* 44
10.3 Osnovni rizici i sigurnost u *cloudu* 47
10.4 Kriptografija kao mjera zaštite *clouda* 47
10.5 Brisanje podataka u *cloudu* 49
10.6 Osiguranje adekvatne zaštite podataka i informacija 49

10.7 Osiguranje kao sredstvo za upravljanje rizikom unutar *clouda* 51
10.8 Provođenje politike privatnosti 52
10.9 Osiguranje *cloud* mreže i sigurnosnih konekcija 53
10.10 Upravljanje sigurnosnim uvjetima u *cloudu* posredstvom SLA ugovora 55
10.11 Odlazak korisnika iz *cloud* okruženja i prekid ugovora 57
11 EKONOMSKI UČINAK U *CLOUD* POSLOVANJU 59
11.1 Statistika uporabe Interneta za privatne korisnike 59
11.2 Statistika uporabe *cloud* okruženja za poslovne korisnike 62
11.3 Ekonomski aspekti *cloud* poslovanja 64
11.3.1 Koristi i rizik *cloud* okruženja 65
11.3.2 Provjera mogućnosti uvođenja *cloud* okruženja u organizaciju 66
11.3.3 Prikaz različitih cijena za neke davatelje *cloud* usluga 67
12 ZAKLJUČAK 69
POPIS LITERATURE 70
POPIS AKRONIMA I KRATICA 78
POPIS STRANIH IZRAZA 80
POPIS ILUSTRACIJA 84
Popis slika 84
Popis tablica 84
Popis grafikona 84

1 UVOD

Računalni *cloud* ili oblak predstavlja isporuku računalnih usluga preko Interneta. Oblak usluge omogućuje pojedincima i tvrtkama da koriste softver zajedno s hardverom kojim se upravlja od strane trećih entiteta na udaljenim lokacijama. Primjeri *cloud* usluge su mrežna pohrana datoteka, društvene mreže, webmail i aplikacije u svrhu mrežnog poslovanja.

Korisnici *clouda* pristupaju cloudu najčešće putem web aplikacija, odnosno putem web-preglednika. Isto tako većina davatelja usluga *clouda* omogućuje preuzimanje aplikacija te korištenje *clouda* putem inicijalnog sučelja uređaja kako bi korisniku bilo što praktičnije upravljati podacima na udaljenoj lokaciji (*cloudu*). Upravo zbog svoje fleksibilnosti pristupa, *cloudu* je moguće pristupiti s bilo kojeg uređaja: pametnog terminalnog uređaja (engl. *Smartphone*), računala, prijenosnog računala, tableta i sl. Različiti modeli računalnog *clouda* koji će temeljito biti obrađeni u nastavku, omogućuju pristup informacijama i različitim računalnim izvorima s bilo kojeg mjesta na svijetu uz uvjet da postoji Internet veza. Ovisno o potrebama organizacije, krajnjeg korisnika odabire se prikladan model koji će udovoljiti obujmu posla i zahtjevima korisnika *clouda*.

Kako računalni *cloud* sve više privlači pozornost od strane korisnika a i medija, postavlja se niz pitanja o sigurnosti takvih sustava tj. o načinu zaštite osobnih podataka te provođenju niza standarda u svrhu sprječavanja moguće krađe, uništavanja i zlouporabe korisničkih podataka. Zakoni koji se apliciraju na *cloud* doneseni su u više od 90 zemalja svijeta kako bi se reguliralo procesiranje osobnih podataka unutar *clouda*. Neuspjeh u zaštiti *clouda* na odgovarajući način rezultira visokim cijenama i gubitku poslovanja i na taj način eliminira svaku potencijalnu korist računalnog *clouda*. Postoji niz standardizacijskih organizacija koji se bave *cloud* okruženjem. Svaka od navedenih organizacija (opisane u nastavku) ima svoje područje djelovanja tj. donosi standarde za točno određena područja (ekonomija, ekologija, napredne tehnologije itd.)

Uz standardizacijske, sigurnosne, pravne i tehničke probleme koji se nameću pred *cloudom*, analizirat će se i ekonomski aspekt *cloud* poslovanja. Tri osnovna elementa čine ekonomsku stranu *clouda*, a to su: cijena, prednosti i nedostaci *clouda* i provjera mogućnosti uvođenja *clouda* u organizaciju.

2 POVIJEST RAZVOJA RAČUNALNOG *CLOUDA*

Računalni *cloud* evoluirao je kroz nekoliko faza koje uključuju mrežu (engl. *Grid computing*[1]), utilitarno računarstvo (engl. *Utility computing*[2]), pružanje usluge za primjenu (akronim: ASP[3]) i softver kao usluga (akronim: SaaS[4]).

2.1 Pregled računalnog *clouda* u 20. stoljeću

Ideja o "međugalaktičkoj računalnoj mreži" uvedena je šezdesetih godina prošlog stoljeća na prijedlog J.C.R. Licklidera, koji je bio zadužen za omogućavanje razvoja ARPANET-a (engl. *Advanced Research Projects Agency Network*[5]), 1969. godine. Ideja je bila ljudima omogućiti međusobni pristup programima i podacima s bilo koje lokacije neovisno o mjestu stanovanja, objasnio je Margaret Lewis, direktor marketinške proizvodnje AMD-a. Drugi stručnjaci pripisuju koncept računalnog *clouda* znanstveniku Johnu McCarthyju, koji je predložio ideju da se općenito računalstvo isporučuje kao potreba od koje će ljudi imati koristi. Takva ideja bila je koncipirana na uredskim uslugama koje datiraju još od šezdesetih godina prošlog stoljeća.

Od šezdesetih godina pa nadalje, *cloud* se razvijao postepeno s dolaskom sve novijih tehnologija. Iako je tada sve bilo u začetnoj fazi polako se izgrađivao koncept *clouda.* Postepeno se počeo razvijati WEB 2.0[6], no glavna prepreka u razvoju takvog *clouda* bile su skromne brzine Interneta koje nisu omogućavale razvoj takvog koncepta i predstavljanje proizvoda javnosti.

Jedan od prvih trenutaka u povijesti kada je *cloud* postepeno počeo dolaziti do izražaja bio je dolazak *Salesforce.com* 1999. godine, koji je razvio koncept isporuke poslovnih aplikacija putem jednostavne web stranice. Zahvaljujući stvaranju pogodne arhitekture za isporuku

---

1 *Grid computing* je distribuirana arhitektura velikog broja računala čija je svrha rješavanje kompleksnih problema.

2 *Utility computing* je usluga putem koje davatelj usluga dodjeljuje računalne resurse po potrebi klijentu. Isto tako omogućuje njeno upravljanje.

3 ASP *cloud* predstavlja entitet treće strane koji upravlja i distribuira različite servise krajnjem korisniku iz centralnog servera preko mreže širokog područja.

4 SaaS *cloud* model je softversko distribucijski model u kojem davatelj omogućuje usluge i distribuira ih korisnicima preko Interneta.

5 ARPANET je prva mreža temeljna na komutaciji paketa i TCP/IP protokolu.

6 WEB 2.0 opisuje web stranice te ističe njihov sadržaj, iskoristivost i interoperabilnost.

aplikacija, specijalizirane tvrtke za izradu aplikacija iskoristile su prvu pravu priliku za lansiranje svojih usluga na tržište [1].

2.2 Pregled računalnog *clouda* u 20. stoljeću

Ulazak u novo tisućljeće, znači i nove novitete na računalnoj sceni, što je impliciralo brži razvoj *clouda* i ojačavanje njegove pozicije na tržištu. Internet je polako postao dostupan svima po prihvatljivoj cijeni što je dovelo do optimizma u razvoju *clouda*.

Sljedeći korak u razvoju bili su *Amazon Web Servisi*, 2002. god., koji su pružali čitav niz usluga baziranih na *cloudu*, uključujući skladištenje, računanje te upotreba ljudske inteligencije kroz *Amazon Mechanical Turk*[7]. Početkom 2006. god., Amazon je lansirao svoj *Elastic Compute Cloud* (akronim: EC2)[8] kao komercijalni web servis koji omogućava malim tvrtkama i pojedincima iznajmljivanje računala na kojemu se pokreću vlastite računalne aplikacije. Prema Jeremyju Allaireu, predsjedniku Uprave tvrtke Brightcove Amazon EC2/S3 to je bila prva široka dostupna usluga koja se temeljila na *cloud* infrastrukturi. Još jedna velika prekretnica došla je 2009. godine, kada je Web 2.0 postigao svoj zamah, a Google i drugi počeli su nuditi pretraživačko-bazirane (engl. *Browser-based*) poslovne aplikacije (primjer su Google aplikacije).

Prema Danu Germainu, glavnom tehnološkom direktoru tvrtke IT CobWeb Solutions, najvažniji doprinos *cloudu* omogućio je nastanak "aplikacija ubojica" (engl. Killer apps), koje su stvorili vodeći tehnološki divovi popu Microsofta i Googlea. Početkom pružanja usluga na pouzdan i jednostavan način, cjelokupna paradigma web usluga se počinje mijenjati [1].

Drugi ključni čimbenici koji su omogućili razvoj *clouda* uključuju sazrijevanje virtualne tehnologije, razvoj velikih brzina propusnosti (engl. *Bandwidth*) i univerzalnih standarda za omogućavanje interoperabilnosti između softvera, rekao je pionir *clouda* Jamie Turner [2].

Prema Andreasu Asanderu, zamjeniku ravnatelja tvrtke za upravljanje proizvodima virtualizacijom – Clavister, nakon što se riješe svi sigurnosni problemi vezani za *cloud* usluge, one mogu omogućiti korisnicima proširenje infrastrukture, preuzimanje kapaciteta na zahtjev

[7] Mechanical Turk je Amazonova platforma koja omogućuje rad korisniku na različitim područjima.
[8] *Elastic Compute Cloud* (EC2) je centralni dio računalnog *clouda* u Amazonu.

ili *outsourcanje* cjelokupne infrastrukture. Posljedica navedenih aktivnosti su pozitivno proširenje računalnih resursa i značajne ekonomske uštede [3].

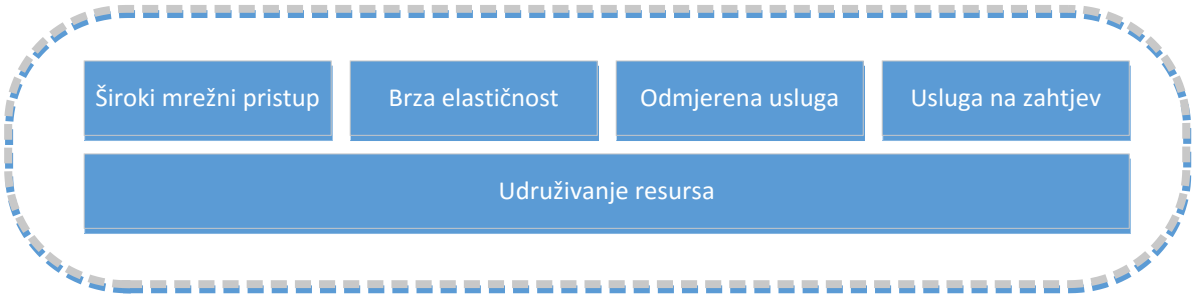
Danas, većina IT profesionalaca prepoznaje prednosti *cloud* ponude u smislu povećanog skladištenja, fleksibilnosti i smanjenja troškova. Glavni problem današnjeg *clouda* je kako zaštiti podatke krajnjeg korisnika odnosno kako zadovoljiti njegove potrebe. Navedeni stručnjaci slažu se da će konstantan napredak *clouda* u konačnici transformirati današnji računalni krajolik.

3 OSNOVNE KARAKTERISTIKE *CLOUD* OKRUŽENJA

Koristeći se tehničkim rječnikom, *cloud* predstavlja uređenje gdje su računalni resursi omogućeni na fleksibilnoj i lokacijsko neovisnoj bazi, koja omogućuje brzu dodjelu resursa, po potrebi. Dodjela *cloud* resursa ovisi o kompleksnim višeslojnim aranžmanima između različitih opskrbljivača.

3.1 Pet ključnih karakteristika *cloud* okruženja

U *cloud* okruženju razlikuje se pet ključnih karakteristika. Te karakteristike prikazuju odnos i razlike između *cloud* okruženja i tradicionalnog načina pristupa računalstvu. Pet ključnih karakteristika *cloud* okruženja prikazano je slikom 1.



Slika 1. Prikaz ključnih karakteristika *cloud* okruženja
izvor: [4]

Kao što je vidljivo sa slike 1. pet ključnih karakteristika *cloud* okruženja su [4]:

- Široki mrežni pristup;
- Brza elastičnost;
- Odmjerena usluga;
- Usluga na zahtjev;
- Udruživanje resursa.

3.1.1 Široki mrežni pristup

Široki mrežni pristup (engl. *Broad network access*) predstavlja mogućnosti dostupne putem mreže kojima se pristupa koristeći standardne mehanizme. Ti mehanizmi promoviraju

heterogenu uporabu „tankih“ i/ili „bogatijih“ klijentskih platformi. Primjer tih platformi predstavljaju: pametni mobilni terminalni uređaji, prijenosna računala (laptopi) i PDA uređaji[9], ali i tradicionalne programske usluge temeljene na *cloudu*. Navedeno je blisko Microsoftovoj strategiji, u kojoj je osnovna ideja da se svaki uređaj, kojeg korisnik posjeduje, može povezati na *cloud* sustav, s bilo koje lokacije, u bilo koje vrijeme [4].

3.1.2 Brza elastičnost

Brza elastičnost (engl. *Rapid elasticity*) podrazumijeva ubrzano i elastično pokretanje korisničkih mogućnosti, od strane *cloud* okruženja. U nekim slučajevima, brza elastičnost podrazumijeva i samostalno, odnosno automatsko pokretanje mogućnosti. Tada se, po potrebi, ostvaruje proporcionalno povećanje ili smanjivanje mogućnosti kada one nisu potrebne. Krajnjem korisniku ove mogućnosti izgledaju kao neograničene i dostupne u svako vrijeme. Primjer toga je Amazon EC2 [4].

3.1.3 Odmjerena usluga

Cloud okruženje ima karakteristiku odmjerene usluge (engl. *Measured service*) zato što sustavi u *cloud* okruženju automatski provjeravaju i optimiziraju uporabu resursa. Uporaba resursa optimizira se utjecajem na mjerenje sposobnosti apstrakcije prikladne potrebnom tipu usluge. Na primjer, navedeno se odnosi na: pohranu podataka, širinu pojasa i aktivni korisnički račun. Uporaba resursa se konstantno može pratiti i provjeravati. O njoj se mogu raditi izvješća, koja davateljima usluge i korisnicima pružaju transparentan uvid u uporabu. Poslužitelji (engl. *Servers*) u c*loud* okruženju se često koriste zajedno s virtualizacijskim tehnologijama ali ne postoje zahtjevi koji usko povezuju virtualizacijsku tehnologiju i apstrakciju sredstava. Sukladno tome, u puno ponuda, virtualizacija operacijskih sustava se ne koristi [4].

[9] PDA uređaji (engl. *Personal Digital Assistant*) predstavlja samostalni uređaj koji najčešće služi za upravljanje određenim informacijama. Primjer tih informacija mogu biti informacije vezane uz: kalendar, adresar, podsjetnik i slično.

3.1.4 Usluga na zahtjev

Usluga na zahtjev korisnika (engl. *On-demand self-service*) označava karakteristiku *cloud* okruženja u kojoj korisnik može samostalno odabrati i pokrenuti određene računalne resurse. Sukladno navedenom, korisnik može birati vrijeme posluživanja i mrežni prostor za pohranu podataka, bez potrebe za interakcijom s djelatnicima određenog davatelja *cloud* usluge. Danas većina poslužitelja svoje usluge temelji na pristupu u kojem korisnici plaćaju usluge ovisno o vremenu i obujmu korištenja.

Navedena karakteristika *cloud* okruženja pomaže u podržavanju izvedbenih i kapacitivnih aspekata objekata, koji ovise o razni usluge. Ova karakteristika organizacijama, kao korisnicima, omogućuje stvaranje elastične okoline, koja se povećava i smanjuje ovisno o radnim uvjetima i ciljanim performansama. Ovakav način plaćanja resursa, „plati po korištenju“, može se smatrati kao plaćanje zakupa opreme, kojem se visina cijene određuje temeljem: količine unajmljene opreme, vremenom trajanja unajmljena i uslugama koje su unajmljene.

Ključ navedene karakteristike predstavlja virtualizacija. Organizacije koje koriste *cloud* okruženje prepoznaju kako im virtualizacija omogućava brzo i jednostavno stvaranje kopija postojećih okolina, uključujući ponekad više virtualnih strojeva (engl. *Virtual machine*), kako bi se podržala ispitivanja, razvoj i pohrana aktivnosti. Trošak navedenih okolina je malen, zato što one postoje na istom poslužitelju kao i proizvodna okolina.

Također, nove aplikacije se razvijaju i rasprostiru u novim virtualnim strojevima na postojećim fizičkim poslužiteljima. Ti poslužitelji otvoreni su za uporabu preko Interneta. Aplikacije mogu biti skalirane u slučaju da su uspješne na tržištu.

Mogućnost korištenja i plaćanja samo onih resursa koji su korišteni prebacuje rizik na odnos: koliko je potrebno zakupiti infrastrukture od organizacije koja razvija aplikaciju na davateljima usluga u *cloud* okruženju. Osim toga, ova mogućnost pomiče odgovornost za arhitekturalne odluke s arhitekta aplikacije na razvojne inženjere. Ovi pomaci odgovornosti mogu povećati rizike [4].

3.1.5 Udruživanje resursa

Karakteristika udruživanja resursa (engl. *Resource pooling*) označava spajanje računalnih resursa pružatelja usluga, kako bi se poslužili svi korisnici, koristeći model s više zakupljenih jedinica (engl. *Multi-Tenant model*). Kod navedenog modela postoje različiti fizički i virtualni resursi koji se dinamički dodjeljuju i uklanjaju ovisno o zahtjevima korisnika. Korisnik uobičajeno nema nadzor i znanje o točnoj fizičkoj lokaciji uporabljenih resursa. Međutim, korisnik može odrediti mjesto na većoj razini apstrakcije, primjerice fizičku lokaciju države. Primjeri resursa uključuju: mrežni prostor, procesore, memoriju, mrežnu propusnost i virtualne strojeve [4].

3.2 Izvedbe *cloud* okruženja

Cloud okruženje, neovisno o svojim modelima (koji su opisani u poglavlju 4.) izvodi se u četiri različita načina provođenja *cloud computing* usluga. Ti načini izvedeni su ovisno o specifičnim potrebama. Načini su [4]:

- Javni oblak;
- Privatni oblak;
- Zajednički oblak;
- Hibridni oblak.

Osnovne usporedbe izvedbi *cloud* okruženja prikazane su tablicom 1.

Tablica 1. Osnovne razlike različitih izvedbi *cloud* okruženja

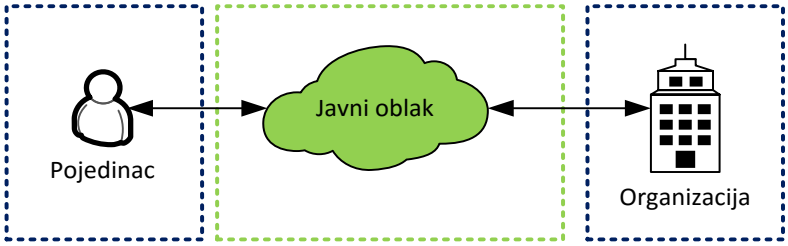
		Javni oblak	Privatni oblak	Zajednički oblak	Hibridni oblak
Mogućnost korištenja	Pojedinci	da	da	ne	ne
	Organizacije	da	da (samo 1)	da	da
Vlasnik		davatelj usluge	organizacija ili davatelj usluge	organizacija ili davatelj usluge	organizacija ili davatelj usluge
Upravljanje		organizacija ili davatelj usluge	organizacija ili davatelj usluge	organizacija ili davatelj usluge	organizacija ili davatelj usluge

izvor: [4]

U nastavku diplomskog rada detaljnije se opisuje svaka od prethodno nabrojanih i ukratko prikazanih u tablici 1., izvedbi *cloud* okruženja.

3.2.1 Javni oblak

Javni oblak, prikazan slikom 2., (engl. *Public cloud*) izvedba je *cloud* okruženja u kojoj je platforma dostupna i otvorena za javnost neovisno o tome radi li se o pojedincima ili organizacijama. *Cloud* je u vlasništvu tvrtke koja prodaje usluge *clouda*. U slučaju javnih platformi javlja se pitanje sigurnosti vlastitih podataka.



Slika 2. Javni oblak
izvor: [4]

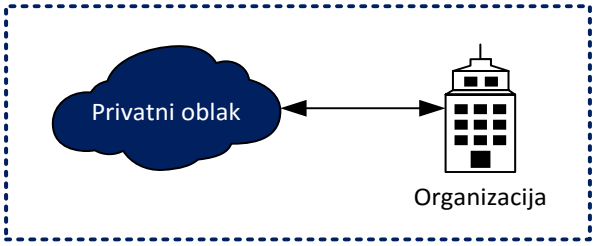
Aplikacije različitih korisnika često se nalaze na istim poslužiteljima, sustavima za pohranjivanje i mrežama. Javni oblaci smanjuju sigurnosne rizike i troškove pružanjem promjenjive infrastrukture.

Ako je *cloud* realiziran s naglaskom na izvedbu, sigurnost i položaj podataka, druge aplikacije koje su pokrenute na *cloudu* ne bi trebale stvarati probleme vezane uz arhitekturu sustava *clouda* i probleme krajnjim korisnicima. Jedna od prednosti javnih oblaka jest veličina u odnosu na privatne oblake odnosno, javni oblaci mogu biti veći nego privatni oblaci. Također, javni oblaci nude mogućnost povećavanja ili smanjivanja zakupljenog dijela i prebacivanja odgovornosti s organizacije na davatelja usluge.

Dijelovi javnog oblaka mogu biti isključivo pod uporabom samo jednog korisnika. Tada ti dijelovi čine privatni podatkovni centar (engl. *Datacenter*). Zauzimanje slika virtualnih strojeva (engl. *Virtual machine images*) u javnom oblaku ne daje korisnicima potpuni uvid u infrastrukturu oblaka, dok zakupljivanjem podatkovnih centara korisnici dobiju potpuni uvid u infrastrukturu. Tada mogu upravljati i poslužiteljima, sustavima pohrane, mrežnim uređajima i mrežnim topologijama. Stvaranjem privatnog virtualnog podatkovnog centra smanjuje se problem postojanja većeg broja različitih lokacija, čime se povećava brzina prijenosa prilikom povezivanja objekata unutar istog oblaka [4].

