Privatnost i sigurnost podataka u oblaku

Dražić, Bernarda

Sveučilište Jurja Dobrile u Puli
Fakultet informatike u Puli

BERNARDA DRAŽIĆ

PRIVATNOST I SIGURNOST PODATAKA U OBLAKU

Diplomski rad

Pula, srpanj, 2022.

Sveučilište Jurja Dobrile u Puli
Fakultet informatike u Puli

BERNARDA DRAŽIĆ

PRIVATNOST I SIGURNOST PODATAKA U OBLAKU

Diplomski rad

JMBAG: 0066272293

Studijski smjer: informatika

Kolegij: Telematika
Znanstveno područje: Područje društvenih znanosti
Znanstveno polje: Informacijske i komunikacijske znanosti
Znanstvena grana: Informacijsko i programsko inženjerstvo

Mentor: izv. doc. dr. sc. Ivan Pogarčić

Pula, srpanj, 2022.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani **Bernarda Dražić**, kandidat za magistra informatike ovime izjavljujem da je ovaj Diplomski rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Diplomskog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

U Puli, 14.7, 2022. godine

IZJAVA O KORIŠTENJU AUTORSKOG DJELA

Ja, **Bernarda Dražić** dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj diplomski rad pod nazivom „Privatnost i sigurnost podataka u oblaku“ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.
Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, 14.7.2021.

Potpis

Sadržaj

1. Uvod

Fokus ovog rada je privatnost i sigurnost podataka u oblaku. Širenjem popularnosti računala i mobilnih uređaja, raste i doseg računarstva u oblaku. Od sandučića e-pošte do objavljivanja fotografija na društvenim mrežama, mnogi korisnici nisu niti svjesni prisutnosti oblaka. Iako računarstvo u oblaku ima mnoge prednosti, potrebno je navesti i njegove mane, pogotovo kada se govori o sigurnosti i privatnosti podataka.

Cilj ovog rada je upoznati se s računarstvom u oblaku, njegovim vrstama i modelima, koracima koje poduzeti pri prelasku na računarstvo u oblaku, a zatim i njegovim rizicima u pogledu sigurnosti i privatnosti. Značajke oblaka imaju utjecaj na tradicionalne sigurnosne metode, javljaju se nove prijetnje i novi oblici napada. Te prijetnje proizlaze iz nezakonite ili neetične uporabe osobnih informacija i njihova učestalost mogla bi značajno smanjiti korisnikovo prihvaćanje računarstva u oblaku.

Početna poglavlja rada bave se općenito računarstvom u oblaku, njegovom povijesnom evolucijom, modelima pružanja usluga oblaka i vrstama oblaka, prednostima i nedostacima, potrebama za novim metodama kao i računarstvom u oblaku i telematikom. Cilj je upoznavanje računarstva u oblaku da bi bilo jasnije kako se podaci i informacije u njemu pohranjuju kao i kakve su razlike između pojedinih oblaka i sigurnosti i privatnosti vezane za njih.

U idućim poglavljima definirani su pojmovi sigurnost i privatnost i zatim su primijenjeni na koncept računarstva u oblaku. Potom su opisane sigurnosne, pravne i kriminalne prijetnje podacima pohranjenim u oblaku kao i načini na koje dijeljenje podataka s drugima utječe na sigurnost i privatnost.

U posljednjem dijelu rada opisani su koraci koje treba poduzeti prije prelaska na računarstvo u oblaku, upravljanje rizikom od strane poslužitelja i korisnika te su navedeni neki od najpoznatijih povreda podataka pohranjenih u oblaku.

2. Računarstvo u oblaku

Računarstvo u oblaku (eng. cloud computing) služi isporuci računalnih resursa i usluga kao što su baze podataka, serveri, pohrana podataka, softveri itd. putem interneta i na zahtjev korisnika. „Cloud computing je nastao iz želje IT stručnjaka za povećanjem kapaciteta i dodavanjem novih mogućnosti na vlastite sustave bez investiranja u novu infrastrukturu i potrebe za osposobljavanjem novog osoblja ili kupnje novih licenciranih programa.“ (CERT, 2010.) Nacionalni institut za standarde u Americi Cloud Computing opisuje kao „model „plati koliko koristiš“ koji, na zahtjev, omogućuje praktičan pristup, putem računalne mreže, skupu konfigurabilnih računalnih resursa (mrežama, poslužiteljima, spremištima podataka, aplikacijama i ostalim uslugama) koji se mogu brzo pripremiti za uporabu i staviti na raspolaganje, uz minimalan napor ili interakciju davatelja usluge.“ (Bronzin, Adamec, 2011., str. 25.) Kao što navodi Sultan (2010., str. 110.), uobičajeno prihvaćena definicija opisuje računarstvo u oblaku kao skup distribuiranih računala, odnosno ogromnih podatkovnih centara i farmi poslužitelja, koji pruža resurse i usluge na zahtjev putem računalne mreže, odnosno Interneta. Računarstvo u oblaku omogućuje korisnicima pristup istim datotekama, uslugama i aplikacijama s gotovo bilo kojeg uređaja koji ima pristup internetu jer se pohrana odvija na poslužiteljima u podatkovnim centrima umjesto lokalno na korisničkom uređaju. Primjer toga su pružatelji usluga e-pošte u oblaku (Gmail ili Microsoft Office 365) i pohrane podataka u oblaku (Dropbox ili Google Drive) kojima istovremeno možemo pristupati s više uređaja, kao i na sasvim novom uređaju.