3.2.2 Privatni oblak

Privatni oblak, prikazan slikom 3., (engl. *Private cloud*) je izvedba *cloud* okruženja u kojoj je infrastruktura dostupna samo jednoj organizaciji. U toj izvedbi oblakom upravlja sama organizacija ili davatelj usluge. Privatni oblak se koristi kada je potreban veći nadzor nad podacima, nego što postoji u javnom oblaku.



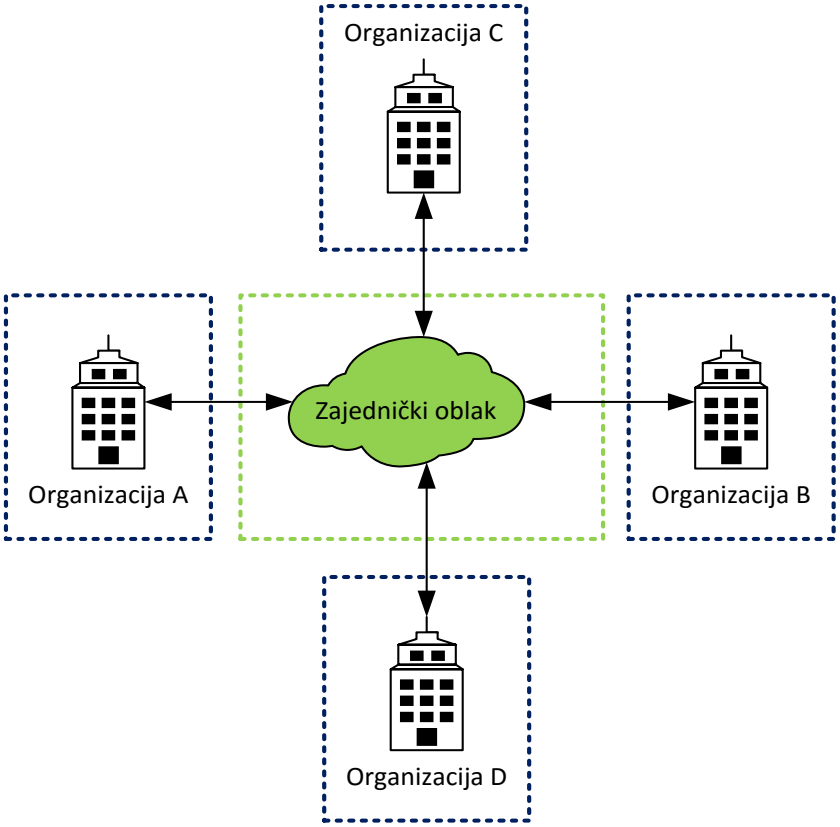
Slika 3. Privatni oblak
izvor: [4]

Privatni oblaci napravljeni su isključivo za jednog klijenta. Oni tom klijentu pružaju najveći nadzor nad podacima i jamče sigurnost imovine pohranjene na *cloudu*. Organizacija posjeduje infrastrukturu i ima nadzor nad raspodjelom aplikacija na vlastitoj infrastrukturi. Privatni oblaci mogu biti raspoređeni unutar organizacijskog podatkovnog centra.

Organizacije koje posjeduju privatni oblak na njemu instaliraju programe, aplikacije, pohranjuju podatke i upravljaju strukturom *clouda*. Privatni oblaci pružaju organizacijama visoku razinu nadzora nad korištenim resursima, zato što korištenjem privatnog oblaka organizacije imaju potrebne vještine i mogućnosti za uspostavljanje i upravljanje okolinom. Izgradnjom privatnih oblaka i njihovim upravljanjem najčešće se bave IT službe organizacija ili davatelji usluga [4].

3.2.3 Zajednički oblak

Kod zajedničkog oblaka (engl. *Community cloud*) nekoliko organizacija dijeli strukturu oblaka. Zajednički oblak prikazan je slikom 4.

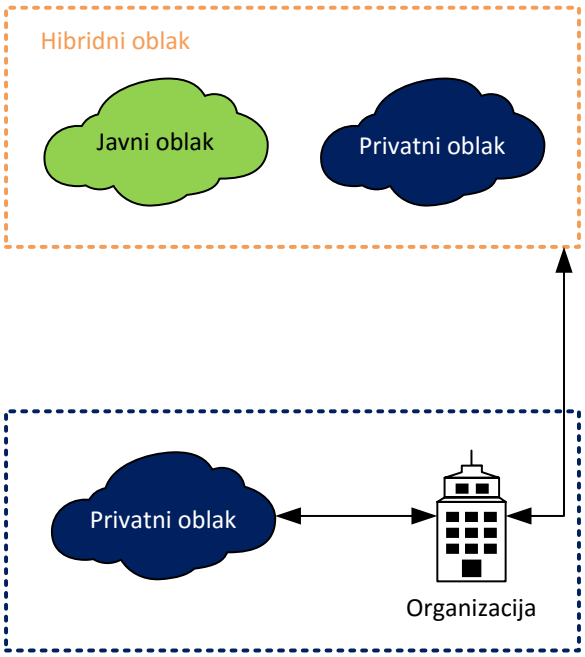


Slika 4. Zajednički oblak
izvor: [4]

Infrastruktura kod zajedničkog oblaka podržava posebne zajednice. Te zajednice imaju zajedničke: potrebe, misije zahtjeve sigurnosti i slično. Tim zajednicama upravljaju same organizacije ili netko drugi, odnosno davatelj usluga *clouda* [4].

3.2.4 Hibridni oblak

Izvedbu hibridnog oblaka, prikazana slikom 5., (engl. *Hybrid cloud*) čine dva ili više različitih oblaka koji tada predstavljaju jedinstvenu cjelinu. Međusobno su povezani standardiziranim ili prikladnim tehnologijama koje omogućuju efikasan prijenos podataka.



Slika 5. Hibridni oblak
izvor: [4]

Hibridni oblaci služe povezivanju javnih i privatnih modela oblaka. Mogućnost proširivanja privatnog oblaka s javim oblakom može se koristiti za održavanje uslužnih razina, zbog lakšeg izdržavanja velikih opterećenja. Navedeno se najčešće može primijetiti kod pohrane podataka vezanih uz Web 2.0 aplikacije. Također, hibridni oblak se može koristiti za upravljanje planiranim velikim opterećenjima. Isto tako, hibridni oblak može se koristiti za izvođenje periodičkih zadataka. Tada se zadaci rasporede na javne oblake.

Hibridni oblaci susreću se sa složenošću određivanja raspodijele aplikacija po javnom i privatnom oblaku. Također, u hibridnim oblacima javlja se problem odnosa podataka i obrade resursa. Kod malih podataka ili kada aplikacije ne pamte stanja, hibridni oblaci mogu biti bolje rješenje od prepisivanja velike količine podataka u javni oblak [4].

4 SERVISNI MODELI U RAČUNALNOM *CLOUDU*

Zbog mogućih permutacija, ali i aktivnosti, u *cloud* okruženju, *cloud* se najčešće svrstava u sljedeće tri kategorije, koje se zbog početnih slova imena često nazivaju i SPI model [4], odnosno tri servisa (čije su razlike u upravljanju prikazane tablicom 2.):

- Infrastruktura kao usluga (engl. *Infrastructure as a service*, IaaS);
- Platforma kao usluga (engl. *Platform as a service*, PaaS);
- Softver kao usluga (engl. Software as a service, SaaS).

Tablica 2. *Cloud* servisni modeli

Klasični model	Infrastruktura kao usluga	Platforma kao usluga	Softver kao usluga
Aplikacije	Aplikacije	Aplikacije	Aplikacije
Podaci	Podaci	Podaci	Podaci
Izvorišno okruženje	Izvorišno okruženje	Izvorišno okruženje	Izvorišno okruženje
Srednji sloj	Srednji sloj	Srednji sloj	Srednji sloj
O/S	O/S	O/S	O/S
Virtualizacija	Virtualizacija	Virtualizacija	Virtualizacija
Serveri	Serveri	Serveri	Serveri
Pohrana	Pohrana	Pohrana	Pohrana
Mreža	Mreža	Mreža	Mreža

izvor: [5]

Iz tablice 2. vidljiva je najbitnija razlika između svakog servisnog modela, a ona je način upravljanja. Prema klasičnom modelu korisnik upravlja svim elementima (zlatna boja). Kod IaaS modela, korisnik upravlja: aplikacijama, podacima, izvorišnim okruženjem, srednjim slojem i O/S-om, dok davatelj usluge upravlja virtualizacijom, serverima, pohranom i mrežom (narančasta boja). Kod PaaS modela, korisnik upravlja samo aplikacijom i podacima, dok svime ostalim upravlja davatelj usluge. U SaaS modelu, korisnik ne upravlja niti jednim elementom, već svim elementima upravlja davatelj usluge. Kod ovog modela korisnik samo koristi mogućnosti *cloud* okruženja, bez ikakvog utjecaja na njih.

4.1 Servisni model: Infrastruktura kao usluga

Infrastruktura kao usluga (IaaS) je način isporuke infrastrukture računalnog *clouda* - poslužitelja, pohrane podataka, mreže i operativnih sustava, kao usluga na zahtjev. Umjesto

kupnje poslužitelja, različitih softvera, prostora podataka ili mrežne opreme, klijenti imaju mogućnost kupovine isključivo onih resursa koji su njima potrebni.

Općenito IaaS mogu će je ostvariti tj. dobiti kao javnu ili privatnu infrastrukturu ili kombinacijom tih dviju infrastruktura. Javni oblak infrastruktura prednjači jer se sastoji od zajedničkih resursa te je dostupan cjelokupnoj Internet publici. Primjer takvog modela može se razmatrati kroz organizaciju koja posjeduje privatni *cloud* koji procesira svoje aktivnosti javnom *cloudu* za potrebe balansiranje opterećenja podataka u razdobljima kada se ostvaruju enormni zahtjevi ka privatnom *cloudu* [6].

Glavne karakteristike SaaS-a su [6]:

- Distribucija resursa kao usluge;
- omogućavanje dinamičkog skaliranja;
- Posjeduje varijabilni trošak, uslužni model cijena;
- Općenito uključuje više korisnika na jednom djelu hardvera (servera).

Primjena IaaS-a najbolje se može vidjeti u puno primjera koji su povezani s koristima koje donosi računalni *cloud*. Situacije koje su posebno prikladne za ovu računalnu infrastrukturu su [6]:

- Kada je potražnja vrlo nepostojana (engl. Volatile) - u svako vrijeme postoji velik broj zahtjeva prema serveru tj. potražnja za resursima je izričito velika;
- Za nove organizacije koje ne posjeduju dovoljni kapital kojeg bi uložile u kupovinu servera i pripadajućih tehnologija za pokretanje istih;
- Gdje organizacija ubrzano raste i skaliranje tj. nabava hardvera predstavlja veliki problem;
- Gdje postoje specifični poslovni zahtjevi, probni ili kratkotrajna potreba za korištenjem infrastrukture za pohranu podataka.

Dok IaaS pruža ogromne prednosti za situacije u kojima skalabilnost i brza rezervacija predstavljaju iznimnu korist, postoje situacije koje nisu prikladne za ovu infrastrukturu [6]:

- Gdje regulatorna usklađenost čini izvoz podataka (engl. *Outsourcing*), pohranu i obradu zahtjevnom;
- Gdje su potrebni najviši nivoi performansa i gdje posvećena infrastruktura posjeduje kapacitet koji udovoljava zahtjevima velikih kompanija/organizacija.

4.2 Servisni model: Platforma kao usluga

PaaS se može definirati kao računalna platforma koja omogućuje stvaranje web aplikacija brzo i lako bez potrebe ostalih aktivnosti poput kupnje i održavanja softvera kao i infrastrukture. umjesto da se softver isporučuje preko *weba*, PaaS predstavlja platformu za stvaranje softvera za isporuku preko *weba*.

PaaS olakšava implementaciju aplikacija bez velikih troškova i složenosti kupovanja i upravljanja sklopovljem i programima. Pruža sve što je potrebno kako bi cijeli sustav izgradnje i isporuke aplikacija i usluga u cijelosti bio dostupan putem interneta. PaaS ponuda uključuje alate za dizajn aplikacija, testiranje, implementaciju te poslužiteljske funkcionalnosti. Nudi i aplikacijske usluge kao što su timska suradnja, integracija baze podataka, sigurnost, skalabilnost, skladištenje i sl. [7].

Karakteristike ovog modela su [8]:

- Radni okvir;
- Apstrakcija;
- Automatizacija;
- *Cloud* servisi.

Radni okvir izvršava računalni kod od strane krajnjeg korisnika prema načelima programa postavljenima od strane vlasnika programa i pružatelja *cloud* usluge. PaaS radni okvir dolazi u puno varijanti. Neke varijante baziraju se na tradicionalnim radnim okvirima, dok se druge baziraju na 4GL i vizualnim programskim konceptima.

PaaS se odlikuje višom razinom apstrakcije koju pruža. S IaaS, fokus je na tome da se pruža korisnicima "sirov" pristup fizičkoj ili virtualnoj infrastrukturi. Za razliku od toga, u PaaS, fokus se premješta na aplikacije koje *cloud* može i mora podržati. Dok za IaaS servisni model pruža korisniku hrpu virtualnih sučelja koji moraju biti konfigurirani i na kojem se aplikacije moraju pokrenuti, PaaS s druge strane pruža korisniku način za razvijanje svoje aplikacije u naizgled neograničenom prostoru računalnih resursa u kojemu se eliminira složenost implementacije i konfiguracije infrastrukture.

PaaS okruženje automatizira proces implementacije aplikacija za infrastrukturu i konfiguriranje komponente aplikacije. Osiguravanje i konfiguracija podržava tehnologiju poput ujednačavanja opterećenja i implementaciju baze podataka, te upravljanje promjenama sustava na temelju pravila postavljenih od strane korisnika.

Ponuda *cloud* servisa od strane PaaS-a pruža programerima i arhitektima usluge i API[10]-je koji pomažu u pojednostavljenju posla i isporuke rješenja visoko dostupnih *cloud* aplikacija. Ove *cloud* usluge pružaju široku paletu mogućnosti, te u puno slučajeva predstavljaju ključnu razliku među konkurentskim PaaS ponudama, [8].

4.3 Servisni model: Softver kao usluga

Softver kao usluga (SaaS), ponekad i pod nazivom i "softvera na zahtjev" je softver koji je raspoređen preko Interneta i/ili je angažiran za pokretanje iza vatrozida (engl. *Firewall*[11]) na lokalnoj mreži ili osobnom računalu. Koristeći SaaS servis, davatelj usluge licencira zahtjev za kupce kao uslugu na zahtjev kroz pretplatu u "*pay-as-you-go*" modelu ili bez naknade. Ovaj pristup za isporuku aplikacija je dio računalnog modela u kojemu se tehnologija nalazi u *cloudu* i pristupa joj se putem interneta kao servisu, [6].

[10] API (engl. *Application programming interface*) je set funkcija i procedura koje omogućuju kreaciju aplikacija koje imaju pristup značajkama, podacima operativnog sustava, aplikacije ili nekog drugog servisa.

[11] Vatrozid je mrežni sigurnosni sustav koji upravlja ulaznim i izlaznim mrežnim prometom zasnovanim na skupu primijenjenih pravila.

Ključne karakteristike SaaS servisa su [6]:

- Krajnji korisnik pristupa usluzi putem Interneta. Usluga se nalazi na udaljenoj lokaciji i za njeno održavanje brine se pripadajuća organizacija/tvrtka.
- Aktivnostima se upravlja iz središnje lokacije, što ne zahtijeva potrebu da se usluga održava za svakog korisnika/kupca pojedinačno.
- Organizacija vrši centralna ažuriranja, što olakšava krajnjim korisnicima upotrebu usluge jer ne trebaju istu ažurirati ako dođe do promjena već se ažuriranje izvršava automatski.
- Preuzeta aplikacija/usluga plaća se po preuzimanju usluge tj. njene količine. Dostupnost aplikacije moguća je s bilo koje lokacije koja ima internet pristup.
- Aplikacija se može jednostavno skalirati bez ikakvih problema za krajnjeg korisnika prilikom ažuriranje aplikacije od strane organizacije. Sigurnost i odgovornost spada u domenu organizacije. Ako dođe do narušavanja sigurnosti, organizacija u vlasništvu aplikacije uglavnom nudi alternativu za krajnjeg korisnika.

Kao i kod svakog servisa SaaS isto tako sadrži mane. Glavni nedostatak je taj što krajnji korisnik mora imati internet vezu odnosno ugovor sa svojim ISP-om[12] kako bi uopće mogao pristupiti sadržaju na serveru. Iako će se takav problem postepeno riješiti, puno kućanstava ne posjeduju internet vezu. Drugi bitni zaostatak predstavlja to što SaaS aplikacije nemaju iste značajke kao i aplikacije koje nisu dio SaaS modela. Još jedan problem predstavlja brzina pri korištenju SaaS aplikacija za razliku od aplikacija koja ne spadaju u SaaS ali su puno brže. Glavne tri mane pokušavaju se na što bolji način popraviti te se očekuje da će kroz nekoliko godina one biti u potpunosti zanemarive [6].

[12] ISP (engl. *Internet service provider*) predstavlja organizaciju koja omogućava servise kako bi krajnji korisnik imao pristup Internetu.

5 ULOGA STANDARDIZACIJE U *CLOUD* OKRUŽENJU

Uloga standardizacije u *cloud* okruženju je olakšati razvoj i postavljanje različitih ekonomskih, društvenih i ekoloških rješenja, koja se temelje na *cloud* okruženju. Proces standardizacije je važan zbog uspostavljanja svjetskog tržišta za usluge bazirane na *cloud* okruženju. Također, uloga standardizacije u *cloud* okruženju je voditi i podržavati inovacije i natjecanja između organizacija koje daju usluge u *cloud* okruženju te povećati broj učesnika u procesu stvaranja standarda, vezanih uz *cloud* okruženje.

Standardizacija u *cloud* okruženju postiže se različitim povjerenstvima (odborima), koja pokušavaju uravnotežiti javne i privatne razloge vezane za *cloud* okruženje. Članovi povjerenstava mogu predstavljati:

- Korisnike okruženja;
- Akademsku zajednicu;
- Davatelje usluga;
- Proizvođača opreme;
- Vladine organizacije.

Osim navedenih, članove povjerenstava mogu predstavljati i predstavnici političkih organizacija. Motivacija predstavnika u povjerenstvima za standardizaciju prikazana je tablicom 3.

Tablica 3. Motivacija članova u povjerenstvima za standardizaciju

Članovi povjerenstva	**Motivacija**
Proizvođači opreme	Definirati najbolju tehnologiju za korištenje *cloudu* okruženja
Davatelji usluge	Ostvarivanje organizacijskih ciljeva (profit, širenje organizacije i sl.)
Korisnici	Standardiziranje korisničkih zahtjeva
Državne institucije	Javni interes

izvor: [9]

Standardizacija se može odvijati u:

- Organizacijama;
- Industrijskim grupama (npr. konzorcijima);
- Državama;
- Regijama;
- Cijelom svijetu.

Točnije, standardizacija se odvija tamo gdje je geografski potrebna, odnosno gdje je pogodno tržište za odvijanje standardizacije. To znači, na primjer, kako određena organizacija može implementirati određenu lokalnu računalnu mrežu (engl. *Local area network*) i odrediti da se takva mreža mora implementirati u svim sastavnicama te organizacije, ali ne može to odrediti za cijeli svijet. Razmjerno, standardi *cloud* okruženja, kao i Internet standard, moraju biti doneseni i prihvaćeni na razini cijelog svijeta [9].

5.1 *Cloud* standardi

Model javnog *clouda* predstavlja velik izazov u pogledu zaštite podataka za krajnjeg korisnika. Kako krajnji korisnici neprestano procjenjuju sigurnosnu podršku svojih *cloud* servisa koje im omogućuju specifični davatelji usluga bitno je razumjeti i razlikovati različite vrste sigurnosnih standarda koje postoje. Najčešće vrste standarda su:

- Savjetodavni standardi;
- Sigurnosni okviri;
- Standardne specifikacije.

Savjetodavni standardi (engl. *Advisory standards*) su standardi koji se primjenjuju na sve vrste organizacija, neovisno o njihovoj veličini. Također su u skladu s informacijsko sigurnosnim rizicima s kojima se suočavaju. U praksi, takva fleksibilnost omogućuje korisnicima veliku širinu za usvajanje kontrole informacijske sigurnosti koje imaju smisla za njih, ali čini neprikladnom za relativno jednostavna testiranja usklađenosti u većini formalnih programa certificiranja.

Sigurnosni okviri (engl. *Security frameworks*) često se nazivaju i najboljom praksom. Takva vrsta standarda je pogodna za certifikaciju. Sigurnosni okviri definiraju specifičnu

politiku, kontrolu provjere i ostale postupke zajedno s postupcima za ispitivanja potpore, koja se može koristiti od strane revizora za procjenu i mjerenje usklađenosti pružatelja usluge.

Standardne specifikacije (engl. *Standards specification*) posebno definiraju API-je i komunikacijske protokole koji moraju biti implementirani kako bi se proveo zahtjev za standardnu podršku. U puno slučajeva, standardima je omogućeno proširivanje koje omogućuju provoditelji uključivanja funkcija koje nadilaze one definirane u standardu. Općenito, formalni certifikati nisu uvjet za ovu vrstu standarda iako testne mogućnosti/opcije sukladnosti i ispitivanja interoperabilnosti mogu biti dostupne [9].

5.2 Certificiranje

Certificiranje predstavlja bitan aspekt, kako bi korisnici *cloud* usluga procijenili kvalitetu *clouda* i naposljetku donijeli odluku o korištenju istoga. Certificiranje se učestalo provodi od treće strane, iako u nekim okolnostima moguće je samo certificiranje od strane davatelja usluga. Za certifikaciju, tipično revizori ispituju:

- Dokumentiranu politiku;
- Procedure;
- Arhitekturu davatelja *clouda*.

Na kraju, revizori naknadno ispituju poslovanje davatelja i provjeravaju urednost poslovanja davatelja usluge.

Certifikat daje jamstvo korisnicima *cloud* usluga koje se odnosi na ispunjavanje sigurnosnih zahtjeva koji se pred njima nameće. Stoga se preporučuje da korisnici *cloud* usluga prepoznaju ustaljene sigurnosne certifikate koji su važni za njihovu organizaciju i inzistiraju da davatelji *cloud* usluga predstave svoju sukladnost (engl. *Conformance*). Iako se sigurnosni certifikati računalnog *clouda* još uvijek pojavljuju, generalni certifikati koji već odavno postoje apliciraju se na *cloud* i strogo su preporučljivi da se koriste u *cloudu* [9].

5.3 *Cloud Security Standards Guidance*

Kako korisnici prenose svoje aplikacije i podatke na *cloud*, iznimno je bitno da je sigurnost njihovih aplikacija i podataka barem jednaka onoj sigurnosti koje su te aplikacije/podaci imali u tradicionalnom IT okruženju. Neuspjeh u zaštiti *clouda* na odgovarajući način rezultira visokim cijenama i potencijalnom gubitku poslovanja i tako eliminira svaku potencijalnu korist računalnog *clouda*.

CSCC "Sigurnost za *Cloud* u deset koraka kako bi osigurali uspjeh" predstavlja seriju koraka kojih bi se *cloud* korisnici trebali pridržavati kako bi na uspješan način upravljali svojim *cloud* okruženjem kojeg su rezervirali. Ovih deset koraka znatno ublažava rizik od nastanka mnogobrojnih neželjenih postupaka za korisnika tako da isporučuje adekvatne mjere zaštite i pravilnog načina razmišljanja unutar *clouda*. Tih deset koraka su [10]:

- Provjera djelotvornog upravljanja, postojanje rizika i sukladnost procesa;
- Operativna revizija i poslovni procesi;
- Upravljanje ljudima, uloge i identiteti;
- Osiguranje adekvatne zaštite podataka i informacija;
- Provođenje politike privatnosti;
- Procjena sigurnosnih odredbi za *cloud* aplikacije;
- Osiguranje *cloud* mreže i sigurnosnih konekcija;
- Procjena sigurnosnih kontrola na fizičkoj infrastrukturi i objektima;
- Upravljanje sigurnosnim uvjetima SLA *cloudu*;
- Razumijevanje sigurnosnih zahtjeva izlaznih procesa.

Kako se većina od prethodno navedenih koraka neposredno obrađuje u nastavku diplomskog rada, u ovom poglavlju će se obraditi koraci: Provjera djelotvornog upravljanja, postojanje rizika i sukladnost procesa i Operativna revizija i poslovni procesi.

5.3.1 Provjera djelotvornog upravljanja, postojanje rizika i sukladnost procesa

Standardi za podršku općim upravljanjem IT-em postoje već nekoliko godina i oni su u općoj upotrebi diljem svijeta. Ovi standardi upravljanja nisu specifični za *cloud*, ali su dovoljno općeniti, tako da se mogu primijeniti na upravljanje *cloud*.

U standarde za upravljanje *cloudom* uključuju se [10]:

- ISO 38500;
- COBIT;
- ITIL;
- Serija ISO 20000 normi.

COBIT je izrađen od strane ISACA organizacije i pruža okvir za upravljanje poslovanjem i upravljanjem IT-a. Pozicioniran je kao okvir visoke razine koji se nalazi između poslovnih ciljeva i procesa te IT ciljeva i procesa. COBIT se može koristiti u kombinaciji s detaljnijim standardima kao što su ISO 20000[13] i ISO 27000[14].

ITIL (engl. *Information Technology Infrastructure Library*) je skup praksi za upravljanje IT uslugama koje se pak mogu primijeniti za upravljanje *cloud* uslugama. Pokriveno je i upravljanje sigurnošću informacija, ali za područje informacijske sigurnosti pogodnije je i više se primjenjuje 27002 ISO standard.

ISO standardi bit će opisani u poglavlju 7.

Pored općih normi i okvira gore navedenih, postoje i druge norme koje imaju utjecaj: na neku državu, one koje se primjenjuju na regionalnoj razini ili pak one koje se odnose na određene industrije ili određene vrste podataka. Opisane norme su:

- HIPAA;
- PCI-DSS7;
- FedRAMP;
- FISMA.

HIPAA je standard koji se odnosi na upravljanje informacijama u zdravstvenom sektoru. Standard se prvenstveno primjenjuje u SAD-u.

PCI-DSS7 je standard koji se odnosi na sigurnost podataka prilikom plaćanja karticama. FedRAMP predstavlja američki vladin program, koji pruža:

[13] ISO 20000 je standard koji specificira zahtjeve za kvalitetnim upravljačkim sustavom unutar organizacije kako bi se demonstriralo konzistentno razvijanje kvalitetnih proizvoda koji udovoljavaju korisničkim zahtjevima.

[14] ISO 27000 je međunarodni standard koji objašnjava ulogu osiguravanja informacijsko sigurnosnog upravljanja.

- standardizirani pristup sigurnosnoj procjeni;
- autorizaciju;
- kontinuirano praćenje *cloud* proizvoda i usluga.

FISMA predstavlja američki savezni zakon koji postavlja sigurnosne zahtjeve za informacijama o saveznim agencijama.

Ako upravljanje IT-em od strane pružatelja *cloud* usluga predstavlja bitan faktor za klijente *cloud* usluge onda se korisnicima *clouda* savjetuje da se utvrdi je li pružatelj usluga *clouda* u skladu s jednim ili više od navedenih upravljačkih standarda. Od navedenih standarda (COBIT, SSAE 16, ISO/IEC 27000 serija ili ITIL) klijent treba od davatelja usluge tražiti one standarde pomoću kojih se može provjeriti kvaliteta *cloud* okruženja koja se nudi korisniku [10].

5.3.2 Operativna revizija i poslovni procesi

Korisnici *cloud* usluga moraju prvo provjeriti je li davatelj usluga *clouda* otvoren za revizore. Trebali bi postojati jasni uvjeti u ugovoru i/ili dogovornoj razini usluge koja se odnosi na *cloud*. Revizori moraju moći vršiti tekuće kontrole i imati pristup revizijskim tragovima u obliku povijesnih/arhivskih podataka (engl. *Log data*) za sustave koji su dostupni krajnjim korisnicima *clouda*.

Tipično, revizori prilikom rada koriste zahtjeve jednog od zajedničkih programa certificiranja ili standardizacije. Iz sigurnosnih kontrola, serija ISO 27000 široko je prihvaćena a njegova zrelost znači kako postoji niz certifikata na temelju njega – primjerice Cybertrust[15] certifikat, kojeg preferiraju davatelji usluga *clouda*. Za *cloud* usluge, koje imaju značajan utjecaj na financijske izvještaje krajnjih korisnika, *cloud* sustav mora zadovoljiti dugogodišnji SSAE 16 standard.

Osim vanjske revizije, postoji niz napora usmjerenih na pružanje standardnih mehanizma za *cloud* usluge klijentima kako bi samostalno upravljali i vršili vlastiti nadzor kao i reviziju svojih aplikacija i podataka koji su spremljeni u *cloudu*. Jedna od takvih inicijativa je DMTF *Cloud* federacija za reviziju podataka (CADF), standard koji podržava slanje i vraćanje

[15] CyberTrust certifikat je certifikat kojeg je izdavala CyberTrust organizacija u svrhu autentifikacije web servisa.

normativnih podataka i reviziju događaja iz oblaka usluga, u obliku prilagođenih izvješća i zapisnika koji se mogu dinamički generirati za *cloud* usluge krajnjim korisnicima koji koriste njihove kriterije. U ovom trenutku, implementacije CADF je nesigurna, ali podrška ovom standardu je planirana za buduća izdanja od strane OpenStacka[16] [10].

[16] OpenStack je besplatna *open source* softver platforma za računalni *cloud*. Sastavljena je od komponenta koje kontroliraju procesiranje podataka, pohranu podataka i mrežne resurse preko podatkovnog centra.

6 REGULATORNE I STANDARDIZACIJSKE ORGANIZACIJE KAO DONOSITELJI PROPISA U *CLOUDU*

Puno organizacija i neformalnih grupa fokusirano je na rješavanje pitanja vezanih za *cloud* okruženje. Standardizacijska tijela pomažu stvaranju i održavanju raznih standarda, vezanih za *cloud* okruženje, te stvaranju najbolje prakse, kako bi sustavi različitih davatelja usluga i proizvođača opreme mogli funkcionirati [11]. Ulogu regulatora u Republici Hrvatskoj ima Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM) [12], izuzev zaštite osobnih podataka. Ulogu zaštite osobnih podataka u Republici Hrvatskoj ima Agencija za zaštitu osobnih podataka (AZOP) [13].

6.1 ISACA

ISACA je neprofitna organizacija koja okuplja IT stručnjake. Nekada je ISACA predstavljala akronim za *Information Systems Audit nad Control Association*, međutim danas ISACA predstavlja akronim samo po sebi, bez značenja. Glavni cilj ISACA-e je postizanje individualnog i organizacijskog uspjeha za svakog IT stručnjaka.

Jedna od aktivnosti kojima se ISACA bavi je izdavanje smjernica vezanih uz informacijsku sigurnost. Te smjernice su rezultat aktivnih istraživanja. Osim smjernica, rezultat aktivnih istraživanja je i razvoj proizvoda, odnosno aplikacija, korisnih i IT i sigurnosnim stručnjacima.

ISACA je razvila i održava međunarodno priznate: COBIT, Val IT i Risk IT okvire, pomažući IT stručnjacima i poslovnim voditeljima da ispune svoje zakonodavne obveze, povećavajući vrijednost organizacije u kojoj rade [14], [15].

6.2 *Cloud Security Alliance*

Cloud Security Alliance (akronim: CSA) predstavlja svjetsku vodeću organizaciju za definiranje i podizanje svijesti o najboljim praksama za osiguravanje sigurnog *cloud* okruženja. CSA iskorištava znanja eksperata iz: industrije, vlade, korporacija, ali individualne članove, koji mogu svojim znanjem i iskustvom izraditi određeni dokument vezan uz sigurnost *cloud* okruženja. Od CSA aktivnosti, koristi imaju svi dionici na tržištu *cloud* okruženja: korisnici, davatelji usluga, državne institucije, poduzetnici i osiguravajuća industrija.

Prvi industrijski *cloud* sigurnosni certifikat CSA izdaje se 2010. godine. Naziv tog standarda je *Certificate of Cloud Security Knowledge* (akronim: CCSK), a predstavlja mjerilo za profesionalne kompetencije vezane za sigurnost u *cloud* okruženju. Također, CSA je razvio najpopularniji certifikacijski program za *cloud* sigurnost, *CSA Security Trust & Assurance Registry* (akronim: STAR) [16].

6.3 *Distributed Management Task Force*

Distributed Management Task Force (akronim: DMTF) je organizacija, koja se bavi razvojem industrijskih standarda, kako bi se pojednostavnila upravljivost računalnih i mrežnih komponenata u pojedinačnim organizacijama. DMTF definira i poboljšava standarde koji su međunarodno usvojeni, te podržava implementaciju koja omogućuje upravljanje i uključivanje tradicionalnih tehnologija, mreža i infrastrukture, s novim tehnologijama, *cloud* okruženjem i virtualizacijom.

DTMF standardi osiguravaju zajedničko upravljanje infrastrukturnim komponentama, za: instrumentaciju, kontrolu i komunikaciju, neovisno o platformi i tehnologijama. Sukladno, DTMF standard opisuje i način komunikacije između *cloud* okruženja i korisnika, odnosno između korisnika i *cloud* okruženja, posredstvom određenog terminalnog uređaja [17], [18].

6.4 *Open Commons Consortium*

Open Commons Consortium (akronim: OCC), prethodno *Open Cloud Consortium*, je neprofitna organizacija koja se bavi upravljanjem *cloud* okruženjem i podacima koji se nalaze u tom okruženju. Područja interesa OCC-a su: znanstvena, medicinska i ekološka istraživanja. Članovi OCC organizacije su većinom zaposlenici u tridesetak različitih: sveučilišta, privatnih kompanija, državnih agencija i laboratorija. OCC radi tako da je organiziran u male skupine [19].

Jedna od tih malih skupina je i *The Open Science Data Cloud Working Group* (akronim: OSDC). Zadaća OSDC-a je upravljati velikom bazom podataka (podaci spremljeni u terabajtnim veličinama), koja se nalaze u *cloud* okruženju. Osim upravljanja velikim bazama podataka, OCC

podržava i pomaže prilikom donošenja standardnih rješenja vezanih za velike baze podatka i za komunikaciju između dva različita *cloud* okruženja [20].

6.5 *Open Grid Forum*

Open Grid Forum (akronim: OGF) globalna je zajednica koja je posvećena brzoj evoluciji i prihvaćanju naprednih tehnologija za distribuciju podataka kao što su primjerice: *cloud* okruženje, mreže, alokacija memorijskog prostora te metode tijeka rada. OGF je fokusiran na razvoj i promociju inovativnih i skalabilnih tehnologija, aplikacija i infrastrukture, kako bi se poboljšala produktivnost poduzetništva i znanstvene zajednice.

Jedna od najkompleksnijih zadaća OGF-a, nakon stvaranja, je praćenje napretka *Open Cloud Computing Interface* (akronim: OCCI) specifikacija [21]. OCCI je protokol i API koji je napravljen da može služiti za udaljeno upravljanje API-em za IaaS model *cloud* okruženja, koji se bazira na uslugama. Razvoj OCCI-a je pokrenuo razvoj interoperabilnih alata za uobičajene zadatke kao što su autonomno skaliranje i nadzor rada sustava. Danas je OCCI evoluirao u fleksibilan API s naglaskom na integraciju, prenosivost, interoperabilnost i inovativnost, a osim rada u IaaS modelu može raditi i u PaaS i SaaS modelima *cloud* okruženja [22].

6.6 *The Object Management Group* i *The Cloud Standards Customer Council*

The Object Management Group (akronim: OMG) je međunarodni neprofitni konzorcij vezan za stvaranje tehnologijskih standarda. Tehnologijske standarde u OMG-u zajednički razvijaju: krajnji korisnici, davatelji opreme (engl. *vendor*), akademske i državne institucije. Osim standarda za *cloud* okružja, OMG je autor i standarda za UML dijagrame[17].

OMG sudjeluje u stvaranju *cloud* standarda predlažući standarde za razvoj poduzetničkih rješenja, temeljenih na *cloud* okruženju. Također OMG sudjeluje kao domaćin organizacijama, gdje dolazi do razmjene znanja između članova OMG-a i ostalih informacija. Jedna od tih organizacija je *The Cloud Standards Customer Council* (akronim: CSCC) [23].

[17] UML (engl. *Unified Modeling Language*) predstavlja općeprihvaćeni standard za dokumentiranje podrške i prikaz rada računalnih sustava.

CSCC je organizacija koja je određena ubrzavanju prihvaćanja *cloud* okruženja, ali i predlaganjem različitih standarda, koji se tiču sigurnosti i interoperabilnosti između okružja izvan *clouda* i *clouda*. CSCC, također, pruža podršku korisnicima implementirajući korisničke zahtjeve u standarde ali i poduzetnicima isporučujući materijale kao što su najbolja praksa i slučajevi uporabe *(engl. Use case)* [24].

7 USVAJANJE ISO STANDARDA I PREPORUKA U *CLOUD* POSLOVANJU

Međunarodna organizacija za standardizaciju (engl. *International Organization for Standardization*) je međunarodno tijelo za donošenje industrijskih i komercijalnih normi. ISO je osnovan 1947. godine a danas broji 164 države. Sjedište organizacije je u Ženevi. Prilikom donošenja standarda ISO je surađivao i s drugim organizacijama, primjerice s Međunarodnim elektrotehničkim povjerenstvom (engl. *International Electro technical Commission*). Tada standardi nemaju samo oznaku ISO, već i oznaku ISO/IEC [25].

Za samo *cloud* okruženje ISO je 2014. godine donio dva standarda: ISO/IEC 17788 i ISO/IEC 17789. Cilj navedenih standarda je „uvođenja reda u kaos". Prema standardima ISO nadopunjuje NIST[18]-ovu definiciju po kojoj je *cloud* računalstvo model koji omogućuje sveprisutan, pogodan i na zahtjev dostupan pristup zajedničkim računalnim resursima, koji se mogu brzo pustiti u rad, uz minimalne napore ili interakcije. Po ISO, *cloud* predstavlja razvojnu paradigmu. Neki od ključnih koncepata *clouda*, prema ISO-u su:

- Širokopojasni mrežni pristup;
- Mjerljiva usluga;
- Dijeljena usluga;
- Usluga na zahtjev;
- Brza elastičnost i skalabilnost.

Također, za razliku od NIST-a, ISO preko svoja dva standarda uz SaaS, IaaS i PaaS servisne modele prepoznaje i dodatne servisne modele *clouda*. To su: mreža kao usluga (engl. *network as a service*) i spremište podataka kao usluga (engl. *Data storage as a service*). Nadalje, ISO prepoznaje novu izvedbu oblaka a to je društveni oblak [26].

Za razliku od tih standarda koji opisuju *cloud* postoje standardi vezani za upravljanje u *cloud* okruženju. Ti standardi su: ISO 38500 i ISO 20000.

ISO 38500 pruža vodeća načela za direktore organizacija (uključujući vlasnike, članove odbora, direktore, partnere, više rukovoditelje, ili druge) za učinkovito, djelotvorno i prihvatljivo korištenje IT-a unutar svojih organizacija. Ovaj standard primjenjuje se na sve

[18] NIST je organizacija koja objavljuje standarde, smjernice, preporuke i istraživanja u svezi računalne / *cyber* / informacijske sigurnosti i privatnosti.

organizacije, koje uključuju javne i privatne tvrtke, državna tijela i neprofitne organizacije. Standard je primjenjiv na organizacije svih veličina od najmanjih do najvećih, bez obzira na stupanj njihovog korištenja informacijskih tehnologija [27].

Serije ISO 20000 norme: predstavljaju međunarodni standard za upravljanje IT uslugama - ova serija je na adekvatan način uspostavljena i međunarodno priznata. To nije specifično za računalni *cloud* i *cloud* usluge ali razvija se novi standard koji se bavi primjenom ISO 20000 za računalni *cloud* - ovaj novi standard zove se ISO 20000-7. Osim toga, ISO 20000-11 specifikacija je u fazi razvoja. ISO 20000-11 standard opisuje odnos ISO 20000 s drugim okvirima, a posebno njegov odnosa prema ITIL-u.

Također postoji standard kojim se opisuje opći pristup sigurnosti podataka. Takav pristup dobro je opisan u specifikaciji ISO 27002. Opisani pristupi kontrole u tom standardu primjenjuju se na korištenje *cloud* usluga uz ostale *cloud* specifikacije kao što je opisano u standardu ISO 27017. Sigurnosne kontrole kao što je opisano u ISO 27002 ističu opće značajke koje treba riješiti uključujući i upravljanje imovinom, kontrolu pristupa i kriptografije, a na koje se tada može primijeniti posebne tehnike i tehnologije [10].

Osim ISO 27001 i 27002 standarda, ISO/IEC 270333 standardi pružaju detaljne upute o provedbi sigurnosne kontrole mreže koje su uvedene u ISO/IEC 27002. Dokumentacija pridržavanja važećih dijelova tih standarda obično će biti uključena u sklopu ISO 27002 certifikata.

Ti certifikati su [10], [28], [29]:

- ISO/IEC 27033-1: Pregled i koncept mreže sigurnosti;
- ISO/IEC 27033-2: Smjernice za dizajn i implementaciju sigurnosti mreže;
- ISO/IEC 27033-3: Referentna umrežavanja scenarija - prijetnje, dizajn tehnike i pitanja kontrole.

8 EUROPSKI ZAKON O ZAŠTITI PODATAKA NA *CLOUDU*

Prije prikaza europskih i hrvatskih pravnih akata vezanih za zaštitu osobnih podataka u *cloud* okruženju, potrebno je objasniti pojam direktive ili smjernice. Naime, Europska unija ne donosi zakone već direktive kao jedan od pravnih akata. Direktive su pravni akti Unije upućeni svim ili nekim državama članicama a koje države članice moraju usvojiti odnosno, do nekog određenog roka prenijeti u vlastito zakonodavstvo. Direktive imaju posredan učinak. Iznimno, direktive imaju neposredan učinak ako direktiva nije u roku pretočena u nacionalno pravo i ako je sadržajno bezuvjetna i jasno određena te ako iz nje pojedinac stječe neko pravo prema državi [30]. Niti jedan pravni akt se ne odnosi konkretno na zaštitu korisničkih podataka na *cloudu* već se odnosi na općenitu zaštitu osobnih podataka u elektroničkim komunikacijama.

8.1 Europske Direktive

Europski parlament donio je najprije Direktivu[19] iz 1995. godine a zatim zbog potreba pojašnjavanja i nadopunjavanja direktive iz 1995. godine, Direktivu[20] iz 2002. godine. Direktiva iz 2002. godine bit će detaljnije razrađena.

Direktiva 2002/58/EZ najprije donosi pregled definicija koje se primjenjuju u njoj [31]:

- Korisnik;
- Podaci o prometu;
- Podaci o lokaciji;
- Komunikacija;
- Poziv;
- Pristanak;
- Usluga s dodatnom vrijednosti;
- Elektronička pošta.

Korisnik predstavlja svaku fizičku osobu koja koristi elektroničke komunikacije u privatne i/ili poslovne svrhe. Korisnik prema Direktivi ne mora biti nužno i pretplatnik. Podaci o

[19] Direktiva 95/46/EZ.
[20] Direktiva 2002/58/EZ.

prometu označavaju podatke koji se obrađuju u svrhu prijenosa odnosno komunikacije na elektroničkoj komunikacijskoj mreži ili za njeno naplaćivanje.

Podaci o lokaciji označavaju podatke koji su obrađeni u elektroničkoj komunikacijskoj mreži, koji naznačuju zemljopisni položaj korisničkog terminala, javno dostupne elektroničke komunikacijske usluge.

Komunikacija je definirana kao svaka informacija koja se razmjenjuje ili prenosi između ograničenog broja strana putem javno dostupne elektroničke komunikacijske usluge. Komunikacija ne uključuje bilo koju informaciju prenesenu kao dio usluge emitiranja za javnost osim u onoj mjeri u kojoj se informacija može odnositi na pretplatnika ili na korisnika koji prima informaciju a koji se može identificirati.

Poziv predstavlja uspostavljenu vezu putem javno dostupne telefonske usluge, a koja omogućuje stvarno vremensku dvosmjernu komunikaciju. Pristanak korisnika ili pretplatnika predstavlja proces prihvaćanja. Usluga s dodatnom vrijednosti definirana je kao svaka usluga koja zahtijeva obradu podataka o prometu ili lokaciji, osim podataka o prometu koji nisu nužno potrebni za prijenos komunikacije ili za njeno naplaćivanje.

Elektronička pošta je svaka tekstualna, glasovna, zvučna ili slikovna poruka, poslana preko javne komunikacijske mreže a koja se može pohraniti u mreži ili u primateljevom terminalu sve dok ju primatelj ne preuzme.

U članku 3. određeno je kako će se Direktiva odnositi na obradu osobnih podataka, vezano s pružanjem javno dostupnih elektroničkih komunikacija, u javnim komunikacijskim mrežama u Zajednici[21].

Sigurnost podataka određena je člankom 4. Direktive. Prema članku 4., davatelj usluga elektroničkih komunikacija dužan je poduzeti odgovarajuće tehničke i organizacijske mjere, kako bi se zaštitila sigurnost svojih usluga, odnosno sigurnost mreže. Za provođenje tih aktivnosti, davatelj usluga dužan je surađivati s pružateljem javne komunikacijske mreže. Također, u ovom članku predviđeno je kako davatelj usluge mora pratiti trendove, odnosno poduzimati odgovarajuće mjere zaštite, ovisno o razini mogućih prijetnji. Nadalje, ovim člankom se određuje kako je davatelj javno dostupne elektroničke komunikacije usluge dužan

[21] Pod pojmom „Zajednica“ smatra se Europska zajednica, jedna od preteči EU-a.

obavijestiti pretplatnike o određenoj sigurnosnoj opasnosti i poduzeti sve mjere za otklanjanje opasnosti.