Slika 1. Oblaku možemo pristupiti s više uređaja
Izvor: https://www.linuxadictos.com/hr/vlastiti-poslu%C5%BEitelj-vps-oblak.html

2.1. Povijesna evolucija

Kako navode Sehgal i Bhatt (2018.) tijekom posljednjih pola stoljeća računalne tehnologije razvijale su se u nekoliko faza:

- *Prva faza* – doba velikih mainframe sustava u pozadini povezanim s više korisnika putem terminala. Ti su terminali bili elektronički ili elektromehanički hardverski uređaji koji su koristili zasebne uređaje za unos podataka i prikaz podataka. Nisu imali mogućnosti lokalne obrade podataka. Glavni zaključak iz ove ere je koncept više korisnika koji dijele isti veliki stroj u pozadini, a pritom nemaju svijest o drugim korisnicima. Na apstraktnoj razini, ovo je slično računarstvu u oblaku s korisnicima na tankim klijentima povezanim sa poslužiteljima u pozadinskim podatkovnim centrima.
- *Druga faza* – doba započelo 1980-ih s osobnim računalima, od kojih su mnoga bila samostalna ili povezana putem modema. Svaki je korisnik komunicirao s računalom jedan na jedan, s tipkovnicom, mišem i zaslonskim terminalom. Sva pohrana, računalna snaga i memorija sadržane su u kućištu. Sav potreban softver instaliran je na diskete s ograničenim kapacitetom za pohranu za rad na osobnim računalima. Računala su se ranih 90-ih razvila u prijenosna računala s integracijom zaslona, tipkovnice, miša i računala u jednu jedinicu. Također je početkom 90-ih postojao pokušaj stvaranja mrežnog računala bez diska i povezanog s moćnijim računalima u pozadini, ali je možda ideja bila prije svog vremena jer su mreže još uvijek bile spore. Glavni razvoj ovog doba bilo je rođenje radne površine za oponašanje stola zaposlenih profesionalaca. Pomoću programa za grafičko sučelje i operacijskih sustava bilo je moguće stvoriti pojam radne površine na računalu, prijeći s jednog modela posla s jednim korisnikom na jedan posao s više korisnika koji se izvode istovremeno. To uzrokuje prelazak korisničkih interakcija s naredbenih upita na klikove koje pokreće miš.
- *Treća faza* – sredinom 90-ih bilo je doba web preglednika koji su softverska aplikacija za dohvaćanje, prezentiranje i premještanje izvora informacija na World Wide Webu. Oni su proizašli iz istraživačkog projekta, ali su postali popularni kod svakodnevnih korisnika računala za pristup informacijama koje se

nalaze na drugim računalima i poslužiteljima. Glavni zaključak iz ove ere bilo je rođenje World Wide Weba, pri čemu je računalo predstavljalo pristupnik za povezivanje korisnika s internetom.

- *Četvrta faza* – novo stoljeće najavilo je doba potpunog pregledavanja Interneta s osobnim računalima i revolucije mobilnosti s brojnim mobitelima. Bilo je neizbježno da će se tehnologije uzajamno susresti s pokretanjem inovativnih mobilnih aplikacija na mobitelima. Mobiteli su stvorili još jedan pristup oblaku. To je korisnicima omogućilo da rezerviraju hotele, iznajmljuju sobe i kupuju u pokretu. Glavni zaključak ove ere bilo je rođenje mobilnih klijenata, slično modelu Client-Server, osim s ograničenom računalnom snagom. Tisuće moćnih poslužitelja nalazilo se u velikim, udaljenim podatkovnim centrima.
- *Peta faza* – kada su tvrtke otkrile da je broj pametnih telefona i mobilnih uređaja koje mogu prodati ograničen svjetskim stanovništvom, počeli su tražiti nove poslovne mogućnosti. Došli su u obliku Interneta stvari, koji svakodnevnim uobičajenim objektima, poput televizije, hladnjaka ili čak žarulje, daje IP adresu. To dovodi do novih modela uporabe, kao što su ušteda energije, objekti Interneta stvari mogu se daljinski nadzirati, uključivati ili isključivati radi uštede energije itd. Računalni doseg proširio se na bolje informirano odlučivanje i u društvene odnose.