Povjerljivost komunikacija opisana je člankom 5. Prema tom članku države članice moraju osigurati povjerljivost komunikacija i s time povezanih podataka o prometu, koji se šalje preko javne komunikacijske mreže i javno dostupnih elektroničkih komunikacijskih usluga. Članak nalaže državama članicama da zabrani svim neautoriziranim osobama[22]: slušanje, prisluškivanje, pohranjivanje ili bilo koji drugi oblik presretanja i nadzora nad komunikacijama, a za kojeg nemaju pristanak korisnika.

Prema članku 6. podaci o korisničkom prometu, nakon obrade i pohrane moraju se brisati ili učiniti anonimnima, u trenutku kada više nisu potrebni za prijenos komunikacije. Članak, nadalje, predviđa mogućnost obrade podataka o korisničkom prometu u cilju naplate usluga. Međutim, tada se podaci o prometu mogu obrađivati samo u razdoblju, dok postoji mogućnost pravnog pobijanja računa.

Članak 9. opisuje podatke o lokaciji. Prema tom članku podaci o lokaciji, a koji nisu podaci o prometu, a odnose se na korisnike javnih komunikacijskih mreža, mogu se obrađivati, ali samo kada su ti podaci učinjeni anonimnima. Međutim, članak predviđa mogućnost obrade takvih podataka, a da nisu anonimni samo kada korisnik da pristanak za obradu podataka.

Osim zaštite podataka, Direktiva određuje i druge elemente komunikacija kao što su: imenici pretplatnika, neželjene komunikacije, automatsko prosljeđivanje poziva i drugo [31].

8.2 Uredba Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka

Osim prethodno opisane Direktive, zaštita osobnih podataka, opisana je Uredbom[23] o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka[24]. Tom Uredbom ažurirana su i osuvremenjena načela sadržana u Direktivi o zaštiti podataka iz

[22] Neautorizirane osobe su sve osobe koje nemaju zakonsko dopuštenje, niti dopuštenje korisnika, za obavljanjem presretanja i nadzora prometa.

[23] Prema [28], uredbe EU su pravni akti koji su u cjelini obavezni i neposredno vrijede za sve države članice.

[24] Uredba (EU) 2016/679.

1995. godine. Njome su utvrđena prava pojedinaca i obveze organizacija koje obrađuju osobne podatke, ali i obveze odgovornih za osobne podatke.

U Uredbi se navode pojačana prava pojedinaca. Tim pravima pojedincima se daje više kontrole nad njihovim osobnim podacima. Kontrola je dana pomoću [32]:

- Potrebe za jasnim pristankom pojedinaca na obradu osobnih podataka;
- Lakšeg pristupa pojedinaca njegovim ili njezinim osobnim podacima;
- Prava na ispravljanje, brisanje i „zaborav“;
- Prava na prigovor, pa i za upotrebu osobnih podataka za potrebe izrade profila;
- Prava na prenosivost podataka s jednog poslužitelja na drugi.

Uredba, također, donosi opće obveze voditelja obrade odnosno, osobe zadužene za obradu podataka. Jedna od obveza voditelja obrade je pružanje transparentnih i lako dostupnih informacija o ispitanicima i obradi njihovih podataka. Također, voditelj obrade ima obvezu provoditi odgovarajuće sigurnosne mjere, koje moraju biti usklađene s prisutnim rizikom, pri obradi podataka. Od voditelja obrade može se zatražiti izvješće o mogućoj povredi osobnih podataka. Nadalje, Uredba obvezuje organizacije, koje obavljaju određene rizične radnje obrade podataka, na imenovanje službenika za zaštitu podataka.

Uredba previđa potrebu svake države članice da na nacionalnoj razini uspostavi neovisno nadzorno tijelo. Cilj uspostave takvog nadzornog tijela je, uz zaštitu osobnih podataka, uspostaviti mehanizam za osiguravanje dosljednosti u primjeni prava o zaštiti podataka, diljem EU. U RH to nadzorno tijelo je Agencija za zaštitu osobnih podataka.

Također, Uredba prepoznaje mogućnost ispitanika za podnošenjem pritužbe određenom nadzornom tijelu, a posljedično i pravo na pravni tijek, naknadu i odgovornost. Zbog potrebe zbližavanja pojedinaca i nadzornih tijela, vezanih za odluke ispitanici imaju pravo da odluku nadzornog tijela ispita određeni sud (Upravni sud za RH).

Protiv prekršitelja ove Uredbe određene su administrativne sankcije. Sankcije predstavljaju novčanu kaznu, kojom će se kazniti voditelji obrade podataka, i to u iznosu do 20 milijuna EUR ili do 4% ukupnog godišnjeg prihoda. Veličinu administrativnih uvoditi i određivat će tijela za zaštitu podataka [32], [33].

8.3 Hrvatsko zakonodavstvo

Prethodno opisane Direktive i Uredbe, Republika Hrvatska prenijela je u vlastito zakonodavstvo. Zaštita osobnih podataka u RH predviđena je Ustavom RH[25] i Zakonom o zaštiti osobnih podataka (dalje: ZZOP)[26].

Pitanje osobnih podataka Ustavom je određeno člankom 37. Ustav predviđa svakom građaninu RH sigurnost i tajnost osobnih podataka. Nadalje, Ustav zabranjuje prikupljanje, obrađivanje i korištenje osobnih podataka, a da to nije određeno zakonom ili da građanin nije dao pristanak. Također, Ustav zabranjuje uporabu osobnih podataka, na način koji je suprotan utvrđenoj svrsi prikupljanja osobnih podataka [34].

Temeljitije uređenje zaštite osobnih podataka, ali i nadzora nad prikupljanjem, obradom i korištenjem osobnih podataka te iznošenjem iz RH provedeno je ZZOP-om. Prema ZZOP-u svrha zaštite osobnih podataka je zaštita privatnosti ljudskog života i ljudskih prava te temeljnih sloboda, u koje se može ući: prikupljanjem, obradom i korištenjem osobnih podataka. Zaštita osobnih podataka, prema ZZOP-u, omogućena je svakoj fizičkoj osobi, bez obzira na: rasu, boju kože, spol, jezik, političko ili drugo uvjerenje, nacionalno ili socijalno podrijetlo, imovinu, rođenje, naobrazbu, društveni položaj ili neko drugo svojstvo ili obilježje.

Člankom 2, ZZOP, daje značenje određenim pojmovima [35]:

- Osobni podatak;
- Obrada osobnih podataka;
- Zbirka podataka;
- Ispitanik;
- Voditelj zbirke osobnih podataka;
- Privola ispitanika.

Osobni podatak jest svaki podatak ili informacija, koja se odnosi na fizičku osobu (pravna osoba je isključena iz definicije), koja se pomoću te informacije može identificirati, izravnim ili neizravnim putem, preko jednog ili skupine podataka.

[25] Ustav Republike Hrvatske, NN br. 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14.

[26] Zakon o zaštiti osobnih podataka, NN br. 103/03, 118/06, 41/08, 130/11, 106/12.

Obrada osobnih podataka je svaka aktivnosti nad podacima: prikupljanje, pohrana, organiziranje, tehnička obrada i objava podataka te ostale aktivnosti. U ovom slučaju, ZZOP se odnosi na sve vrste obrada, neovisno provodi li ih državna uprava ili pravne osobe te fizičke osobe, ali se ne odnosi na provođenje zbog osobnih ili obiteljskih razloga.

Zbirka osobnih podataka je skup podataka koji je organiziran i dostupan prema nekom kriteriju. Pojam osobnog podatka i zbirke odnosi se na sve podatke neovisno o formi i mediju na kojem se nalaze.

Ispitanik, prema ZZOP-u, je svaka fizička osoba koja je dala svoje osobne podatke ili čiji se osobni podaci prikupljaju.

Voditelj zbirke osobnih podataka je osoba čiji je zadatak voditi brigu te provoditi određene postupke nad osobnim podacima. Vođenje brige i provođenje određenih postupaka moraju biti u skladu sa ZZOP-om.

Pristanak ispitanika je suglasnost ispitanika nad obradom njegovih osobnih podataka u određene svrhe. Prilikom traženja pristanka koji mora biti jasno opisan, potrebno je jasno naznačiti svrhu prikupljanja. Međutim, ZZOP predviđa mogućnost prikupljanja osobnih podataka kada ih ispitanik samostalno javno objavi ili kada su u nacionalnom interesu (borba protiv korupcije, zaštita života i slično).

Osim osobnih podataka, ZZOP predviđa posebnu kategoriju podataka. Posebna kategorija podataka su svi podaci koji su smatrani posebno osjetljivima [35], [36]:

- Porijeklo;
- Politička stajališta;
- Vjerska i druga uvjerenja;
- Sindikalno članstvo;
- Zdravlje i spolni život;
- Osobni podaci o kaznenom i prekršajnom postupku.

ZZOP zabranjuje prikupljanje i daljnju obradu posebne kategorije podataka. Izuzetak od istoga je prikupljanje i obrada u okviru djelatnosti ustanove, udruženja ili bilo kojeg drugog neprofitnog tijela, koje je neposredno vezano uz takve podatke, a koji se moraju odnositi na njihove članove. Zbirke osobnih podataka ne smiju sadržavati posebne kategorije podataka.

Proces prikupljanja osobnih podataka vrlo je jasno definiran čak u odnosu na uobičajenu praksu, ZZOP uvodi značajna ograničenja. Po pitanju opsega osobnih podataka ZZOP nalaže da traženi podaci moraju biti bitnu u svrhu prikupljanja, odnosno da ispitanik može svo prikupljane podatke odbiti dati. Primjer takvih prikupljenih podataka su spol i godina rođenja. Također, ZZOP jasno definira potrebu za određivanjem svrhe i informiranja ispitanika. Cilj ove definicije je spriječiti neprimjereno i prekomjerno korištenje osobnih podataka. Temeljem toga ispitanik mora biti jasno i nedvosmisleno upoznat sa svrhom prikupljanja osobnih podataka, temom i opsegom. ZZOP zabranjuje davanje prikupljenih podataka trećim stranama. Nadalje, ZZOP inzistira na točnosti, potpunosti i ažurnosti osobnih podataka.

Ako treća strana želi koristiti osobne podatke, mora podnijeti voditelju zbirke osobnih podataka pisani zahtjev. U zahtjevu mora biti jasno navedena svrha i pravni temelj korištenja podataka. Korištenje podataka, voditelj zbirke, može odobriti samo za obavljanje poslova utvrđenih zakonom. Voditelj zbirke dužan je voditi evidenciju davanja osobnih podataka, sa svrhom davanja. Svaki ispitanik ima pravo uvida u evidenciju korištenja njegovih osobnih podataka. Iako se takvi podaci smatraju osobnima, dani podaci ne smiju omogućiti identifikaciju pojedinaca.

ZZOP predviđa mogućnost iznošenja osobnih podataka izvan teritorija RH. To je jako bitno za *cloud* okruženje, zato što se *cloud* poslužitelji većinom ne nalaze na teritoriju RH. Voditelj zbirke osobnih podataka može staviti podatke na raspolaganje na teritoriju izvan RH. Međutim, država u koju se ti podaci „iznose“ mora imati jasno i kvalitetno uređenu zaštitu osobnih podataka. Ako postoji sumnja u uređenost zaštite osobnih podataka, voditelj zbirke dužan je zatražiti AZOP-ovo mišljenje.

Prema ZZOP-u, ispitanik ima pravo, zatražiti od voditelja zbirke na vlastiti zahtjev a u vremenskom roku od 30 dana [35]:

- Potvrdu u kojoj je navedeno obrađuju li se ispitanikovi osobni, ili ne;
- Obavijest u razumljivom obliku, o podacima koji se odnose na ispitanika, čija je obrada u tijeku i izvor tih podataka;
- Uvid u evidenciju zbirke osobnih podataka i uvid u osobne podatke, sadržane u zbirci osobnih podataka;
- Izvatke, potvrde ili ispise osobnih podataka, koji su sadržani u zbirci osobnih podataka;
- Ispis podataka o tome tko je i s kojom svrhom te po kojem pravnom temelju dobio na korištenje ispitanikove osobne podatke;
- Obavijest o logici automatske obrade osobnih podataka;
- Dopunjavanje, izmjenu ili brisanje osobnih podataka, koji su: netočni, nepotpuni ili neažurni.

Sve zbirke osobnih podataka nalaze se u evidenciji osobnih podataka. Vođenje evidencije osobnih podataka spada pod nadležnost AZOP-a [35], [37].

Zaključno, može se reći kako pravno uređene države paze na privatnost, odnosno osobne podatke svakog građanina, kako u klasičnim okruženjima tako i u *cloud* okruženju. Organizacijama koje se bave *cloud* okruženjem zabranjeno je prikupljanje podataka o svojim klijentima, osim ako to krajnji korisnik ne dozvoli. Organizacije najčešće traže različita dopuštenja za prikupljanje podataka u ugovoru o korištenju (engl. *User agreement*) a korisnici najčešće daju pristanak zato što ne čitaju ugovor.

9 „*SAFE HARBOR*“ SIGURNOSNA NAČELA KAO DOGOVOR IZMEĐU EUROPSKE UNIJE I SJEDINJENIH AMERIČKIH DRŽAVA

Sigurna luka (engl. *Safe harbor*) predstavlja ugovor, kojim je previđen mehanizam između Europske unije i Sjedinjenih Američkih Država, kojim bi se trgovačkim društvima koja obrađuju osobne podatke europskih građana (npr. Googleu ili Facebooku i sl.), dao alat koji bi im omogućio prijenos podataka iz EU u SAD. Prijenos bi trebao pružiti odgovarajuću razinu zaštite. Sigurnosna luka uspostavljena je zbog rješavanja problema nastalog zbog nedovoljne prikladnosti američkog pravnog okvira u pogledu privatnosti osobnih podataka.

Sigurna luka bi omogućila nadzorniku EU prijenos osobnih podataka u organizaciju, koja se nalazi u SAD-u, a koja je potvrdila pridržavanje Sporazuma o sigurnoj luci i obvezala se osigurati poštivanje načela Sigurne luke. Sigurna luka, od samog početka bila je predmet političkih nesuglasica. Europski parlament istaknuo je zabrinutost koja se temelji na nepostojanju pojedinačnog prava sudske tužbe i nedostatku obveze trgovačkih društava za plaćanjem odštete, nastale kao posljedica za nezakonitim obrađivanjem podataka, te zbog različitih sustava zaštite, koji postoje u SAD-u, a ovise o tome jesu li vlasnici podataka Amerikanci ili Europljani.

Sporazum o sigurnoj luci podrazumijevao je dvostrani sustav za obustavu ili prekid mehanizma prijenosa i obrade osobnih podataka. Sporazum se mogao prekinuti trenutkom kršenja odluke 2000/520/EZ. Država članica može obustaviti protok podataka organizaciji u slučaju kada je utvrđena znatna vjerojatnost kršenja načela Sporazuma, odnosno kada bi prijenos i obrada osobnih podataka predstavljala opasnost od ozbiljne štete za osobu čiji se podaci prenose i obrađuju. U slučaju obustave protoka podataka, država članica je dužna obavijestiti Europsku komisiju o provedenim aktivnostima. Tada bi EK ocijenila provedbu odluke temeljem dostupnih informacija te izvijestila državu članicu o važnim otkrićima. Sukladno tome, EK može izjaviti kako provedba Sigurne luke ne funkcionira i predložiti mjere za obustavu ili opoziv Sporazuma.

Zbog zabrinutosti vezane za prikladnost Sigurne luke s obzirom na opseg masovnog nadzora privatnog ponašanja korisnika odnosno, prema Izvješću europsko-američke radne grupe o zaštiti podataka, ustvrđeno je kako osobe koje nisu američki državljani, nemaju nikakav administrativni put pogledu pristupa, pravne zaštite i informacija o njihovim osobnim

podacima, koji se obrađuju radi provedbe zakona ili u svrhu nacionalne sigurnosti. Zbog toga dolazi do spora pred Sudom Europske unije [38].

9.1 Odluka Suda Europske unije

Austrijanac Maximillian Schrems pokreće spor[27] protiv sjevernoirskog povjerenika za zaštitu osobnih podataka, pred Sudom Europske unije. Tužba je vezana za sigurnost podataka tužitelja koje potencijalno narušava Facebook.

Tužitelj je tvrdio kako je došlo do prijenosa njegovih podataka s poslužitelja koji se nalaze u Sjevernoj Irskoj na poslužitelje koji se nalaze u SAD-u. Tražio je od sjevernoirskog povjerenika za zaštitu osobnih podataka da provjeri načela sigurnosti Sigurne luke. Povjerenik je njegov zahtjev odbio, pozivajući se na Sporazum sigurne luke, a tvrdeći kako SAD udovoljava traženim sigurnosnim načelima. Također, prije tužbe pred Sudom Europske unije, ovaj slučaj je proučavala i EK, koja je utvrdila kako SAD udovoljava traženim sigurnosnim načelima.

6. listopada 2015. godine, Sud Europske unije za navedeni slučaj donosi odluku. U odluci, Sud je najprije ustvrdio kako država članica, od čijih se građana prenose osobni podaci, nema mogućnost nadzora tijeka osobnih podataka, kako je utvrdila EK. Prema sporazumu, država članica mora imati mogućnost samostalnog i potpunog nadziranja tijeka osobnih podataka prema zemljama koje nisu članice (engl. *Third countries*).

Nadalje, Sud je ustvrdio kako je EK trebala u navedenom slučaju konkretno odrediti udovoljava li SAD traženim sigurnosnim načelima. Prema Sudu, EK nije konkretno odredila udovoljava li SAD sigurnosnim načelima već je samo pregledala shemu Sigurne luke (engl. *Safe harbor scheme*). Sud je utvrdio da je navedena shema primjenjiva samo u SAD-u i organizacijama koje su vezane uz SAD.

Također, u odluci Sud je utvrdio kako bilo kakva pa tako i generalizirana (općenita) baza elektroničke komunikacije, predstavlja esencijalnu povredu osnovnih ljudskih prava, vezanih uz poštivanje privatnosti u životu. Osim toga, Sud je utvrdio kako je shemom došlo do povrede

[27] Maximillian Schrems protiv povjerenika za zaštitu osobnih podataka (*Maximillian Schrems v Data Protection Commissioner*), slučaj: C-362/14.

ljudskih prava na zakonodavnu zaštitu. Prema Sporazumu, državljanin zemlje članice, nema mogućnost pokretanja potencijalnog spora zbog prijenosa i obrade podataka.

Zbog svega navedenog Sud je presudio u korist tužitelja. Također, Sud je prepoznao kršenje načela sigurnosti Sigurne luke, pa je sukladno tome Sporazum proglasio nevaljanim. Nadalje, Sud je naložio sjevernoirskom povjereniku za zaštitu osobnih podataka da ponovno razmotri tužiteljev zahtjev [39].

9.2 Donošenje novog sporazuma između Europske unije i Sjedinjenih Američkih Država

U veljači 2016. godine, dogovorena su načela novog sporazuma o Sigurnoj luci. Za implementaciju novog dogovora odgovorni su Potpredsjednik EK i Povjerenica za pravosuđe, potrošače i ravnopravnost spolova. Ovim sporazumom prava Europljana su bolje zaštićena. Prema novom sporazumu američka komisija za trgovinu dužna je nadzirati tijek podataka, a po potrebi i surađivati s europskim agencijama za zaštitu osobnih podataka.

Novi sporazum nalaže organizacijama u SAD-u, osim bolje zaštite osobnih podataka, ograničavanje pristupa podacima. Međutim, ograničavanje pristupa trebalo bi se provoditi pod jasnim uvjetima uz dostatne ograde i propisani nadzor. Ovom odredbom bi se trebao spriječiti masovni pristup osobnim podacima. Europski državljani moći će zatražiti istragu ili uložiti prigovore prema Europskom ombudsmanu[28] [40], [41].

[28] Europski ombudsman je nezavisno i nepristrano tijelo koje ima pravnu mogućnost prozivanja europske administracije na odgovornost.

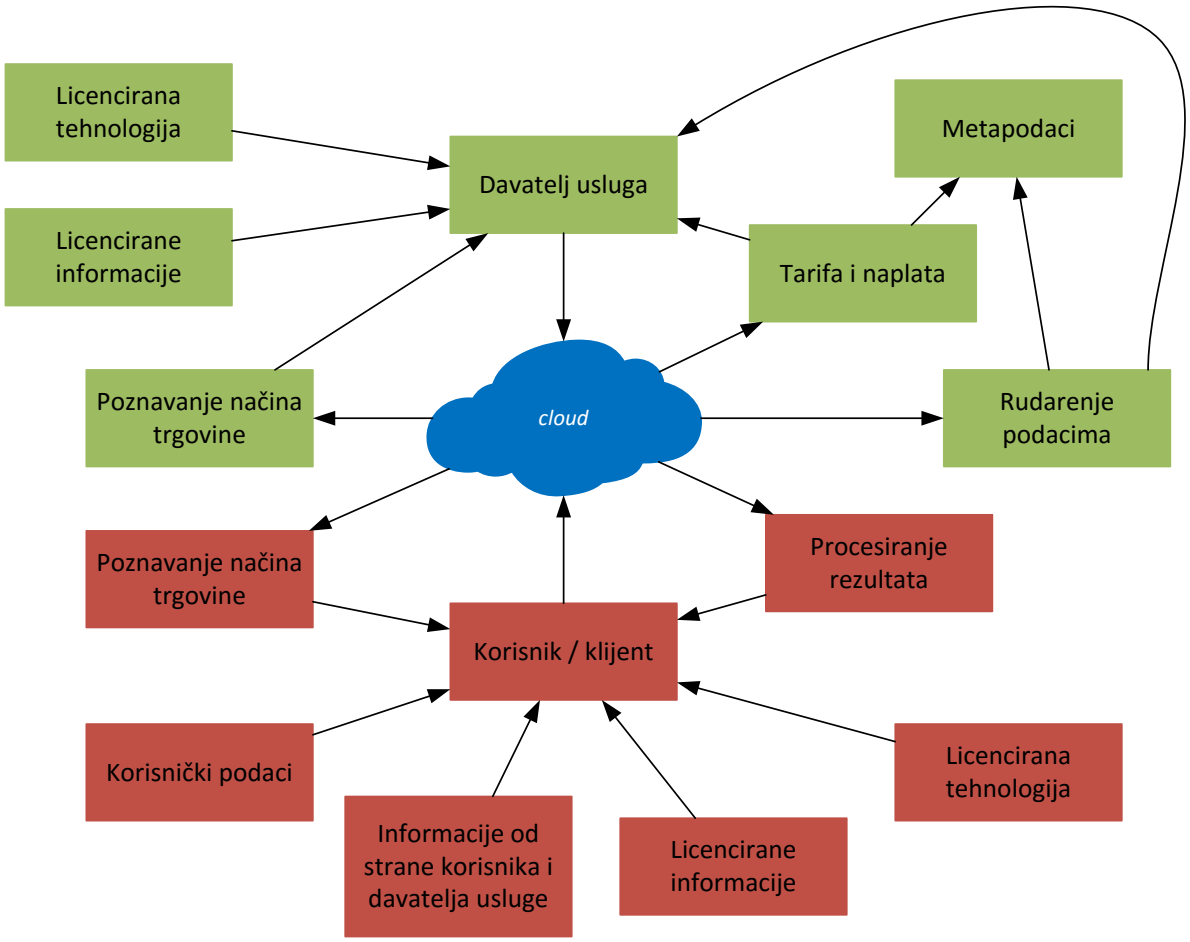
10 SIGURNOSNI RIZICI I OPASNOST U *CLOUDU*

Prije analize mogućih sigurnosnih rizika i opasnosti u *cloud* okruženju potrebno je analizirati vlasništvo nad informacijama u *cloud* okruženju. Stoga će prva dva potpoglavlja istražiti niz pitanja koja se odnose na to kako se informacije pohranjuju, obrađuju i/ili distribuiraju u *cloud* okruženju. Isto tako obradit će se zahtjevi odnosno problemi koji se nameću samom *cloudu.* Uz normativni mod vlasništva kreiran od strane intelektualnog tipa vlasništva (engl. *Intellectual property*), akcija povjerljivosti ili ona od strane ugovora, istražuje se kakve računarski *cloud* ima implikacije u pogledu otvorenih modela vlasništva. Konačno, zbog autorskih prava i implikacije razvoja *clouda* kao industrije u cjelini također se istražuju pitanja vlasništva nad sučeljem za programiranje aplikacija (API) koji su neophodni za interoperabilnost *clouda.*

Prvo se usmjerava pozornost pohranjenom i obrađenom sadržaju od strane korisnika (ili kupca) usluge i također, kratko, sadržaja ili informacija koje su pohranjene ili obrađene od strane samog davatelja usluga. Takav sadržaj, bez obzira je li kontroliran od strane korisnika ili usluga bit će proizveden izvan ili unutar oblaka.

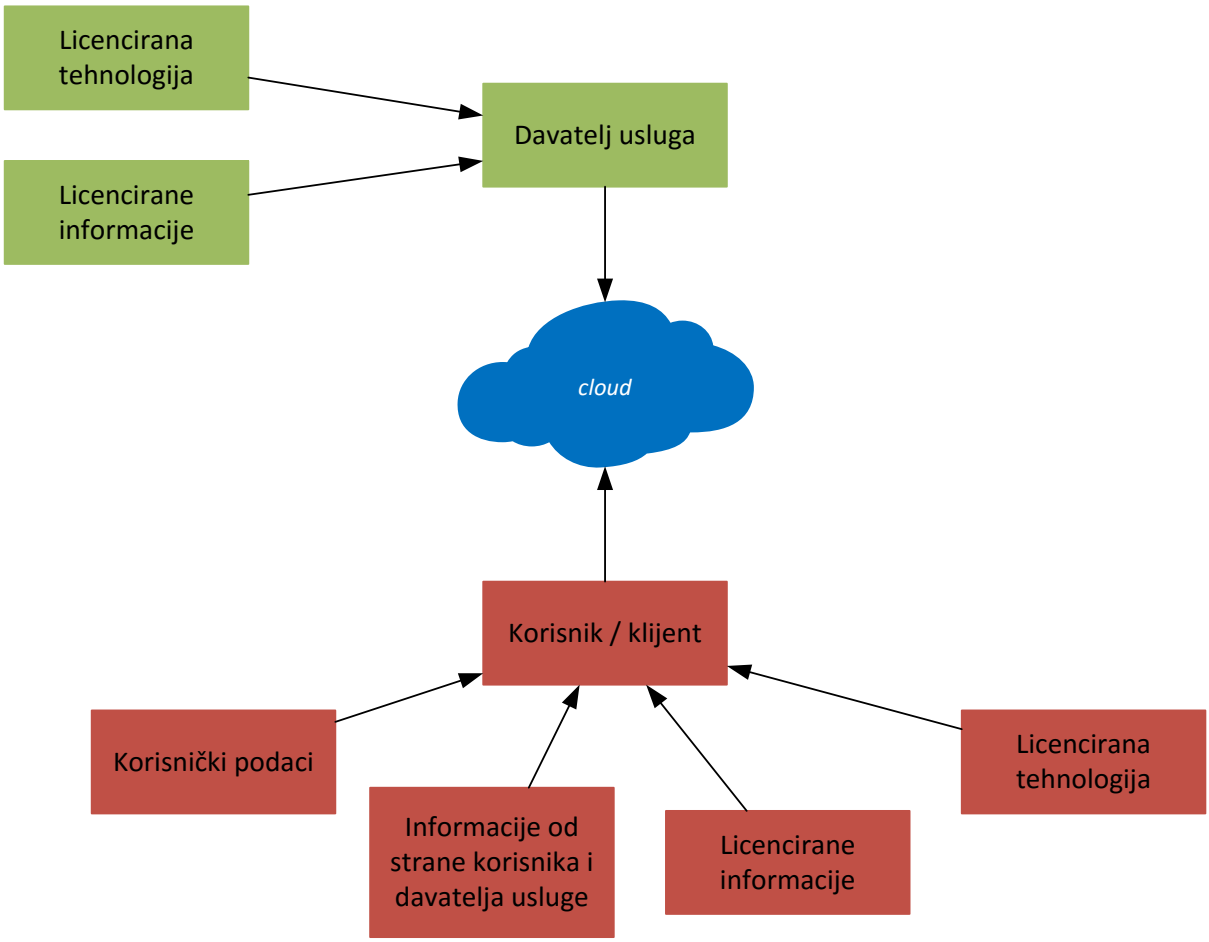
10.1 Korisnički sadržaj pohranjen i procesiran u *cloudu*

Konceptualna mapa informacijskih tokova između davatelja usluge i korisnika prikazana je na slici 6. Iako mapa izgleda složeno moguće ju je pojednostaviti.



Slika 6. Prikaz toka podataka u relacijskom modelu *clouda*
izvor: [42]

Velik dio generiranih informacija su izvan *clouda* (slika 7.). Informacije imaju već uspostavljen vlasnički status prije nego li se postave na *cloud*. Međutim, informacije postavljene na *cloud* od strane korisnika mogu postati problematične. Primjer problema je kada milijuni korisnika dijele audio sadržaj putem *clouda*, isto se odnosi na dijeljenje fotografija putem društvenih mreža (primjerice: Facebook, Twitter, Instagram, itd.). Ako je inicijalno vlasništvo takvog sadržaja poznato, u praksi kompleksne norme dijeljenje informacija među korisnicima označava dolazak tj. otkrivanje stvarnog vlasnika koji omogućuje *cloud* usluge postaje gotovo nemoguće. Čini se razumnim tvrditi kako su očekivanja svih sudionika da postavljanje sadržaja na *cloud* ne bi smjelo izmijeniti status vlasnika [42].



Slika 7. Informacije generirane izvan *clouda*
izvor: [42]

Glavna ideja relacije računalnog *clouda* jest omogućavanje korisniku korištenje *cloud* tehnologije kako bi se procesirale informacije i tako generirali rezultati (engl. *Outputs*). Međutim, klijent može generirati trgovačke tajne (engl. *Trade secrets*), koje nisu prikazane u niti jednom rezultatu obrade informacija ali su skladištene u strukturama podataka ili procesima koje korisnik uspostavlja korištenjem *clouda* [42].

10.2 Vlasništvo nad podacima generiranim izvan *clouda*

Informacije generiranje izvan *clouda* obično imaju uspostavljeni status vlasnika. U većini slučajeva takve informacije pohranjene su u *cloudu* na potpuno digitalan način za razliku od korištenja fizičkog medija. Tako se izbjegavaju pravne posljedice u vezi vlasništva nad podacima, u suprotnome potrebno je potražiti pravo na vlasništvo u četiri područja/sekcije prava.

Prvo područje predstavlja područje autorskih prava. Jedno od najvažnijih intelektualnih vlasništva koji bi moglo opstajati u informaciji. Nacionalni zakoni autorskih prava diljem svijeta prepoznaju da autorska prava opstaju u digitalnim radovima, ali se razlikuju u konceptu koji konstituira/sačinjava rad. Anglosaksonski propisi zaštićuju sva djela gdje dovoljna vještina rada ili prosudba biva korištena u njihovoj kreaciji. Ne postoji potreba za aktivnostima samim po sebi (engl. *Per se*) ali se informacija neće zaštiti ako njena kreacija zahtjeva minimalan trud.

Građansko pravo, koje zaštićuje autorska prava, zahtjeva minimalan nivo kreativnosti kako bi se kvalificiralo za zaštitu. Njemačka nudi dobar primjer koji zahtjeva inicijalni korak koji razotkriva cjelokupan rad od same informacije. Prije nego li je stupila direktiva EU, softver direktiva na snagu, njemački sud držao je do toga kako su neki tipovi softvera (kao na primjer operativni sustavi) više funkcionalni nego kreativni i zbog toga nisu zaštićeni autorskim pravom. Ovakvo što je još uvijek karakteristično za informacije u čistom obliku kao na primjer tablice podataka (engl. *Data tables*). Iako je takav dio zakona odbačen od strane američkog saveznog zakona i sada zahtjeva minimalni nivo kreativnosti za zaštitu prava. Međutim, nivo kreativnosti je znatno manji u Njemačkoj.

Drugo, ako se koristi zakon od strane Europske unije (zakon se primjenjuje na sve države članice) tada se informacija u obliku baze podataka prima pod zaštitom direktive baze podataka**.** Kako bi se baza podataka uspjela kvalificirati za takvu zaštitu onda je nužno postojanje kvalitetnog i/ili kvalitetnog sadržaja informacije (engl. *Qualitatively and/or quantity information*). Ako je to tako, tada bilježnik ima pravo spriječiti ekstrakciju i/ili ponovnu uporabu sadržaja te baze podataka. Dugotrajnost zaštite iznosi 10 godina počevši od onog dana kada je baza dostupna javnosti ili 15 godina od kreacije same baze podataka.

Treće područje prava koje je relevantno jest ono koje se odnosi na zaštitu povjerljivih informacija ili poslovnih tajni (engl. *Trade secrets*). Postoji internacionalni konsenzus za minimalni nivo zaštite naveden u članku 39., stavku 2., koji se odnosi na usuglašenije trgovinskog aspekta intelektualnog prava vlasništva (engl. *TRIPS agreement*) koje specificira da zaštita mora biti dana informacijama. Te informacije [43]:

- Su tajne u smislu da je dio ili cijeli sadržaj informacije tajan (informacije su tajne u određenom krugu ljudi);
- Posjeduju komercijalnu vrijednost zbog toga što su tajne;

- Bile su predmet smislenih koraka pod određenim okolnostima, od strane u skladu sa zakonom da sačuva tajnost informacije.

Većina sudova, uključujući engleski sud isto tako štiti nekomercijalne informacije koje su povjerljive po prirodi. Velik broj podataka u *cloudu*, bile one zaštićene intelektualnim vlasništvom ili ne, biti će povjerljive prirode sve dok korisnici koji su uključeni u relaciju računalnog *clouda* prihvate da duguju obveze povjerljivosti davatelju usluge (vlasniku).

Na kraju, četvrto područje predstavlja zakon o ugovoru koji predstavlja ključnu ulogu u određivanju vlasništva preko ToS-a (engl. *Terms of service*, hrv. Uvjeti pružanja usluge) za relaciju računalnog *clouda*. Za informacije koje se generiraju izvan *clouda* ovaj ugovor može razjasniti zaštitu autorskih prava i povjerljivu relaciju na tri načina, [42]:

- Odobrenje prava intelektualnog vlasništva koje različiti entiteti posjeduju i osiguravanje da kroz odgovarajući odabir niti jedno pitanje koje ima implikaciju na licence ili se pojavi kroz nepristrane zadatke.
- Omogućavanje licence prava intelektualnih vlasništva koji su potrebni kako bi relacije u *cloudu* funkcionirale. Krajnji korisnik/kupac koristit će softver i podatke čija su prava intelektualnog vlasništva u vlasništvu davatelja usluge ili neke treće strane (engl. *Third party*) i korištenje ne licencirane tehnologije predstavlja prekršaj. Na sličan način, davatelj usluga procesirat će informacije u kojemu krajnji korisnik/kupac posjeduje IP prava i kojemu će također trebati licenca. Tamo gdje je softver i podatak dostupan od treće strane, vjerojatno je da je vlasnik prava izvršio licenciranje.
- Davatelju usluga pod uvjetima koji postavljaju ograničenje na korištenje. Krajnji korisnik/kupac mora biti svjestan tih ograničenja/restrikcija kako bi se izbjegla mogućnost prekršaja s obje strane (kupac i davatelj usluga).
- Definiranje obveza povjerljivosti kojih svaki sudionik duguje drugima, uključujući sva ograničenja nad tim obvezama i ugovaranje položaja povjerljivosti nakon prekida odnosa.

10.3 Osnovni rizici i sigurnost u *cloudu*

Jedno od glavnih obilježja *clouda* je to što omogućuje apstrakciju dok se korisnička funkcionalnost može odvojiti od upravljanja resursa. Ali, oslanjanje na apstraktne resurse koji su kontrolirani od trećih strana i čija se korisnost dijeli predstavlja rizik. Zabrinutost se obično pojavljuje oko smanjenja korisničkih funkcionalisti i povećanja funkcionalnosti davatelja usluge, posebice sigurnosti podataka pogonjena vjerojatno od smanjenja dostupnih informacija prema korisnicima koji se odnose na detalje od strane davatelja komponenti, dobavljača i mehanike.

Ko-lokacijski rizik isto tako može postojati, ako se za hardver sumnja da sadrži neprikladne odnosno neprovjerene dijelove tada se podaci povlače od strane zaduženog osoblja [44]. Isto tako, podaci koji se skladište na istoj opremi ili bazi podataka nekog drugog korisnika na kojeg se vrši napad sa udaljene lokacije također mogu biti ugroženi. Neovisno o tome je li meta lokalna ili se pak nalazi na nekoj udaljenoj lokaciji, podaci na koje se vrši napad su uvijek ugroženiji nego podaci koji su isto tako skladišteni na istom resursu ali na koje se napad ne vrši direktno. Primjerice ako postoji osoba A, koja ima spremljene podatke na istom poslužitelju kao i osoba B ali je slučaj da je napad je usmjeren na osobu A isključivo, tada podaci osobe B mogu ostati sigurni neovisno o tome što je poslužitelj na kojemu se nalaze računi (engl. *Account*) mnogih korisnika cijeli kompromitiran tj. vrši se napad na njega [42]. Generalno sigurnost *clouda* ovisi o tipu odnosno, servisnom modelu i dizajnu (svaka organizacija na drugačiji način izrađuje dizajn: Microsoft, Apple, Google, itd.).

10.4 Kriptografija kao mjera zaštite *clouda*

Neautorizirani ulazak može se spriječiti tako da korisnici kriptiraju svoje podatke prije nego što ih pohrane na *cloud*. Kriptografski programi mogu transformirati cjelokupni set podataka tako da primjene adekvatni kriptografski algoritam na tu skupinu podataka. Na primjer, informacija se translatira u neki drugi jezik tako da samo oni koji poznaju jezik mogu razumjeti napravljenu translaciju. Jednosmjerna kriptografija aplicira jednosmjernu funkciju na podatke i tako producira fiksnu zaštitu (engl. *Hash*[29]) ili zaštitnu vrijednost. Funkcionalnost

[29] Hash funkcija je funkcija koja služi za mapiranje podataka različitih veličina u podatke fiksne veličine.

izvedena je tako da je nemoguće vratiti podatak u prvobitno stanje. Za razliku od jednosmjernih funkcija za zaštitu podataka, primjenom dvosmjerne funkcije u zaštiti podataka moguće je vratiti podatak u prvobitno stanje ali samo od strane ovlaštenih osoba, pod striktno definiranim uvjetima.

Bitni faktori koji utječu na kriptiranje podataka ovise o jačini odnosno intenzitetu enkripcije, duljini enkripcijskog ključa (dulji ključevi su uglavnom manje podložni napadima nego kraći) i raspolaganje ključevima. Generalno podaci se smatraju dobro kriptiranim ako se kriptografske metode pokažu efikasnim i sigurnim u realnom svijetu [42].

Kriptografiju je moguće primijeniti na podatke unutar elektroničkog dokumenta, datoteke, baze podataka ili neke druge kolekcije informacija. Korisnici mogu primijeniti kriptografiju na dijelove ili još češće na cjelokupne skupine podataka prije nego što ih pohrane na *cloud*. Primjerice jednosmjerna ili dvosmjerna kriptografija može se primijeniti samo na imena dok ostali podaci mogu ostati netaknutima u pogledu kriptografije.

Dekriptiranje te ponovna enkripcija podataka reducira performanse, što predstavlja veliku manu kriptografiji. Nadalje, isto tako s podacima koji su kriptirani vrlo moćnim kriptografskim algoritmima poput vojnih podataka i podataka od iznimne državne važnosti moraju proći proces dekriptiranja kako bi se nad njima mogla vršiti daljnja obrada u pogledu dodatne analize, sortiranje podataka, indeksiranje, optimizacija i sl. Dekriptiranje podataka može dovesti do kompromitacije istih zato se uvijek nastoji prilikom dekriptiranja pohraniti kriptirane podatke na siguran sustav (primjerice *offline* računalo) te tek tada izvršiti potpuno dekriptiranje.

Neovlašteni pristup je isto tako moguć ako se podaci presretnu prilikom transmisije na sam *cloud*. Ako korisnik šalje ne kriptirane podatke putem kriptiranog kanala, davatelji usluga će opet dobiti ne kriptirane podatke. Obrnuto, kriptirani kanali nisu potrebni za pouzdanu transmisiju od već snažno kriptiranih podataka, iako netko tko nadzire kanal ionako može samo presrest kriptirane podatke koji nisu od nikakvog značaja.

10.5 Brisanje podataka u *cloudu*

Različiti stupnjevi brisanja podataka postoje u *cloudu*. Ako korisnik obriše podatak, tada se podatak premješta u „koš za smeće“ (engl. *Recycle bin/trash*) ali se određeno vrijeme ne briše u potpunosti, tj. ostaje na raspolaganju korisniku ako treba vratiti podatak, ako mu kojim slučajem zatreba. Kada ugovor između korisnika i davatelja usluga istekne, korisnički podaci ne brišu se odmah, nego nakon određenog razdoblja. Korištenje „koša za smeće“ i brisanje podataka sa vremenom/razdobljem odgode može potencijalno ugroziti ostale elemente sigurnosti kao što su npr. integritet[30] i dostupnost[31].

Problem ponekad nastaje u tome da nakon brisanja podataka u „košu za smeće“ stvarni podaci ostaju jer se brišu reference, točnije pokazivači (engl. *Pointers*[32]) koji pokazuju na stvarne podatke koji su pak spremljeni u memoriji na nekom drugom mjestu. Stvarni podaci se zapravo brišu tako da njihovo mjesto zauzimaju nadolazeći, svježi podaci spremljeni od strane istih ili različitih korisnika [45].

Remanentnost podataka odnosno brisanje nominalnih podataka zbog navedenih problema predstavlja podosta velik problem. Kako bi se postigla efektivna povjerljivost podataka potrebno je u više navrata izvršiti aktivnost brisanja već obrisanih podataka. Krajnja mjera čak navodi demagnetizaciju diska ili sigurnosno uništavanje fizičkog medija. Privatni *cloud* u ovom slučaju pokazuje se kao bolje rješenje jer je jednostavnije zatražiti da se podaci „unište“ do kraja za razliku od javnog modela gdje krajnji korisnik nikada ne može biti siguran je li kakav fragment podataka ostao na dislociranom serveru ili nije [42], [46].

10.6 Osiguranje adekvatne zaštite podataka i informacija

Podaci su u srži informacijskih sigurnosnih problema za bilo koju organizaciju, bez obzira na oblik infrastrukture koja se pritom koristi. Računani *cloud* to ne mijenja ali pridonosi dodatnom fokusu zbog distribuirane prirode računalne i *cloud* infrastrukture. Sigurnosni

[30] Integritet (engl. *Integrity*) se u pogledu računalnih mreža odnosi se na zaštitu informacije da bude modificirana od strane neovlaštenih entiteta.

[31] Dostupnost (engl. *Availability*) se u pogledu računalnih mreža predstavlja osiguranjem da ovlaštene osobe mogu pristupiti podatku onda kada je to potrebno

[32] Pokazivači u programiranju predstavljaju vrijednosti koje označavaju lokaciju podataka u memoriji. Pokazivači su adrese koje pokazuju na vrijednost u memoriji.

razlozi odnose se i na podatke u mirovanju (čuvani na nekom sustavu pohrane) i podacima u pokretu (koji se prenosi preko nekog oblika komunikacijske veze), oba od kojih će možda biti potrebno uzeti u obzir pozornost pri korištenju *cloud* računalnih usluga.

U suštini, pitanje koje se odnosi na podatke za računalni *cloud* o različitim oblicima rizika: rizik od krađe ili neovlaštenog otkrivanja podataka, rizik od neovlaštenog ili neovlaštenih izmjena podataka, rizik od gubitka ili nedostupnosti podataka. Također je vrijedno zapamtiti da u slučaju imovine podatka u *cloudu* je moguće uključi stvari kao što su aplikacijski programi ili strojne slike što može imati isti rizik kao i sadržaj baze podataka ili podatke datoteka.

Sigurnosni standardi za razmatranje podataka u pokretu su:

- HTTPS - za redovite veze s krajnjim korisnicima interneta na cloud usluge;
- SFTP - za prijenos hrpe podataka;
- VPN koristeći IPSec[33] ili SSL[34] - pogodno za povezivanje zaposlenika s krajnjim korisnicima *clouda*.

Za podatke u mirovanju - pohranjenim u *cloudu* - načelo je da osjetljivi podaci trebaju biti šifrirani. To može biti potrebno u skladu s nekim informacijsko sigurnosnim standardima kao što su PCI-DSS i HIPAA. Postoji više pristupa za šifriranje u *cloud computingu* - šifriranje na razini uređaja za pohranu, šifriranje na temelju agenata (engl. *Agent based*), šifriranje temeljeno na datotečnom sustavu i ono na aplikacijskoj razini. Svaki pristup ima svoje određene karakteristike koje se odnose na performanse i rukovanju šifriranim ključevima. Tu je i pitanje granulacije šifriranja - cjelokupni volumen, direktorij ili samo datoteka. Odabir pristupa ovisi o mogućnostima koje nudi davatelj usluga u oblaku, a dijelom ovise o sigurnosnim zahtjevima krajnjih korisnika *cloud* usluga [10].