2.2. Tehnologije koje su omogućile razvoj računarstva u oblaku

Kao što su istaknuli Cook et al. (2017.), usluge oblaka temelje se na zajedničkom nizu podržavajućih tehnologija koje su razvijene prije nego što se računarstvo u oblaku pojavilo kao poslovni model. Te tehnologije unutar konteksta svog djelovanja u oblaku su:

- Virtualizacija – Prema Danielsu (2009.) virtualizacija je mogućnost postavljanja više operativnih okruženja na jedan fizički uređaj. Obični su operacijski sustavi inkapsulirani unutar virtualnog stroja, od kojih je veliki broj postavljen na jedan fizički poslužitelj.
- Pohrana – Kao što tvrde Grosman et al. (2009.) pohranu unutar cloud okruženja možemo okarakterizirati kao usluge temeljene na datotekama ili blokovima ili

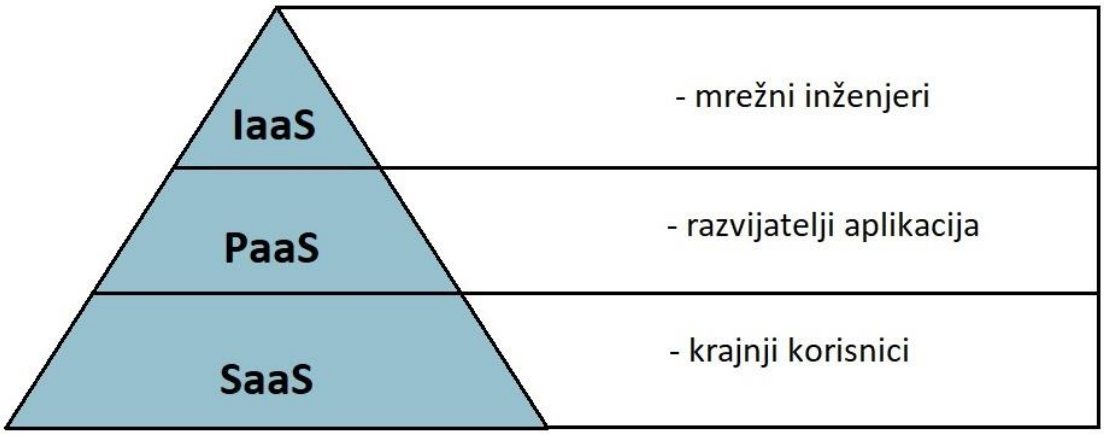
upravljanje podacima koji se sastoje od zapisa, kolona ili usluga temeljenih na objektima. Oni se obično nalaze na mreži prostora za pohranu koja pruža postojanu platformu koja podupire podatkovni centar. Kako se podaci šire unutar velike baze podataka, postaje potrebno optimizirati pohranu na temelju učestalosti pristupa i lokacije potrošača. Podaci unutar oblaka mogu se jednostavno replicirati kako bi se dobile privremene kopije u predmemoriji itd. koje poboljšavaju performanse, kao i smanjuju utjecaj sigurnosnih kopija na produkcijske podatke.

- Praćenje i opskrba – Kirschnik et al. (2010.) pišu kako su praćenje i opskrba sposobnost pružatelja usluga u oblaku da automatski pruža usluge ključni element njegove ponude. Automatsko opskrbljivanje obično se temelji na katalogu iz kojeg potrošači mogu odabrati proširenje ili smanjenje usluge nad kojom su odlučili zadržati kontrolu. Slično, za pružatelja usluga u oblaku potrebna je mogućnost izmjene okruženja izvođenja u skladu s dogovorenim ugovorom o razini usluge, sa ili bez ljudske intervencije. Omogućavanjem se obično upravlja slojem orkestracije usluge koji stupa u interakciju s uslugom praćenja radi određivanja razine izvedbe elemenata oblaka u skladu s ugovorom o razini usluge. On zatim koordinira manipulaciju infrastrukturom, raspoređivanje i ponovno dodjeljivanje resursa prema potrebi za održavanje uravnotežene i učinkovito korištenje dostupne arhitekture.
- Naplata – Kako tvrde Elmroth et al. (2010.), s obzirom na različite modele usluga i implementacije koje pružatelji usluga oblaka mogu ponuditi, usluga naplate mora biti integrirana s praćenjem i opskrbom kako bi se osiguralo točno računovodstvo potrošnje. Usluge naplate, u nekim slučajevima, podržavaju plaćanje unaprijed i naknadno pa je potrebno da se usluga naplate smanji, odnosno prikupi. Usluga također mora uzeti u obzir samo potrošnju kakva se dogodi i biti svjesna elastičnosti implementacije i oslobađanja. Budući da se priroda usluge u oblaku koja se pruža potrošačima može razlikovati, usluga naplate mora podržavati mnogo, a u mnogim slučajevima i složene modele cijena kako bi se osiguralo točno računovodstvo.

2.3. Modeli pružanja usluga računarstva u oblaku

S obzirom na različite zahtjeve i potrebe pojedinca ili organizacije, spomenut ćemo tri osnovna modela pružanja usluga računarstva u oblaku:

- Iaas (Infrastructure as a Service) – infrastruktura kao usluga
- Paas (Platform as a Service) – platforma kao usluga
- Saas (Software as a Service) – softver kao usluga



Slika 2. Modeli računarstva u oblaku i korisnici usluga

2.3.1. Infrastruktura kao usluga

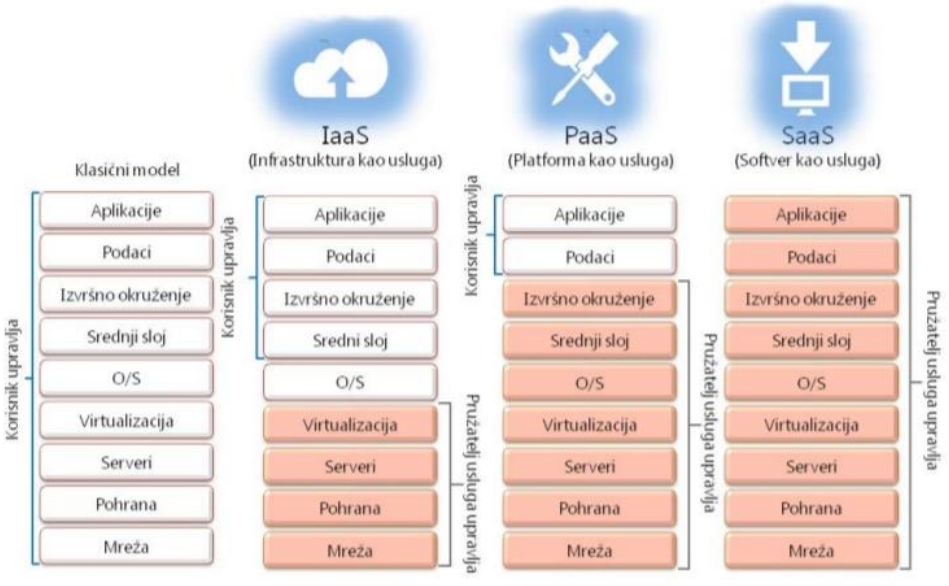
Model koji korisniku omogućuje korištenje računalne infrastrukture koja se nalazi u oblaku i označava skup računalnih, memorijskih i mrežnih resursa. Infrastrukturom upravlja pružatelj usluga oblaka. Organizacije ili pojedinci koji koriste ovaj model nemaju potrebe za kupnjom i održavanjem hardvera čime se smanjuje trošak. Sve je popularniji odabir jer smanjuje početno ulaganje, skalabilan je, lako ga je nadograditi i dodati resurse. Primjeri IaaS-a su Microsoft Azure, Google Compute Engine i Amazon's Elastic Compute.

2.3.2. Platforma kao usluga

„PaaS omogućuje pružateljima usluga da isporučuju platformu kao uslugu korisnicima da razvijaju, pokreću i upravljaju programima bez potrebe da izgrađuju i održavaju svoju infrastrukturu. PaaS uključuje pružanje platforme za razvoj softvera kao i potrebnih sadržaja koji podržavaju cijeli životni ciklus izrade i isporuke Web aplikacija.“ (Chang, Abu-Amara, Sanford, 2010., str. 55.) Razvojni programeri imaju znatno manje zadataka koje moraju obaviti jer iznajmljuju gotovo sve što im je potrebno za izradu aplikacije – razvojne alate, operacijske sustave i infrastrukturu. „IaaS pruža potpunu kontrolu, dok PaaS obično ne pruža nikakvu kontrolu ili daje samo ugovorenu kontrolu. Razvoj aplikacija pomoću PaaS usluge je brži, jeftiniji i manje rizičan. Razvojnim programerima ostaje manje posla koji moraju sami odraditi. Platforma odrađuje veći dio posla. Međutim, PaaS usluga je jednostavnija za korištenje u manje slučajeva u odnosu na IaaS usluge. PaaS usluga je izvrsno rješenje u slučajevima gdje je određeno okruženje postavljeno, ali nije pogodno za široku upotrebu kao što je IaaS usluga.“ (Panian, 2010.) Primjer ovog modela je Apprenda.

2.3.3. Softver kao usluga

Softver kao usluga je model koji omogućava isporuku aplikacija putem interneta. Pružatelji usluga oblaka su domaćini tim aplikacijama i omogućuju njihovo korištenje putem interneta. Kao i prethodni modeli, smanjuje troškove održavanja i kupnje infrastrukture, a uz to smanjuje i vrijeme provedeno na upravljanju i ažuriranju aplikacije jer je za to odgovoran pružatelj usluge SaaS-a. Većini SaaS aplikacija se pristupa preko Internet browsera te ne zahtijevaju preuzimanje i instalaciju na vlastito računalo. Ovaj model uključuje mnoge poslovne aplikacije kao što su e-mail, upravljanje ljudskim resursima, financijsko upravljanje, upravljanje prodajom, aplikacije vezane za zdravstvo itd. Primjeri SaaS-a su Hotmail, Gmail, Salesforce.