[33] Ipsec je protokol koji osigurava zaštitu IP protokolu tako da se vrši autentifikacija i enkripcija svakog IP paketa komunikacijske sesije koja je u tijeku.

[34] SSL (engl. *Secure socket layer*) predstavlja standardnu sigurnosnu tehnologiju za uspostavu kriptirane veze (linka) između web servera i pretraživača (engl. *browser*). Link osigurava da svaki podatak koji prođe između poslužitelja i pretraživača ostaje privatan (kriptiran). Ovaj proces naziva se enkripcijom kanala.

Za svaki od ovih načina šifriranja, postoji mnogo algoritama za šifriranje koji se mogu koristiti [47]:

- Odabran algoritam trebao bi biti preporučen od strane standarda kao na primjer US FIPS 140-2;
- Ključevima za šifriranje (engl. *Encryption keys*) treba postupati na odgovarajući način. Ključevi ne bi trebali biti pohranjeni zajedno s podacima. Za IaaS i PaaS modele, može biti slučaj da su ključevi pohranjeni od strane krajnjeg korisnika i proslijeđeni aplikaciji po potrebi. Za SaaS model, enkripcija se nalazi u rukama davatelja usluga, u kojem slučaju treba tražiti odgovarajuća uvjerenja o rukovanju enkripcijskim ključem. protokol (KMIP)[35] koji služi za upravljanje enkripcijski ključevima pruža standardizirani način za upravljanjem ključevima kao i za šifriranje u različitim infrastrukturama. Korisnici *clouda* mogu se raspitati kod davatelja usluga *clouda* odnosno pogledati u njihovim pravilnicima je li podržavaju KMIP protokol.

10.7 Osiguranje kao sredstvo za upravljanje rizikom unutar *clouda*

Potencijalni korisnici *clouda* mogu upravljati rizikom u *cloudu* ne samo tehnološkim ili ugovornim putem već i putem osiguranja. Osiguravatelji (odvojeni entitet od davatelja usluge i korisnika) nude mogućnost korisnicima zaštite od različitih rizika koji se mogu pojaviti unutar *clouda*. Osiguravatelji mogu poticati promulgaciju najboljih primjera među *cloud* korisnicima i davateljima usluge tako da inzistiraju na kupovini sigurnosnih certifikata kao preduvjet za pokriće ili mogućnost dobivanja popusta. Uloga osiguravatelja u *cloudu* naglo raste tj. osiguravatelji postaju ključni entiteti u *cloudu*, posebice ako se nametnu stroge zakonske pretpostavke nad korisnicima *clouda* u skoroj budućnosti.

[35] KMIP protokol (engl. *Key management interoperability protocol*) je komunikacijski protokol koji definira format poruke za upravljanje kriptografskim ključevima. Ključevi se obično generiraju na serveru a onda se kasnije povlače s njega. Simetrični i asimetrični ključevi su podržani.

Tablica 4. Prikaz ovisnosti opterećenja i servisnih modela

	Poslovni proces kao servis	Softver kao usluga (SaaS)	Infrastruktura kao usluga (IaaS)	Privatni IaaS
Razvoj i testiranje	pogodan	Pogodan	pogodan	pogodan
Osjetljive informacije	pogodan	Loš	loš	pogodan
Kritične misije	pogodan	Prosječan	loš	prosječan
Suradnja	loš	Pogodan	prosječan	prosječan
Veliki broj podataka i analiza	loš	Loš	prosječan	pogodan
Visoka sposobnost računanja i analiza	loš	Pogodan	pogodan	pogodan
Relativno ugašene funkcionalnosti	pogodan	Pogodan	pogodan	pogodan

izvor: [48]

S perspektive osiguravatelja *cloud* predstavlja jednu potpuno novu paradigmu koju takav sektor još nije imao priliku doživjeti. Osiguravatelji postepeno ulaze na IT tržište i zauzimaju svoje mjesto. Tablica 4. prikazuje karakteristike funkcija koje osiguravatelji obnašaju u *cloudu*. Temeljem tih karakteristika funkcija napravljena je matrica koja prikazuje ovisnost funkcije osiguravatelja i *cloud* servisnog modela [48].

10.8 Provođenje politike privatnosti

Zaštita se prvenstveno odnosi na nabavu, skladištenje i korištenje osobnih podataka (engl. *Personally identifiable information*). Postoje zakoni i propisi u puno zemalja koje se odnose na korištenje osobnih podataka. Svaki krajnji korisnik *clouda* mora ozbiljno razmotriti bilo kakvo davanje osobnih podataka davatelju usluga *clouda*. Tipično, privatnost podrazumijeva ograničenja o uporabi i dostupnosti korisničkih podataka, s pripadajućim zahtjevima za označavanje podataka na odgovarajući način, spremiti ih na sigurno mjesto i da se omogući pristup samo na odgovarajući način i to isključivo ovlaštenim korisnicima.

Probleme vezane uz privatnost treba rješavati na razini sklopljenog ugovora *cloud* korisnika i davatelja *cloud* usluga. Trebalo bi biti u potpunosti jasno na koji način su odgovornosti podijeljene između davatelja i korisnika i također mora biti poznati pravni sustav koji je uključen u rješavanju pravnih pitanja i problema sa sklopljenim ugovorima. Vrlo je vjerojatno da će razina odgovornosti uvelike ovisiti o prirodi *cloud* usluga koje su uključene tj. ovisit će o kvaliteti samog *cloud* sustava. Za pružanje virtualnih usluga od strane IaaS modela

usluga, vrlo je vjerojatno da će pružatelj cloud usluga biti nesvjestan prirode podataka koji se pohranjuju na poslužitelju i da se sva odgovornost preusmjerava ka krajnjem korisniku koji je kupio/iznajmio server za svoje potrebe.

Za aplikaciju koja se eksplicitno bavi osobnim podacima ponuđena kao SaaS usluga od strane davatelja *cloud* usluga bilo bi prirodno očekivati da davatelj bude odgovoran za odgovarajuću zaštitu osobne informacije u službi - osobito šifriranje podataka i pružanje prikladne kontrole pristupa. Osim enkripcije praćenje aktivnosti baze podataka kao i ranjivosti baze podataka nužno je kako bi se na pravilan način u konačnici odabrao pouzdan davatelj *cloud* servisa.

Postoje neke specifikacije i norme koje se odnose na privatnost i rukovanje osobnim podacima. Jedan od utvrđenih okvira je onaj između sjedinjenih država i europske unije SAD - EU Safe Harbor framework [49], koji jamči usklađenost zahtjevima direktiva o zaštiti podataka unutar europske unije. To je još dodatno podržano od strane komercijalnih certifikata kao što je TRUSTe Safe Harbor certifikat. klijenti mogu koristiti taj okvir kao jamstvo da će davatelj usluga štititi osobne podatke krajnjeg korisnika na primjeren način [45]. Više o Safe Harbour pisano je u poglavlju 9 [10].

10.9 Osiguranje *cloud* mreže i sigurnosnih konekcija

Davatelj *cloud* usluga mora omogućiti legitiman i nesmetan mrežni promet i ispuštanje odnosno uklanjanje zlonamjernog (engl. *Malicious*) mrežnog prometa baš kao što to rade i ostale organizacije čiji se dobar dio poslovanja odvija na Internetu. Međutim, za razliku od puno drugih organizacija, davatelj usluga neće nužno moći uvijek predvidjeti sadržaj kojeg mrežni promet nosi i koji se pohranjuje na njegov poslužitelj. Upravo zbog mogućnosti zlonamjernih Internet paketa korisnici bi trebali očekivati određenu zaštitu vanjske mreže perimetra i mjere odvajanja unutarnjih mreža od svojeg *clouda*.

Jedan od načina osiguravanja *cloud* mreže i sigurnosnih konekcija opisane su ISO/IEC 27001 i ISO/IEC 27002 standardima, koji su opisani u 7. poglavlju ovog rada.

Savezna agencija za rizik i program za autorizacijskim upravljanjem (FedRAMP) nudi odobrenja za davatelje *cloud* usluga kako bi omogućili pristup američkim informacijskim

sustavima. Ne postoje nove kontrole za FedRAMP. FedRAMP sigurnosne kontrole temelje se na NIST posebnoj publikaciji 800-53 R3 kontrole za niske i umjerene sustave utjecaja, a sadrže kontrole i poboljšanja iznad NIST osnovica za niske i umjerene sustave utjecaja koji se bave jedinstvenim elementima računalnog *clouda*. Postoji veliki broj organizacija za ocjenjivanje trećih osoba koje mogu potvrditi je li *cloud* udovoljava svim kriterijima koje nalaže FedRAMP [10].

TM Forum također održava TM Forum sučelje X (engl. *Frameworks*) [50], koji predstavlja najbolju praksu i standarde koji omogućuju „nacrt" za učinkovito i djelotvorno poslovanje. Treba napomenuti da ti dokumenti samo pomažu davatelju usluge u izradi strategije. Kako bi se učinkovito ublažio rizik, politika mora biti potpomognuta od strane kvalificiranih zaposlenika i mrežne arhitekture koja je unaprijed testirana od strane stručnjaka.

Relativno novi koncept umrežavanja su "Softverski definirane mreže" (SDN), koje omogućuju kontrolu mreže i prosljeđivanje funkcija gdje se te operacije koriste odvojeno. Iako je arhitektura mreže drugačija, većina istih sigurnosnih kontrola odnose se na SDN. Iako postoje standardi za SDN protokole, kao što su *OpenFlow*[36], zasad ne postoje specifični SDN sigurnosni standardi.

U ovom trenutku, sigurnosni mrežni certifikat je i dalje rijetkost, a samo najvećim davateljima *cloud* usluga omogućena je certifikacija u skladu s ISO 27002.

Ipak, ako *cloud* usluga nema sigurnosnu mrežnu potvrdu ili certifikat, korisnici bi trebali barem osigurati da pružatelj usluga posjeduje dokumentaciju i da je proveo testiranje za sljedeće procese:

- Pristup kontroli za upravljanje mrežnom infrastrukturom;
- Filtriranje prometa, pružanje vatrozida;
- Stvaranje sigurne virtualne privatne mreže (VPN, ako je ponuđena);
- Otkrivanje upada i način prevencije iste;
- Ublažavanje posljedica DDoS (engl. *Distributed denial of service*[37]);
- Prijava i obavijesti, tako da sustavni napadi mogu biti pregledani.

[36] OpenFlow je otvoreni standard koji omogućuje znanstvenicima da testiraju eksperimentalne protokole.

[37] DDoS je tip računalnog napada odnosno napada kojim se ugrožava više sustava koji bivaju zaraženi najčešće Trojan virusom.

10.10 Upravljanje sigurnosnim uvjetima u *cloudu* posredstvom SLA ugovora

Kako *cloud* tipično uključuje dva entiteta – davatelja usluga i krajnjeg korisnika, odgovornosti svake strane moraju biti jasno istaknute. To se obično obavlja putem ugovora o razini usluge (engl. *Service level agreement*), koji se odnosi na usluge koje pružaju, kao i uvjetima ugovora o uslugama između klijenta i davatelja usluga. SLA ugovor treba navesti sigurnosne odgovornosti i treba uključiti određene aspekte, od kojih je jedan primjer izvještavanje o narušavanju sigurnosti.

Metrike za mjerenje performansi i učinkovitost upravljanja informacijskom sigurnošću treba utvrditi prije pretplate na *cloud* usluge i također trebaju biti navedene u *cloud* SLA ugovoru. Organizacije trebaju razumjeti i dokumentirati njihove trenutne podatke (podatke krajnjeg korisnika) i kako će se oni promijeniti kada će različite operacije koristiti *cloud* i gdje davatelj usluga može upotrijebiti različitu metriku.

Mjerenje i izvještavanje o usklađenosti pružatelja s obzirom na zaštitu podataka krajnjeg korisnika moguće je izmjeriti tj. valorizirati na temelju učinkovitosti sigurnosnog plana cjelokupnog poduzeća. Izvješće o sukladnosti podataka ili informacijska sigurnost ovjere treba zahtijevati od davatelja usluga u *cloudu* jer to odražava snagu ili slabost kontrole, usluge i mehanizme podržanih od strane davatelja usluga u svim sigurnosnim domenama. U ovom trenutku, ne postoje standardi za opisivanje i mjerenje specifičnih podatke o sigurnosti u *cloudu*. Jednokratne ili periodične procjene usluga, kao što su ISO 2700x, SSAE 16 ili ISAE 3402, uvjeravaju da je za probnog razdoblja određeni skup kontrola i procedura bio na mjestu. Ove procjene su vitalni dio učinkovitog upravljanja sigurnošću. Međutim, oni su nedovoljni bez dodatne povratne informacije u intervalima između procjena, oni ne daju informacije u stvarnom vremenu.

Postoji nekoliko standardnih inicijativa koje su u tijeku i promatraju pobliže zajedničku metriku kao i pristupe upravljanju za SLA ugovore uključujući sigurnosnu metriku u *cloudu*. Konkretno, TM Forum radi na tehničkom izvješću pod nazivom poticajni „*End-to-end Cloud SLA Management*“ odnosno uspostava upravljanjem SLA ugovora od kraja do kraja (od korisnika do davatelja usluga). U izvješću se daje skup zajedničkih pristupa za dvije stranke kako bi se odredio njihov SLA unutar *clouda*. Potrebno je definirati što će se mjeriti, krajnje granice i indikatore kao i arhitekturalna načela dizajna kako bi se upravljanje SLA-om moglo

postići od kraja do kraja automatiziranim procesom i arhitekturalnom fleksibilnošću za podržavanje različite korisničke i poslovne zahtjeve [10].

Dodatni izvori koji sadržavaju specifične informacije o sigurnosnoj metrici također su dostupni. Iako ti izvori nisu strogo namijenjeni *cloudu*, pružaju vrijedne smjernice koje se mogu primijeniti u tradicionalnim organizacijama kao i *cloud* okruženju. Te smjernice su [10], [51], [52]:

- ISO 27004:2009;
- NIST specijalna publikacija (SP) 800-55 Rev. 1, Vodič za mjerenje performanse informacijske sigurnosti;
- CIS, konsenzus sigurnosne metrike v1.1.0.

Europska agencija za mrežnu i informacijsku sigurnost (ENISA, engl. *The European Network and Information Security Agency*, [53]) objavila je vodič pod nazivom „Osigurajte si osiguranje (engl. *Procure secure*) ". Vodič služi praćenju sigurnosnih razina u *cloud* okruženju. Vodič opisuje glavne zahtjeve s kojima krajnji korisnik/klijent mora biti upoznat prilikom zauzimanja prostora odnosno, iznajmljivanje prostora na *cloudu*.

Tako se osigurava strogo pridržavanje sigurnosnih protokola. To uključuje prateći sigurnosni okvir koji daje odgovor na sljedeća pitanja [10]:

- Što mjeriti, koje sigurnosno relevantne parametre treba pratiti;
- Kako ih mjeriti, kako se podaci mogu prikupljati u praksi;
- Kako dobiti neovisna mjerenja. Koje sigurnosno relevantne značajke se mogu pratiti neovisni o davatelju usluga i na koji način ih se može sve pratiti.
- U kojem trenutku prijaviti problem, kada on postaje ozbiljan za korisnika i/ili davatelja usluge;
- Odgovornosti korisnika. Čiji je to problem. Što treba poduzeti davatelje usluge i slučaju pojavljivanja problema na strani krajnjeg korisnika.

Specifične metrike obuhvaćene u priručniku uključuju: dostupnost servisa, odgovor na problem, elastičnost servisa i tolerancija na veličinu podataka, upravljanje životnim ciklusom podataka, tehnička usklađenost i upravljanje ranjivošću, upravljanje promjenama, izolacija podataka i upravljanje autentifikacijama i forenzikom [54].

U javnom sektoru, vladine agencije mogu dati smjernice o tome kako riješiti sigurnosne zahtjeve i uvjete u oblaku temeljem SLA ugovora. Na primjer, američki *General Services Administration* (GSA) posjeduje dokumentirana područja od interesa, u kontekstu sigurnosnih zahtjeva *clouda*, što može zahtijevati dodatne ugovorne klauzule. Upute detaljiziraju sigurnosne uvjete na razini sigurnosnih kontrola i omogućavaju predloške koji se mogu koristiti za dokumentiranje tehničkih uvjeta. Upute od strane GSA odnose se na područja koja predstavljaju zabrinutost poslovnih subjekata i stoga mogu imati i veći utjecaj [10], [55].

10.11 Odlazak korisnika iz *cloud* okruženja i prekid ugovora

Proces izlaska ili prestanka korištenja *cloud* usluge od strane kupca/krajnjeg korisnika zahtijeva pažljivo razmatranje iz perspektive informacijske sigurnosti. Ukupna potreba za dobro definiranim i dokumentiranim procesom izlaza iz *clouda* opisana je u CSCC dokumentu "Praktični vodič za *Cloud Service* sporazumne razine, verzija 1.0, [10]“

Iz sigurnosne perspektive, važno je da kada klijent završi proces raskida ugovora "reverzibilnost" ili "proces prava na zaborav" je postignut tj. svi podaci od klijenata moraju biti izbrisani na *cloudu* od strane davatelja usluga. Pružatelj mora osigurati brisanje svih kopija podataka iz *cloud* okruženja, neovisno o tome na kojoj lokaciji su pohranjeni (uključujući rezervne lokacije, kao i *online* trgovine podataka). Isto tako ostali podaci (npr. metapodaci korisnika) trebaju biti izbrisani od strane davatelja. U nekim državama metapodaci korisnika ostaju pohranjeni neko vrijeme kod davatelja usluga sve dok korisnik eksplicitno ne zatraži brisanje podataka.

Tu je suprotan problem tijekom samog procesa izlaza, tj. napuštanja *clouda* - korisnik mora moći izvršiti napuštanje *clouda* bez ikakvih poteškoća od strane sustava tako da se taj prijelaz izvrši bez gubitka ili povrede podataka. Postupak izlaska iz *clouda* mora omogućiti korisnicima dohvaćanje svojih podataka na siguran način a kopije se moraju čuvati u dogovorenim vremenskim rokovima prije nego što budu eliminirane zajedno sa zapisnicima događaja i izvještajima. Na kraju napuštanja *cloud*, od strane korisnika, praksa pružatelja usluge *clouda* je osiguravanje potvrde korisniku kojom se potvrđuje kako je korisnik zaista napustio sustav. Tako davatelj usluge štiti sebe i svoju organizaciju u slučaju mogućeg podnošenja tužbe.

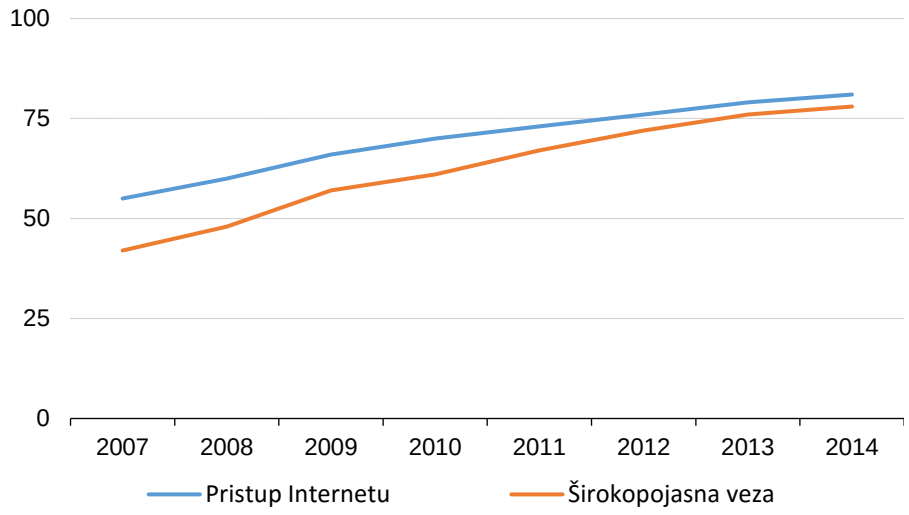
Konkretnih standardi za računalni *cloud*, a vezani za korisničko napuštanje *clouda*, ne postoje već se standardizacija obavlja uzimajući u obzir druge već postojeće standarde koji su primjenjivi u IT-u. ISO izvješće preporučuje pravilno adresiranje subjekata prilikom prekida korištenja i izlaza iz *clouda* i kreiranje novih elementa kojim bi se preispitale i objasnile rupe u tom području (izlazak korisnika). Specifični standardi i pravilnici vjerojatno neće osigurati rješavanje pitanja korisničkog izlaska iz *cloud* okruženja. U međuvremenu krajnji korisnik i davatelj usluga moraju zajedno dogovoriti izlazak iz *clouda* i to na što jednostavniji način (pogotovo za korisnika) držeći se pritom pravila i odredbi definiranih SLA ugovorom [10].

11 EKONOMSKI UČINAK U *CLOUD* POSLOVANJU

Prije analize ekonomskog učinka *cloud* poslovanja, potrebno je analizirati statistiku uporabe Interneta. Zbog toga se u prva dva potpoglavlja diplomskog rada analizira statistika uporabe Interneta za privatne korisnike i statistika uporabe *cloud* okruženja za poslovne korisnike. Analizirani podaci preuzeti su s EUROSTAT-a.

11.1 Statistika uporabe Interneta za privatne korisnike

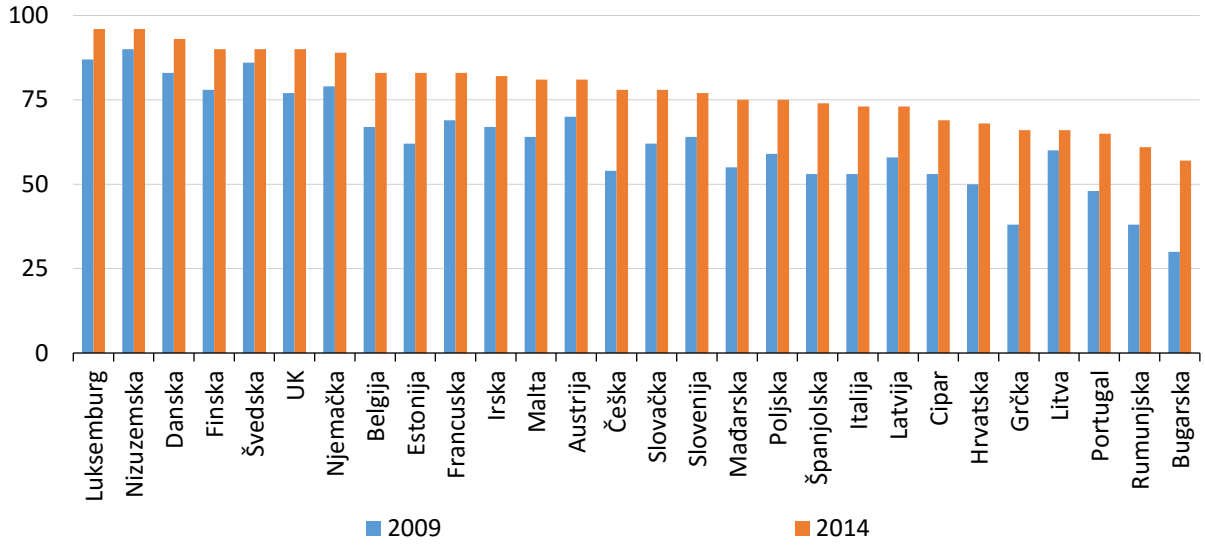
Prema izvješću EUROSTAT-a, iz 2015. godine, u razdoblju između 2007. i 2014. godine broj privatnih (rezidencijalnih) korisnika Interneta, odnosno postotak kućanstava koji imaju pristup Internetu se povećava. Identičan trend je vezan i za postotak korištenja širokopojasne veze. Trend pristupa Internetu i širokopojasnoj vezi prikazan je grafikonom 1.