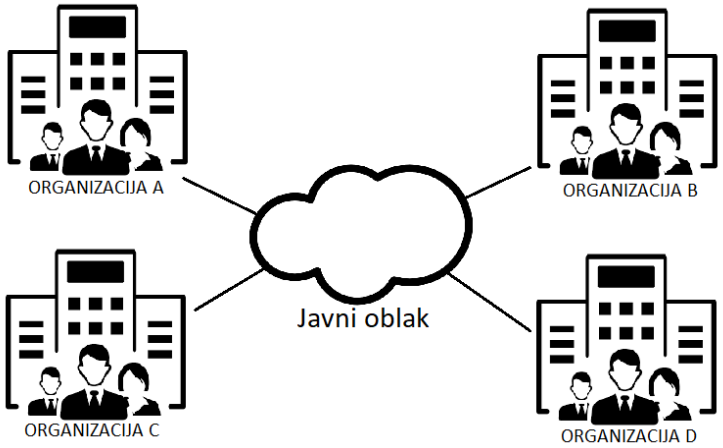
Slika 3. Modeli pružanja usluga oblaka

2.4. Vrste računalnih oblaka

Postoje tri vrste implementacija usluga u oblaku – na javnom oblaku, privatnom oblaku ili hibridnom oblaku. One su neovisne o prethodno navedenim modelima pružanja usluga i ovise o specifičnim potrebama korisnika ili organizacije.

2.4.1. Javni oblak

„Javni oblak je onaj oblak čija je infrastruktura dostupna široj javnosti ili većoj industrijskoj grupi preko Interneta. Infrastruktura nije u vlasništvu korisnika, već je u vlasništvu organizacije koja pruža usluge računarstva u oblaku. Usluge se mogu osigurati kao pretplate ili po modelu pay-as-you-go. Primjeri javnih oblaka su: IBM Cloud, Amazon Elastic Compute Cloud, Google AppEngine i Microsoft Azure App Service.“ (Coyne et al., 2018.) Neke od karakteristika javnog oblaka su: skalabilnost, fleksibilnost, cjenovna pristupačnost, dostupnost, manja sigurnost.

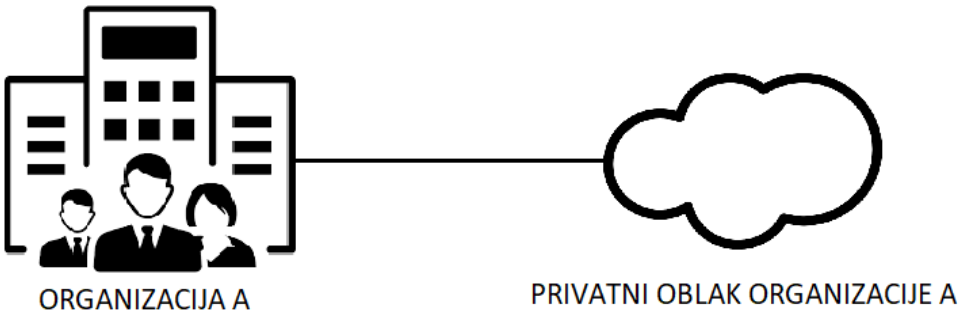


Slika 4. Javni oblak
Izvor: student.fpz.hr/Predmeti/I/Informacijski_sustavi_mreznih_operatera/Materijali/02_-_Razvoj_sustava_za_obradu_podataka.pdf

2.4.2. Privatni oblak

„Pojam privatni oblak izražava određeno vlasništvo. Činjenica je da klijent ima veću razinu kontrole pri korištenju privatnog oblaka. U usporedbi s javnim oblakom, radi se o skupljoj usluzi. Ovakva usluga bi bila cjenovno pristupačna jedino velikim organizacijama uzme li se u obzir infrastruktura i upravljanje sustavom. Postoje četiri tipa privatnih oblaka. U uobičajenom privatnom oblaku, poslovna organizacija služi kao poslužitelj oblaku u jednom od njihovih data centara. Arhitektura je slična korištenju intraneta pri čemu organizacija ograničava pristup sadržaju samo zaposlenicima. Drugi tip privatnog oblaka je oblak kojim upravlja nabavljač. U ovom slučaju, organizacija i dalje posjeduje infrastrukturu koja se nalazi u njihovim data centrima, ali nabavljač upravlja postrojenjem. Takav oblak se zove 'managed private cloud.' Treći tip privatnog oblaka, 'hosted private cloud,' pružatelj usluge računarstva u oblaku tj. nabavljač osigurava infrastrukturu i upravlja tom infrastrukturom. Četvrti tip je 'virtual private cloud' ili VPC, koristi virtualne resurse kao što su virtualni serveri i VPN (virtual private network).“ (Srinivasan, 2014.)

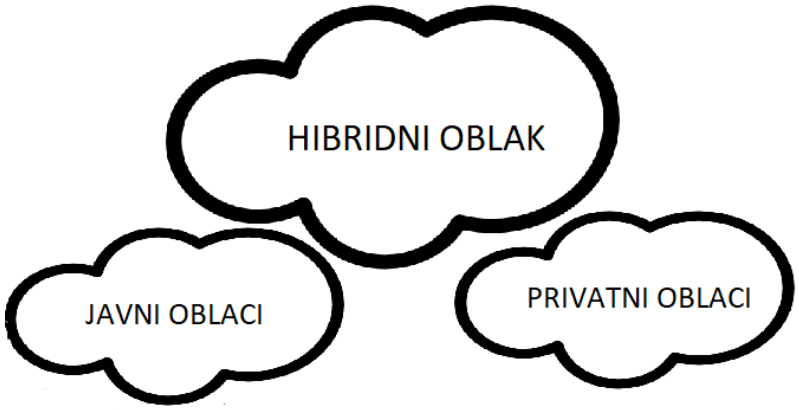
Glavne karakteristike privatnog oblaka su centralna kontrola (organizacija upravlja oblakom i ima potpunu kontrolu) i sigurnost.



Slika 5. Privatni oblak

2.4.3. Hibridni oblak

Hibridni oblak predstavlja kombinaciju javnog i privatnog oblaka i upravlja komunikacijom među njima. Kombinacija usluga javnog i privatnog oblaka se može značajno razlikovati ovisno o potrebama organizacije. Hibridni oblak omogućava fleksibilnost pri prebacivanju aplikacija i podataka između oblaka u skladu s potrebama, troškovima i zahtjevima organizacije.



Slika 6. Hibridni oblak

2.5. Prednosti i nedostaci računarstva u oblaku

Sve je veći broj korisnika računarstva u oblaku, kako privatnih tako i poslovnih. Mnogi ljudi podsvjesno integriraju oblak u svakodnevni život putem npr. Gmaila, Instagrama ili Facebooka. Oblak predstavlja rastući trend u IT industriji i stoga ćemo navesti neke od njegovih glavnih prednosti.

Mathur (2019.) u svom članku navodi sljedeće pozitivne aspekte oblaka:

1. Sveprisutnost
    - Njegova sveprisutnost omogućuje jednostavan pristup funkcionalnostima i podacima. Omogućuje više korisnika da rade na istom projektu bez ikakvih zaostajanja. To ne samo da smanjuje troškove, već i gradi robustan model rada.
2. Smanjenje troškova
    - Jedna od najboljih prednosti računarstva u oblaku je njegov 'pay-as-you-go' model. Moguće je plaćanje za funkcionalnosti koje su pogodne za rad i strukturu pojedine organizacije.
3. Kontrola
    - Organizacije se često suočavaju s ispitivanjima u slučaju zaostalih operacija, gubitka podataka i operativnih smetnji. Imperativ je da organizacije imaju dovoljnu kontrolu nad tekućim radnjama tvrtke, što računarstvo u oblaku omogućava. Iako daje kontrolu menadžmentu, također pojednostavljuje rad jer dijeli zadatke prema zaposlenicima i daje im jedinstven pristup njihovim dužnostima. To omogućuje jasno razumijevanje posla koji treba obaviti i izravan put do izvršenja zadatka.
4. Fleksibilnost
    - Oblak nudi ekspanzivan prostor za hosting i infrastrukturu koji organizacijama omogućavaju fleksibilnost. Mogućnost nenadanog donošenja i izvršavanja poslovnih odluka bez brige o utjecaju na infrastrukturu čine oblak toliko traženim.
5. Mobilnost
    - Uz pomoć veze kroz oblak, tvrtke se mogu s lakoćom povezati na daljinu putem niza uređaja kao što su pametni telefoni, prijenosna računala itd.

6. Oporavak od katastrofe
    - Najveća katastrofa koja se može dogoditi organizacijama je gubitak podataka. Međutim, oblak je spremište za sigurnosno kopirane podatke, što pomaže tvrtkama da s lakoćom i sigurnošću obnove izgubljene podatke.
7. Skalabilnost
    - Skalabilnost oblaka se može definirati kao sposobnost proizvoda da ispuni postavljene zahtjeve. To je jedan od najtraženijih atributa računarstva u oblaku.
8. Automatska ažuriranja softvera
    - Zbog automatskih ažuriranja i ciklične nadogradnje korisnici mogu fokusirati vrijeme na posao.
9. Poboljšana suradnja
    - Jednostavnost korištenja, široka dostupnost i neposredna povezanost dovode do dobrih poslovnih mogućnosti što dodatno povećava šanse za suradnju unutar tima.
10. Jednostavno upravljanje
    - Jednostavan je pristup poslu, uslugama i zadacima što omogućava lakše upravljanje.
11. Prevencija gubitka
    - Oblak omogućuje automatsko podupiranje podataka u svojim bazama podataka čime se može izbjeći njihov gubitak.
12. Bolji uvid u poslovanje
    - Zahvaljujući transparentnosti oblaka, organizacije imaju bolji uvid u poslovanje i mogu proizvesti rezultate na temelju analitičkog pristupa.