Grafikon 1. Trend rasta pristupa Internetu i trend rasta širokopojasne veze za privatne korisnike
izvor: [56]

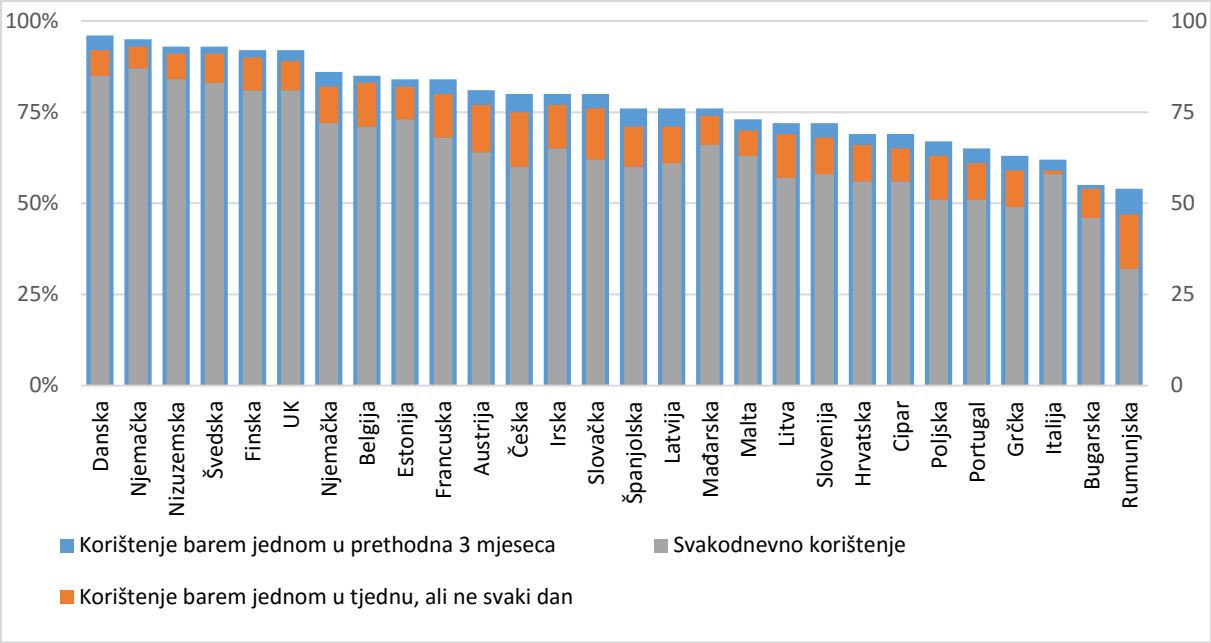
Na grafikonu 2. prikazan je postotak korisnika koji imaju pristup Internetu u vlastitom kućanstvu. Prema grafikonu 2. vidljivo je kako najveći postotak korisnika, koji imaju pristup Internetu, se nalazi u Luksemburgu (96% stanovnika u 2014. godini), a najmanji postotak korisnika s pristupom Internetu je u Bugarskoj, gdje samo 57% ima pristup Internetu. U

Hrvatskoj 68% stanovnika ima pristup Internetu. U odnosu na 2009. godinu, vidljivo je povećanje od 18%.



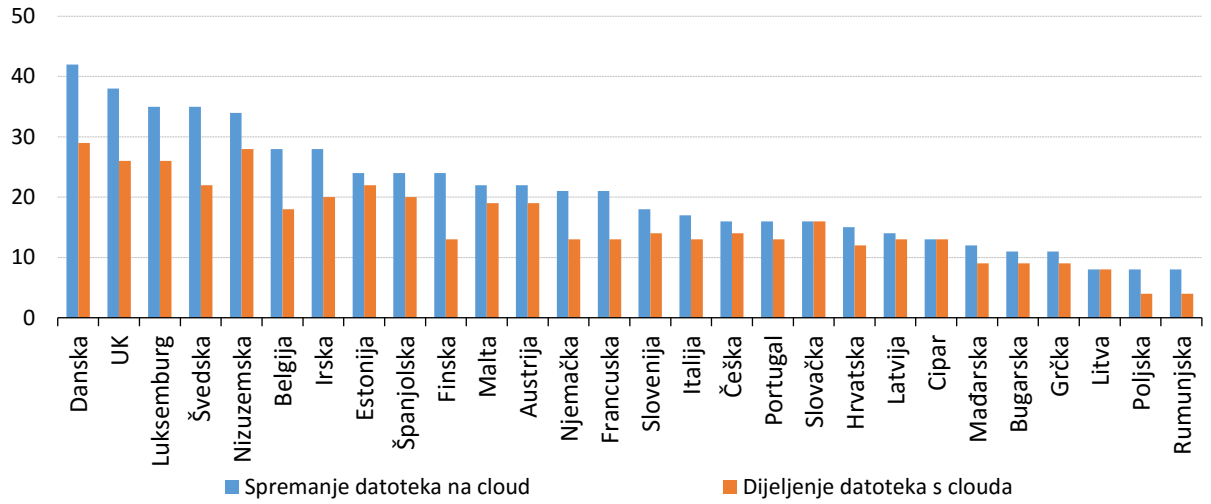
Grafikon 2. Postotak pristupa Internetu u kućanstvima 2009. i 2014. godine
izvor: [56]

Prema podacima prikazanim grafikonom 3., a prema ispitivanjima provedenima među populacijom u dobi od 16 do 74 godine, vidljivo je kako najviše ispitanika svakodnevno koristi Internet, a najmanje jako rijetko, odnosno barem jednom u prethodna tri mjeseca. Međutim, Hrvatska ne prati taj trend. U Hrvatskoj 56% ispitanika koristi Internet svakodnevno.



Grafikon 3. Postotak korištenja Interneta u populaciji između 16 i 74 godina
izvor: [56]

Grafikon 4. prikazuje postotak ispitanika, u dobi između 16 i 74 godina koji koriste *cloud* okruženje za spremanje datoteka i za dijeljenje datoteka. Iz grafikona 4. vidljivo je kako veći postotak ispitanika koristi *cloud* za spremanje datoteka nego za dijeljenje datoteka.



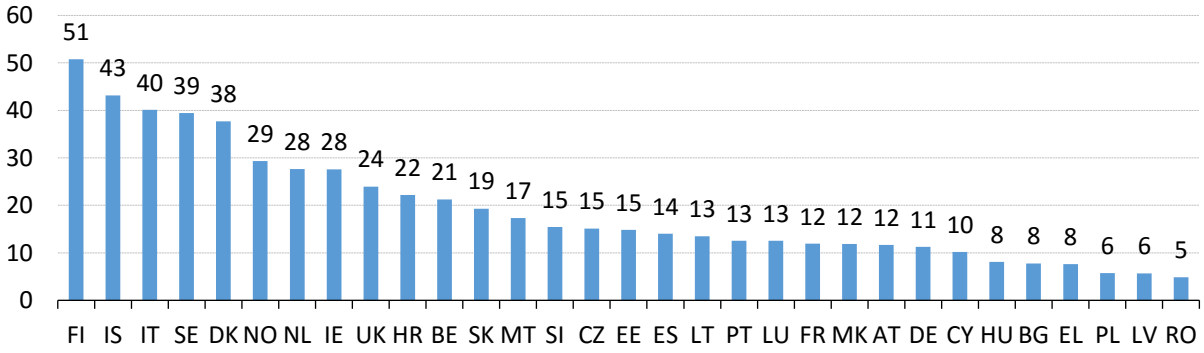
Grafikon 4. Postotak ispitanika koji koriste *cloud* okruženje
izvor: [56]

Iz navedenih grafikona (1-4) vidljivo je kako većina privatnih korisnika svakodnevno koristi Internet. Također, primijećen je trend porasta broja priključaka u kućanstvima u zadnjih

pet godina. Sukladno navedenome, može se zaključiti kako *cloud* okruženje ima mogućnost penetracije na tržište u odnosu na tradicionalno korištenje Internet usluga.

11.2 Statistika uporabe *cloud* okruženja za poslovne korisnike

Zbog potrebe za opstankom na tržištu od poslovnih korisnika očekuje se korištenje Internet usluga. Međutim, kako je tržište dinamično danas bi poslovni korisnici trebali svoje poslove koji se baziraju na računalima prebaciti na *cloud* okruženje. Grafikonom 5. prikazan je postotak korištenja *cloud* okruženja za poslovne korisnike.



Grafikon 5. Postotak korištenja *cloud* okruženja za poslovne korisnike
izvor: [57]

Osim postotaka korištenja *cloud* okruženja potrebno je utvrditi za koje sve aktivnosti poslovni korisnici koriste *cloud* okruženje. Tablicom 5. prikazano je koliki postotak poslovnih korisnika koristi *cloud* okruženje za određene aktivnosti.

Tablica 5. Postotak korištenja *cloud* računalstva za različite aktivnosti

	Korištenje *clouda*	E-pošta	Spremanje datoteka	Baza podataka	Uredski programi	Financijski i računovodstveni programi	CRM[38]	Računalna snaga za pokretanje vlastitih programa
	% poslovnih korisnika	% poslovnih korisnika koji koriste *cloud* okruženje						
EU28	19	66	53	39	34	31	21	17
BE	21	52	62	45	31	33	26	23
BG	8	74	50	53	58	50	24	16
CZ	15	79	41	34	38	35	18	20
DK	38	63	70	55	42	49	34	34
DE	11	46	56	33	21	25	18	20
EE	15	58	41	18	41	47	17	7
IE	28	57	74	37	36	25	23	17
EL	8	67	50	36	31	32	25	26
ES	14	61	69	54	28	21	24	25
FR	12	62	61	49	32	26	23	14
HR	22	85	49	46	52	50	13	26
IT	40	86	32	28	41	33	14	8
CY	10	68	70	26	39	23	29	16
LV	6	58	58	55	42	47	19	26
LT	13	70	50	47	34	45	33	38
LU	13	46	61	41	32	19	18	14
HU	8	64	46	33	43	35	25	20
MT	17	60	57	44	31	17	19	19
NL	28	55	63	64	40	52	37	18
AT	12	51	54	31	33	23	23	16
PL	6	69	54	41	31	27	22	19
PT	13	78	49	31	36	31	18	30
RO	5	76	36	37	37	33	0	19
SI	15	67	44	39	35	33	20	29
SK	19	84	34	31	46	54	13	22
FI	51	66	54	38	39	39	29	13
SE	39	55	65	43	32	37	26	25
UK	24	51	71	44	29	25	24	22

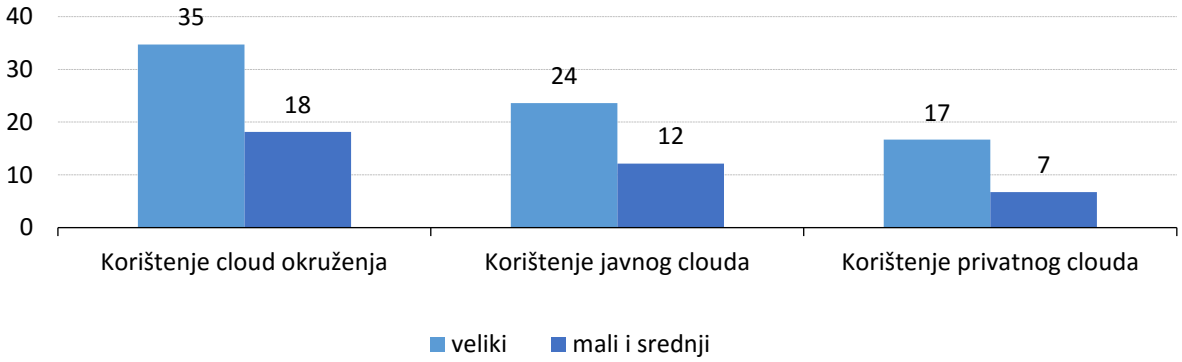
izvor: [57]

Iz tablice 5. vidljivo je kako najveći postotak poslovnih korisnika koristi *cloud* okruženje za slanje elektroničke pošte. Najmanji postotak poslovnih korisnika koristi *cloud* okruženje za pokretanje vlastitih programa korištenjem fizičkih resursa *cloud* okruženja.

Na kraju prikaza ove statistike prikazat će se koliki postotak poslovnih korisnika koristi različite izvedbe *cloud* okruženja (privatni i javni *cloud*). Za potrebe prikaza poslovni korisnici

[38] CRM (engl. C*ustomer relationship management*) je sustav za upravljanje odnosima prema kupcima.

su podijeljeni na velike i male te srednje poslovne korisnike. Prikaz poslovnih korisnika koji koriste javni i privatni oblak prikazan je grafikonom 6.



Grafikon 6. Korištenje različitih izvedbi *cloud* okruženja od strane poslovnih korisnika
izvor: [57]

Iz grafikona 6. vidljivo je kako većina poslovnih korisnika nema potrebe za korištenjem privatnog oblaka zato radije koriste javni oblak. Isto se može protumačiti na tri načina. Korisnici zbog ekonomskih razloga ne koriste privatni *cloud*, korisnici nemaju potrebe za čuvanjem podataka pa ne koriste privatni *cloud* i/ili korisnici dijele podatke s drugim poslovnim korisnicima te zbog toga koriste javni *cloud*.

11.3 Ekonomski aspekti *cloud* poslovanja

Ekonomski aspekt *cloud* poslovanja može se podijeliti na tri osnovna elementa:

- Cijenu;
- Koristi i rizik *cloud* okruženja;
- Provjeru mogućnosti uvođenja *cloud* okruženja u organizaciju.

Osim navedena tri osnovna elementa u obzir kao ekonomski aspekt može se uzeti održavanje računalnih sustava. Prema Gartnerovoj analizi [58], 80% ukupnih troškova u IT sektoru predstavljaju troškovi održavanja IT sustava. Primjenjujući načelo Paretovog principa [59], previđa se kako je moguće korištenjem *cloud* okruženja smanjiti troškove s 80% na 20%, ukupnih troškova predviđenih za IT sektor u nekoj organizaciji. Prema navedenoj analizi, 20% ukupnih troškova odnosilo bi se na: operativne sustave, poslužitelje i data centre a 80%

previđenih troškova, organizacija bi mogla koristiti za izradu i održavanje aplikacija potrebnih organizaciji.

Također, u članku [60], analizirani su načini naplate korištenih resursa u *cloud* okruženju. Naplata korištenih resursa predviđa dinamičan mehanizam određivanja cijena, temeljen na alokaciji dijeljenih resursa. Ekonomska svojstva ovog načina određivanja cijena dokazana su pomoću mehanizma dizajniranja okvira cijena [61].

11.3.1 Koristi i rizik *cloud* okruženja

Prema literaturi [60], za organizacije su navedene tri osnovne koristi korištenjem *cloud* okruženja:

- Operativna korist;
- Ekonomska korist;
- Kadrovska korist.

Operativna korist predstavlja sve koristi koje su vezane za operativu određene organizacije a u nju se mogu nabrojati:

- Povećanje prostora za pohranu;
- Automatizacija;
- Povećanje mobilnost;
- Fleksibilnost.

Ekonomska korist predstavlja sve oni koristi koje su vezane za smanjivanje troškova. Osim smanjivanja troškova u ekonomsku korist ubrajaju se i sve koristi koje služe i povećanju dobiti određene organizacije.

Kadrovska korist vezana je uz zaposlenike organizacije. Primjer kadrovske koristi, primjenom *cloud* okruženja je kvalitetniji rad IT stručnjaka u organizaciji. Na primjer IT stručnjaci u organizaciji neće dane provoditi otklanjajući kvarove na različitim uređajima, već će se posvetiti kvalitetnijim zadaćama koje mogu organizaciji donijeti ekonomsku korist.

Osim navedenih koristi za organizaciju, koristi *cloud* okruženja mogu se promatrati iz pogleda korisnika i iz pogleda davatelja usluge. Iz pogleda korisnika, koristi *cloud* okruženja su:

- Nema potrebe za instalaciju niti održavanjem sustava;
- Kraće vrijeme pokretanja;
- Dostupnost sustava širom svijeta;
- Davatelj usluge se pridržava uvjeta iz SLA ugovora;
- Davatelj se obvezuje stalno usavršavati sustav.

Koristi za davatelja usluge *cloud* okruženja su:

- Posjedovanje radnog okruženja, odnosno fizičkih elemenata *cloud* okruženja;
- Predvidljivi pritok prihoda;
- Male i redovite nadogradnje sustava;
- Sustav za upravljanje odnosima s kupcima.

Osim mogućih koristi *cloud* okruženja potrebno je promotriti i moguće rizike korištenja istoga. Rizici u *cloud* okruženju su:

- Rizik od napada hakera;
- Rizik korištenja istog *cloud* elemenata od strane više korisnika;
- Zaštita granica virtualnih strojeva;
- Rizici vezani za neetično korištenje *cloud* okruženja.

Kao što je vidljivo iz nabrojanih rizika većina rizika je posredno vezana uz mogući gubitak ili promjene informacija. Dolaskom do potencijalnog gubitka ili promjene informacija, organizacija može pretrpjeti određenu materijalnu štetu [60].

11.3.2 Provjera mogućnosti uvođenja *cloud* okruženja u organizaciju

Utvrđivanje prikladnosti (sposobnosti) organizacije za uvođenjem *cloud* okruženja je radnja koja prethodi uvođenju *cloud* okruženja u organizaciju. S tim ciljem u [62], predstavljen je matematički model koji računa prikladnost organizacije za uvođenjem *cloud* okruženja.

Matematički model računa prikladnosti uzimajući u obzir relevantne faktore kojima se dodjeljuje težinska vrijednost koja ovisi o važnosti pojedinog faktora. Neki od tih faktora su:

- Veličina IT sektora (broj poslužitelja, veličina baze korisnika, godišnji prihod od IT usluga i dr.);
- Uzorak korištenja IT resursa (prosječno korištenje, vršno korištenje, veličina podataka, s kojima se radi);
- Osjetljivost organizacijskih podataka;
- Kritičnost posla kojeg radi organizacija.

Ubacivanjem vrijednosti u matematički model kao rezultat dobije se određena numerička vrijednost. Ako je vrijednost te numeričke vrijednosti manja od određene propisane vrijednosti organizacija nije sposobna uvesti *cloud* okruženje.

11.3.3 Prikaz različitih cijena za neke davatelje *cloud* usluga

Prije prikaza različitih cijena za neke davatelje *cloud* usluga potrebno je napomenuti kako su davatelji usluga jako prilagodljivi prilikom izgradnje mreže uređaja. Iako su prilagodljivi, može se javiti problem koji nastaje zbog mogućnosti rušenja poslužitelja ili gubitka podataka prilikom obavljanja određenog posla.

Ako korisnik *cloud* usluge želi sigurnost podataka, odnosno da ne dođe do mogućnosti rušenja poslužitelja ili gubitka podataka mora podatke pohraniti u podatkovnu memoriju *clouda*. Pohrana podataka u navedenu memoriju, zbog povišene razine usluge novčano košta više.

Svaka organizacija ima drukčije načine naplaćivanja svoje usluge [4]. Usporedba okvirnih cijena nekih od davatelja *cloud* usluge prikazana je tablicom 6. Osim navedenih cijena, Amazon naplaćuje i prijenos pohranjenih podataka, za mjernu jedinicu od 10K aplikacijskih zahtjeva naplaćuju 0,01 USD.

Tablica 6. Cijene Googlovih, Amazonovih i Microsoftovih *cloud computing* usluga

		Google	Amazon	Microsoft
Resurs	**Jedinica**	**Cijena u USD [$]**		
Premještanje podataka na poslužitelj	GB	0,12	0,10	0,10
Premještanje podataka s poslužitelja	GB	0,10	0,15	0,14
Vrijeme CPU	Sati rada CPU	0,10	0,12	0,125
Pohrana podataka	GB mjesečno	0,15	0,15	0,15

izvor: [4]

GoGrid organizacija koristi Intel Xeon poslužitelje, koji se smatraju snažnijim poslužiteljima nego poslužitelji drugih organizacija, stoga povećavaju cijenu svojih usluga. Google ne naplaćuje svoju uslugu po vremenu trajanja, već po broju ciklusa procesora. Amazon EC2 koristi strojeve uobičajene veličine ali i one većih kapaciteta. Korištenjem strojeva većih kapaciteta Amazon naplaćuje korisnicima višu cijenu. Prilikom mijenjanja troškova organizacije često smanjuju cijene. Sukladno kada se ispostavi da je cijena usluge viša od očekivane, organizacije krajnjem korisniku povećavaju cijenu korištenja usluge [4].

12 ZAKLJUČAK

Računalni *cloud* je pojam koji ne opisuje jednu stvar, to je opći pojam koji označava niz različitih usluga od infrastrukture kao usluge na bazi, preko platforme kao usluge za razvoj softvera kao servisna zamjena za razvoj aplikacija. Sve veći broj organizacija diljem svijeta polako se prilagođava *cloud* paradigmi koja se pokazala kao neizostavnim djelom u unaprjeđenju poslovnih sposobnosti. Važno je razumjeti različite aspekte *clouda* i procijeniti situaciju i odlučiti koje vrste rješenja su prikladne za određen posao koje organizacija obnaša.

Cloud računarstvo ubrzava revoluciju u IT-u, te će zasigurno postati glavna metoda u isporuci IT usluga. Preporuka organizacijama je da razmotre svoj pristup prema *cloudu* i da što prije iskoriste potencijal ove nove Internet paradigme.

Računalni *cloud* ima potencijal postati nova sila koja će napraviti pozitivni poremećaj u tehnološkom svijetu. *Cloud* bi mogao biti sljedeća evolucija u povijesti računalstva tako sljedeći korake mikroračunala, desktop računala, poslužitelja, pametnih mobilnih uređaja itd. Računalni *cloud* promijenit će način na koji velike kompanije upravljaju IT-em. Još uvijek postoji niz pitanja oko sigurnosti *clouda* ali s vremenom će se naći rješenje za većinu njih te tako maksimalno povećati sigurnost računalno clouda.