Nakon prednosti, potrebno je navesti i nedostatke računarstva u oblaku. Ohri (2021.) u svom članku navodi iduće:

1. Ranjivost na napade
    - Povjerljive informacije o poslovanju se razmjenjuju s pružateljem usluga računarstva u oblaku, te podatke mogu iskoristiti hakeri.
2. Zastoji

- Pružatelji usluga oblaka mogu se suočiti s nestankom struje, lošim pristupom internetu, održavanjem itd.

3. Ovisnosti platforme
   - Često će duboko ukorijenjene razlike među platformama pružatelja usluga otežavati prelazak s jedne platforme oblaka na drugu.
4. Tehnički problemi
   - Infrastruktura oblaka nerijetko je osjetljiva na nestabilnost i druge tehnološke probleme

Prednosti računarstva u oblaku	**Nedostaci računarstva u oblaku**
- smanjenje troškova	- ranjivost na napade
- skalabilnost	- zastoji
- prevencija gubitka	- ovisnosti platforme
- fleksibilnost	- tehnički problemi
- oporavak od katastrofe	- manjak transparentnosti
- jednostavno upravljanje	- nepredviđeni troškovi
- mobilnost	- sigurnost i privatnost

Tablica 1. Prednosti i nedostaci računarstva u oblaku

2.6. Potreba za novim metodama

Kao što tvrde Kumar, Chaisiri i Ko (2017.), tradicionalno IT okruženje sastoji se od različitih vrsta hardvera, koji uključuju računalne uređaje poput stolnih računala, prijenosnih računala, mobilnih uređaja itd. Ovi se uređaji povezuju radi primanja i slanja podataka na više različitih poslužitelja, poput poslužitelja za ispis, poslužitelja aplikacija, poslužitelji baza podataka itd. Svi ovi uređaji i poslužitelji nalaze se na internoj mreži. U takvom okruženju podaci se nalaze unutar perimetra organizacije na različitim poslužiteljima ili korisničkim računalima ili jednostavno na mreži tvrtke. Sigurnost podataka u takvom okruženju može se grubo podijeliti na dva dijela: sigurnost podataka kada izlazi izvan perimetra organizacije i sigurnost podataka unutar perimetra

organizacije. Sigurnosni problemi tradicionalnih IT sustava primjenjuju se i kada se operacije premjeste u oblak. Računarstvo u oblaku uvodi nove vektore napada čime sigurnost postaje još izazovnija. Tri primarna uzroka novih vektora napada u oblacima su nestajanje opsega sigurnosti, nova vrsta insajdera i kontrastni poslovni ciljevi.

- Nestajanje opsega sigurnosti – definicija opsega primijenjena na tradicionalni IT nije korisna u slučaju računarstva u oblaku. Podaci u slučaju računarstva u oblaku nalaze se u oblaku, izvan prostorija tvrtke, dakle izvan tradicionalnog opsega. Pružatelj usluga oblaka, međutim, pruža vlastitu sigurnost na perimetru; stoga ni podaci nisu potpuno izvan opsega. Oblak može dodatno upotrijebiti različite mehanizme kontrole pristupa i autorizacije za zaposlenike organizacije i njene klijente, a oba pristupaju podacima iz oblaka. Time se stvara ogromno sivo područje perimetra umjesto dobro definiranog opsega kao što je to bio slučaj u tradicionalnim sustavima. Ovaj problem dodatno se pojačava ako postoji mogućnost da oblak podatke i aplikacije prenese na svoje partnere u oblaku.
- Nova vrsta insajdera – insajder je netko tko ima ovlašten pristup sustavu. Insajder može biti upoznat sa sustavom i mrežnom arhitekturom te stoga imati i bolje znanje o ranjivostima i slabim stranama sustava u odnosu na autsajdera. Tradicionalno, insajderi su općenito zaposlenici ili kooperanti koji su dobili pristup sustavima. Unutarnji napadi općenito su bili velika prijetnja IT sustavima. Unutarnji ljudi obično se mogu pratiti ako postoje odgovarajući mehanizmi evidentiranja i revizije. Uz tradicionalnog, računarstvo u oblaku uvodi novu vrstu insajdera. Taj zaposlenik ili kooperant radi za davatelja usluga u oblaku ili njegove partnere. Možda neće raditi za vlasnika podataka, ali i dalje ima kontrolu nad podacima i pristup njima. Za razliku od tradicionalnih insajdera, vlasnik podataka nema kontrolu nad takvim insajderima.
- Kontrastni poslovni ciljevi – čak i kad nema zlonamjernih insajdera, vlasniku podataka može biti teško povjeriti se pružatelju usluga oblaka. To je zato što obje ove strane imaju suprotne poslovne ciljeve. Vlasnik podataka, koji plaća usluge oblaka, želi maksimizirati korist od usluga u oblaku i smanjiti troškove

uz održavanje kvalitete usluge. S druge strane, pružatelj usluga koji održava resurse želi maksimizirati povrat ulaganja povećavajući iskorištenost resursa što može utjecati na kvalitetu usluge. To bi moglo dovesti do skrivanja oštećenja ili grešaka radi održavanja ugleda, zanemarivanja ili brisanja podataka kojima se rijetko pristupa radi uštede resursa, pokušaja dobivanja informacija o pohranjenim podacima ili dovesti do suradnje s vanjskim stranama radi prikupljanja korisničkih podataka.