Računalni *cloud* je relativno novi koncept koji predstavlja dobar niz pogodnosti za svoje korisnike, međutim, isto tako računalni *cloud* podiže sigurnosne probleme koji mogu usporiti njegovu uporabu. Razumijevanjem ranjivosti koje postoje u *cloud* pomoći će organizaciji napraviti pomak prema *cloudu.* Računalni cloud iskorištava mnoge postojeće tehnologije u svrhu sveobuhvatne optimizacije *cloud* okruženja ali i nasljeđuje mnoge sigurnosne probleme poput tradicionalnih web aplikacija, usluge spremanja podataka, virtualizacija i sl. Rješenja za savladavanje navedenih problema još uvijek su nezrela ili nepostojeća. U radu su prezentirani prednosti i nedostaci različitih *cloud* modela koji su dostupni krajnjem korisniku (Iaas, PaaS, SaaS). Kako je opisano u radu, pohrana, virtualizacija i mrežna sučelja predstavljaju najveće sigurnosne rizike. Virtualizacija koja omogućuje podjelu fizičkog servera između više korisnika je jedan od glavnih razloga zabrinutosti kod krajnjeg korisnika. Isto tako još jedan izazov jest da postoje različite tehnologije virtualizacije, a što je broj tehnologija nekog rješenja veći to je vjerojatnost sigurnosnih propusta veća. Mrežna virtualizacija podložna je hakerskim napadima pogotovo kada se ostvaruje komunikacija s udaljenim virtualnim računalima.

POPIS LITERATURE

[1] A. Mohamed, »A history of cloud computing,« 2009. [Mrežno]. Available: http://www.computerweekly.com/feature/A-history-of-cloud-computing. [Pokušaj pristupa kolovoz 2016].

[2] A. Chittora, »History of Cloud Computing,« Ožujak 2012. [Mrežno]. Available: https://techbyt.wordpress.com/2012/03/07/history-of-clouds/. [Pokušaj pristupa Kolovoz 2016].

[3] G. Purohit, J. M.P. i S. Pandey, »Challenges Involved in Implementation of ERP on Demand Solution: Cloud Computing,« *International Journal of Computer Science,* svez. 9, br. 4, pp. 481-489, 2012.

[4] CARNet, »Cloud computing,« CARNet, Zagreb, 2010.

[5] »Cloud Computing: Od ideje do realnosti,« Siječanj 2016. [Mrežno]. Available: http://e-student.fpz.hr/Predmeti/S/Sustavi_elektronickog_poslovanja/Materijali/09_-_Cloud_Computing.pdf. [Pokušaj pristupa Kolovoz 2016].

[6] B. Kepes, »Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS,« 2016. [Mrežno]. Available: https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/. [Pokušaj pristupa Kolovoz 2016].

[7] T. Zorić, »Usluge društvenog umrežavanja zasnovane na računarstvu u oblaku,« Lipanj 2012. [Mrežno]. Available: https://www.fer.unizg.hr/_download/repository/Zavrsni_rad_-_Tina_Zoric.pdf. [Pokušaj pristupa Kolovoz 2016].

[8] »The Essential Characteristics of PaaS,« Veljača 2010. [Mrežno]. Available: https://www.cloudpulsestrat.com/posts/the-essential-characteristics-of-paas. [Pokušaj pristupa Kolovoz 2016].

[9] K. Krechmer, »Cloud Computing Standardization,« [Mrežno]. Available: http://www.isology.com/pdf/Standardizationisanevolutionaryprocess.pdf. [Pokušaj pristupa Kolovoz 2016].

[10] Cloud Standards Customer Council, *Cloud Security Standards: What to Expect & What to Negotiate,* 2013.

[11] J. Hurwitz, R. Bloor, M. Kaufman i F. Halper, »Cloud Computing Standards Organizations,« [Mrežno]. Available: http://www.dummies.com/how-to/content/cloud-computing-standards-organizations.html. [Pokušaj pristupa Kolovoz 2016].

[12] HAKOM, »HAKOM: Godišnji plan rada za 2015.,« Srpanj 2014. [Mrežno]. Available: https://www.hakom.hr/UserDocsImages/2014/izvjesca_i_planovi/Godisnji%20program%20rada%20HAKOM-a%20za%202015.pdf. [Pokušaj pristupa Kolovoz 2016].

[13] AZOP, »Djelaznosti i unutarnje ustrojstvo Agencije,« [Mrežno]. Available: http://azop.hr/djelatnost-agencije. [Pokušaj pristupa Kolovoz 2016].

[14] ISACA, »About ISACA,« [Mrežno]. Available: http://www.isaca.org/about-isaca/Pages/default.aspx. [Pokušaj pristupa Kolovoz 2016].

[15] ISACA, »Membership, Guidance and Certification for IT Professionals,« [Mrežno]. Available: http://www.isaca.org/About-ISACA/What-We-Offer-Whom-We-Serve/Pages/default.aspx. [Pokušaj pristupa Kolovoz 2016].

[16] The Cloud Security Alliance, »About,« [Mrežno]. Available: https://cloudsecurityalliance.org/about/. [Pokušaj pristupa Kolovoz 2016].

[17] Distributed Management Task Force, »DMTF Frequently Asked Questions,« [Mrežno]. Available: http://www.dmtf.org/about/faq. [Pokušaj pristupa Kolovoz 2016].

[18] Distributed Management Task Force, »DMTF Management Technologies Diagram,« [Mrežno]. Available: http://www.dmtf.org/managementtechnologiesdiagram. [Pokušaj pristupa Kolovoz 2016].

[19] Open Commons Consortium, »About,« [Mrežno]. Available: http://occ-data.org/about/. [Pokušaj pristupa Kolovoz 2016].

[20] The Open Commons Consortium, »Working Groups,« [Mrežno]. Available: http://occ-data.org/working-groups/. [Pokušaj pristupa Kolovoz 2016].

[21] Open Grid Forum, »An Open Global Forum for Advanced Distributed Computing,« [Mrežno]. Available: https://www.ogf.org/ogf/doku.php. [Pokušaj pristupa Kolovoz 2016].

[22] Open Cloud Computing Interface, »Open Cloud Computing Interface,« [Mrežno]. Available: http://occi-wg.org/. [Pokušaj pristupa Kolovoz 2016].

[23] The Object Management Group, »About OMG,« [Mrežno]. Available: http://www.omg.org/gettingstarted/gettingstartedindex.htm. [Pokušaj pristupa Kolovoz 2016].

[24] The Cloud Standards Customer Council, »Making cloud standards customer-driven,« [Mrežno]. Available: http://www.cloud-council.org/about-us.htm. [Pokušaj pristupa Kolovoz 2016].

[25] G. Vojković, »Normizacija u elektroničkim komunikacijama,« Siječanj 2015. [Mrežno]. Available: http://e-student.fpz.hr/Predmeti/T/Telekomunikacijska_legislativa_i_standardizacija/Materijali/Normizacija_u_elektronickim_komunikacijama.pdf. [Pokušaj pristupa Kolovoz 2016].

[26] J. Bourne, »ISO publishes new cloud computing standards and definitions,« Listopad 2014. [Mrežno]. Available: http://www.cloudcomputing-news.net/news/2014/oct/20/iso-publishes-new-cloud-computing-standards-and-definitions/. [Pokušaj pristupa Kolovoz 2016].

[27] Whatis.com, »ISO/IEC 38500,« [Mrežno]. Available: http://whatis.techtarget.com/definition/ISO-IEC-38500. [Pokušaj pristupa Kolovoz 2016].

[28] Hrvatski zavod za norme, »Hrvatski normativni dokument - HRN ISO/IEC 27033-1:2013,« 2013. [Mrežno]. Available: http://31.45.242.218/HZN/todb.nsf/wFrameset2?OpenFrameSet&Frame=Down&Src=%2FHZN%2Ftodb.nsf%2FNormaSve%2F3c6866cf39f0d80cc1257b24002b06ac%3FOpenDocument%26AutoFramed. [Pokušaj pristupa Rujan 2016].

[29] Hrvatski zavod za norme, »Hrvatski normativni dokument HRN ISO/IEC 27033-2:2013,« 2013. [Mrežno]. Available: http://31.45.242.218/HZN/todb.nsf/wFrameset2?OpenFrameSet&Frame=Down&Src=%2FHZN%2Ftodb.nsf%2FNormaSve%2F66887baa74227eecc1257b24002b34a6%3FOpenDocument%26AutoFramed. [Pokušaj pristupa Rujan 2016].

[30] G. Vojković, »Europska unija - kratki pregled,« 2015. [Mrežno]. Available: http://e-student.fpz.hr/Predmeti/T/Telekomunikacijska_legislativa_i_standardizacija/Materijali/Uvod_u_Europsku_uniju.pdf. [Pokušaj pristupa Kolovoz 2016].

[31] Europski parlament, »Direktiva 2002/58/EZ Europskog parlamenta i Vijeća,« 2002. [Mrežno]. Available: http://www.azop.hr/images/dokumenti/168/direktiva_200258ez_(2).doc. [Pokušaj pristupa Kolovoz 2016].

[32] Europsko vijeće, »Opća uredba o zaštiti podataka,« Travanj 2016. [Mrežno]. Available: http://www.consilium.europa.eu/hr/policies/data-protection-reform/data-protection-regulation/. [Pokušaj pristupa Kolovoz 2016].

[33] Europski parlament i Vijeće, »Uredba o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ, (EU) 2016/679,« Travanj 2016. [Mrežno]. Available: http://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&from=HR. [Pokušaj pristupa Kolovoz 2016].

[34] Zakon.hr, »Ustav Republike Hrvatske, pročišćeni tekst, NN br. 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14,« [Mrežno]. Available: http://www.zakon.hr/z/94/Ustav-Republike-Hrvatske. [Pokušaj pristupa Kolovoz 2016].

[35] CARNet, »Zakon o zaštiti osobnih podataka,« [Mrežno]. Available: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-07-234.pdf. [Pokušaj pristupa Kolovoz 2016].

[36] Narodne novine, »Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka NN. br. 139/04,« [Mrežno]. Available: http://narodne-novine.nn.hr/clanci/sluzbeni/313073.html. [Pokušaj pristupa Rujan 2016].

[37] Zakon.hr, »Zakon o zaštiti osobnih podataka, pročišćeni tekst, NN. br. 103/03, 118/06, 41/08, 130/11, 106/12,« [Mrežno]. Available: http://www.zakon.hr/z/220/Zakon-o-za%C5%A1titi-osobnih-podataka. [Pokušaj pristupa Kolovoz 2016].

[38] C. Moraes i A. Voss, »4. Radni dokument o nadzornim aktivnostima SAD-a u pogledu podataka EU-a te o njihovu mogućem pravnom učinku na transatlantske sporazume i suradnju,« Europski parlament, Strasbourg, 2014.

[39] Court of Justice of the European Union, »Maximillian Schrems v Data Protection Commissioner (C-362/14),« Listopad 2015. [Mrežno]. Available: http://www.politico.eu/wp-content/uploads/2015/10/schrems-judgment.pdf. [Pokušaj pristupa Kolovoz 2016].

[40] A. Raić-Knežević, »Hoće li nova "Sigurna luka" zaštititi osobne podatke građana EU od masovnog tajnog nadzora iz SAD?,« Veljača 2016. [Mrežno]. Available: http://www.svijetsigurnosti.com/blogs/7562-hoce-li-nova-sigurna-luka-zastititi-osobne-podatke-gradana-eu-od-masovnog-tajnog-nadzora-iz-sad. [Pokušaj pristupa Kolovoz 2016].

[41] Europski ombudsman, »Problemi s EU? Tko vam može pomoći?,« 2015. [Mrežno]. Available: http://www.ombudsman.europa.eu/hr/atyourservice/whocanhelpyou.faces#/page/3. [Pokušaj pristupa Kolovoz 2016].

[42] C. Millard, Cloud Computing Law, Oxford: Oxford University Press, 2013.

[43] World Trade Organization, »Agreement on Trade-Related Aspects of Intellectual Property Rights,« [Mrežno]. Available: https://www.wto.org/english/res_e/booksp_e/analytic_index_e/trips_03_e.htm#article39. [Pokušaj pristupa Kolovoz 2016].

[44] J. Urquahrt, »FBI seizures highlight law as cloud impediment,« Travanj 2009. [Mrežno]. Available: http://www.cnet.com/news/fbi-seizures-highlight-law-as-cloud-impediment/. [Pokušaj pristupa Kolovoz 2016].

[45] Google, »Google Apps for Business (Online) Agreement,« [Mrežno]. Available: https://www.google.com/apps/intl/en-GB/terms/premier_terms_ie.html. [Pokušaj pristupa Kolovoz 2016].

[46] Google Inc., »https://www.google.com/policies/terms/,« Travanj 2014. [Mrežno]. Available: https://www.google.com/policies/terms/. [Pokušaj pristupa Rujan 2016].

[47] National Institute of Standards and Technology, »Security Requirements For Cryptographic Modules,« Svibanj 2001. [Mrežno]. Available: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. [Pokušaj pristupa Kolovoz 2016].

[48] »Insurance Industry Trends - Cloud Computing,« Listopad 2015. [Mrežno]. Available: http://www.slideshare.net/EuroITGroup/insurance-industry-trends-2015-and-beyond-3-cloud-computing. [Pokušaj pristupa Kolovoz 2016].

[49] »Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks,« Srpanj 2016. [Mrežno]. Available: http://2016.export.gov/safeharbor/. [Pokušaj pristupa Kolovoz 2016].

[50] tmforum, »What is Frameworx?,« 2015. [Mrežno]. Available: https://www.tmforum.org/tm-forum-frameworx/. [Pokušaj pristupa Kolovoz 2016].

[51] ISO organizacija, »ISO/IEC 27004:2009,« Prosinac 2019. [Mrežno]. Available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=42106. [Pokušaj pristupa Kolovoz 2016].

[52] National Institute of Standards and Technology, »Information Security,« Srpanj 2008. [Mrežno]. Available: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf. [Pokušaj pristupa Kolovoz 2016].

[53] ENISA, »About ENISA,« [Mrežno]. Available: https://www.enisa.europa.eu/about-enisa. [Pokušaj pristupa Rujan 2016].

[54] European Union Agency for Network and Information Security, »Procure Secure: A guide to monitoring of security service levels in cloud contracts,« Travanj 2012. [Mrežno]. Available: https://www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts. [Pokušaj pristupa Kolovoz 2016].

[55] General Services Administration, »FedRAMP Control Specific Clauses,« [Mrežno]. Available: http://www.gsa.gov/graphics/staffoffices/FedRAMP_Control_Specific_Clauses_062712.pdf. [Pokušaj pristupa Kolovoz 2016].

[56] Eurostat, »Information society statistics - households and individuals,« Lipanj 2015. [Mrežno]. Available: http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals. [Pokušaj pristupa Kolovoz 2016].

[57] Eurostat, »Cloud computing - statistics on the use by enterprises,« Studeni 2014. [Mrežno]. Available: http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises. [Pokušaj pristupa Kolovoz 2016].

[58] Gartner, »Gartner Says Eight of Ten Dollars Enterprises Spend on IT is "Dead Money",« Listopad 2006. [Mrežno]. Available: http://www.gartner.com/newsroom/id/497088. [Pokušaj pristupa Kolovoz 2016].

[59] CloudU, »Cloudonomics: The Economics of Cloud Computing,« 2011. [Mrežno]. Available: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Cloudonomics-The_Economics_of_Cloud_Computing.pdf. [Pokušaj pristupa Kolovoz 2016].

[60] D. Andročec, *Research Challenges for Cloud Computing Economics,* Varaždin, 2015.

[61] M. Mihailescu i Y. Teo, »On Economic and Computational-Efficient Resource Pricing in Large Distributed Systems,« u *CCGRID '10 Proceedings of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing*, Washington, 2010.

[62] S. Misra i A. Mondal, »Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding Return on Investment,« *Mathematical and Computer Modelling,* svez. 53, br. 3-4, pp. 504-521, 2011.

POPIS AKRONIMA I KRATICA

ASP - pružanje usluge za primjenu

AZOP - Agencija za zaštitu osobnih podataka

CCSK - Certificate of Cloud Security Knowledge

CRM - customer relationship management

CSA - Cloud Security Alliance

CSCC - The Cloud Standards Customer Council

DMTF - Distributed Management Task Force

DSaaS - data storage as a service

EC2 - Elastic Compute Cloud

EK - Europska komisija

EU - Europska unija

IaaS - Infrastructure as a service

IEC - International Electrotechnical Commission

ISACA - Information Systems Audit nad Control Association

ISO - International Organization for Standardization

IT - Information Technology

LAN - Local Area Network

NaaS - network as a service

OCC - Open Commons Consortium

OCCI - Open Cloud Computing Interface

OGF - Open Grid Forum

OMG - The Object Management Group

OSDC - The Open Science Data Cloud Working Group

PaaS - Platform as a service

SaaS - Software as a service

STAR - Security Trust & Assurance Registry

UML - Unified Modeling Language

ZZOP - Zakon o zaštiti osobnih podataka

POPIS STRANIH IZRAZA

account - račun

Advanced Research Projects Agency Network - prva mreža temeljna na komutaciji paketa i TCP/IP protokolu

advisory standards - savjetodavni standardi

agent based - na temelju agenata

agreement - dogovor

application programming interface - aplikacijsko programabilno sučelje

availability - dostupnost

bandwidth - propusnost

broad network access - široki mrežni pristup

browser - pretraživač

browser-based - pretraživački bazirano

community cloud - zajednički oblak

conformance - sukladnosti

customer relationship management - sustav za upravljanje odnosima prema kupcima

data storage as a service - spremište podataka kao usluga

data tables - tablice podataka

datacenter - podatkovni centri

Distributed denial of service - distribuirani napad na poslužitelje

encryption keys - ključevi za šifriranje

firewall - vatrozid

Frameworx - sučelje X

grid computing - distribuirana arhitektura velikog broja računala

hash - funkcija za mapiranje podataka

hybrid cloud - hibridni oblak

Infrastructure as a service - Infrastruktura kao usluga

integrity - integritet

Intellectual property - intelektualni tip vlasništva

International Electrotechnical Commission - Međunarodno elektrotehničko povjerenstvo

International Organization for Standardization - Međunarodna organizacija za standardizaciju

Internet service provider - davatelj Internet usluge

local area network - lokalna računalna mreža

log data - arhivski podaci

malicious - zlonamjerno

management interoperability protocol - komunikacijski protokol za upravljanje kriptografskim ključevima

measured service - mjerljiva usluga

Multi-Tenant model - model s više zakupljenih jedinica

network as a service - mreža kao usluga

on-demand self-service - usluga na zahtjev korisnika

outputs - rezultati

per se - samo po sebi

Personal Digital Assistant - osobni digitalni pomoćnik

Personally identifiable information - osobni podaci

Platform as a service - Platforma kao usluga

pointers - pokazivači

private cloud - privatni oblak

procure secure - osigurati si osiguranje

public cloud - javni oblak

qualitatively and/or quantity information - kvalitetni i/ili kvalitetni sadržaj informacije

rapid elasticity - brza elastičnost

Recycle bin/trash - "koš za smeće"

resource pooling - udruživanje - resursa

safe harbor - sigurna luka

safe harbor scheme - shema sigurne luke

secure socket layer - standard sigurne tehnologije za uspostavu kriptirane veze

security frameworks - sigurnosni okviri

servers - poslužitelji

service level agreement - ugovor o razini usluge

smartphone - pametni mobilni terminalni uređaj

Software as a service - Softver kao usluga

standards specification - standardne specifikacije

Terms of service - uvjeti pružanja usluge

The European Network and Information Security Agency - Europska agencija za mrežnu i informacijsku sigurnost

Third party - treća strana

trade secrets - trgovačke (poslovne) tajne

Unified Modeling Language - standardni jezik za prikaz računalnih sustava

user agreement - ugovor o korištenju

utility computing - utilitarno računarstvo

vendor - davatelj opreme

virtual machine - virtualni strojevi

virtual machine images - slike virtualnih strojeva

POPIS ILUSTRACIJA

Popis slika

Slika 1. Prikaz ključnih karakteristika *cloud* okruženja 5
Slika 2. Javni oblak 9
Slika 3. Privatni oblak 10
Slika 4. Zajednički oblak 11
Slika 5. Hibridni oblak 12
Slika 6. Prikaz toka podataka u relacijskom modelu *clouda* 43
Slika 7. Informacije generirane izvan *clouda* 44

Popis tablica

Tablica 1. Osnovne razlike različitih izvedbi *cloud* okruženja 8
Tablica 2. *Cloud* servisni modeli 13
Tablica 3. Motivacija članova u povjerenstvima za standardizaciju 18
Tablica 4. Prikaz ovisnosti opterećenja i servisnih modela 52
Tablica 5. Postotak korištenja *cloud* računalstva za različite aktivnosti 63
Tablica 6. Cijene Googlovih, Amazonovih i Microsoftovih *cloud computing* usluga 68

Popis grafikona

Grafikon 1. Trend rasta pristupa Internetu i trend rasta širokopojasne veze za privatne korisnike 59
Grafikon 2. Postotak pristupa Internetu u kućanstvima 2009. i 2014. godine 60
Grafikon 3. Postotak korištenja Interneta u populaciji između 16 i 74 godina 61
Grafikon 4. Postotak ispitanika koji koriste *cloud* okruženje 61
Grafikon 5. Postotak korištenja *cloud* okruženja za poslovne korisnike 62
Grafikon 6. Korištenje različitih izvedbi *cloud* okruženja od strane poslovnih korisnika 64

METAPODACI

Naslov rada: Sigurnosni i pravni aspekt zaštite podataka u *cloud* okruženju

Student: Eugen Sunić

Mentor: doc. dr. sc. Goran Vojković

Naslov na drugom jeziku (engleski): Security and legal aspects of data protection inside the cloud environment

Povjerenstvo za obranu:

- izv. prof. dr. sc. Dragan Peraković, predsjednik
- doc. dr. sc. Goran Vojković, mentor
- doc. dr. sc. Ivan Grgurević, član
- doc. dr. sc. Marko Periša, zamjena

Ustanova koja je dodijelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta u Zagrebu

Zavod: Zavod za informacijsko komunikacijski promet

Vrsta studija: diplomski

Studij: Promet (npr. Promet, ITS i logistika, Aeronautika)

Datum obrane diplomskog rada: 27.09.2016.

Napomena: pod datum obrane diplomskog rada navodi se prvi definirani datum roka obrane.

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

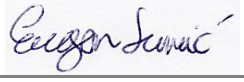
Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom **Sigurnosni i pravni aspekt zaštite podataka u *cloud* okruženju**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 14.9.2016

Student/ica:



(potpis)