Tri gore navedena uzroka zajedno dovode do percepcije nepouzdanosti oblaka i igraju ulogu u smanjenju učinkovitosti tradicionalnih metoda sigurnosti podataka.

2.7. Računarstvo u oblaku i telematika

Liotine (n.d.) navodi da je „telematika kombinacija prijenosa informacija putem telekomunikacijske mreže i obrade tih informacija.“ Koristi se u senzorskim aplikacijama za hvatanje, pohranu i razmjenu podataka sa senzorskih uređaja. U području automobilske telematike, vozilo zapravo postaje računalna platforma i razmjenjuje informacije s drugim vozilima, vozačima ili stacionarnim sustavima pomoću bežične komunikacije. Takva komunikacija postiže se, između ostalog, različitim bežičnim komunikacijskim tehnologijama, poput mobilnih komunikacijskih mreža, satelita i namjenske komunikacije kratkog dometa. Računalna platforma u oblaku mogla bi pružiti pozadinu telematičkom sučelju. Računarstvo u oblaku je internetski model koji je razvijen na temelju paralelnih, mrežnih i distribuiranih koncepata računarstva.

3. Definiranje privatnosti i sigurnosti

Privatnost i sigurnost su složeni pojmovi i za njih se ne može navesti standardna općeprihvaćena definicija. Slijedom toga i odnos između njih je zamršen.

3.1. Privatnost

Kao što su naveli Pearson i Yee (2012.), na najširem nivou i pogotovo s europskog stajališta, privatnost je temeljno ljudsko pravo sadržano u Općoj deklaraciji o ljudskim pravima Ujedinjenih naroda (1948.), a potom i u Europskoj konvenciji o ljudskim pravima te nacionalnim ustavima i poveljama o pravima kao što je britanski Zakon o ljudskim pravima iz 1998. godine. Otprilike od sedamdesetih godina prošlog stoljeća primarni fokus privatnosti bile su osobne informacije, a posebno se brine o zaštiti pojedinaca od državnog nadzora i potencijalnom obveznom otkrivanju privatnih podataka u bazama podataka. Desetljeće kasnije izražena je zabrinutost u vezi s izravnim marketingom i telemarketingom, a kasnije se razmatrala sve veća prijetnja internetske krađe identiteta i spama. Postoje različiti oblici privatnosti, u rasponu od „prava pojedinca da bude ostavljen na miru“ (Warren i Brandeis, 1890.), „kontrola informacija o nama samima“ (Westin, 1967.), „prava i obveze pojedinaca i organizacija u pogledu prikupljanja, uporabe, otkrivanja i čuvanja osobnih podataka“ (AICPA i CICA, 2009.) i „fokus na štetu koja proizlazi iz kršenja privatnosti.“ (Solove, 2006.) Još jedan utjecaj je Nissenbaumova ideja o privatnosti kao „kontekstualnom integritetu“ pri čemu se može mjeriti priroda izazova koje postavljaju informacijske tehnologije. Kontekstualni integritet povezuje odgovarajuću zaštitu privatnosti s normama specifičnih konteksta koji su u biti ograničenja protoka informacija, tako da prikupljanje i širenje informacija treba biti primjereno određenom kontekstu. (Nissenbaum, 2004. i 2009.) U komercijalnom, potrošačkom kontekstu, privatnost podrazumijeva zaštitu i odgovarajuću uporabu osobnih podataka kupaca te ispunjenje očekivanja kupaca o njihovoj uporabi. Za organizacije privatnost podrazumijeva primjenu zakona, politika, standarda i procesa kojima se upravlja osobnim podacima. Ono što je prikladno ovisit će o primjenjivim zakonima, očekivanjima pojedinaca o prikupljanju, korištenju i otkrivanju njihovih osobnih podataka i drugih kontekstualnih podataka; stoga je jedan od načina razmišljanja o privatnosti jednak „prikladnom korištenju osobnih informacija u datim okolnostima“. (Swire i Berman, 2007.) Zaštita podataka je upravljanje osobnim podacima i često se koristi unutar Europske unije u vezi sa zakonima i propisima koji se odnose na privatnost (iako se u SAD-u uporaba ovog izraza više fokusira na sigurnost). Općenito, osobni podaci opisuju činjenice, komunikacije ili mišljenja koja se odnose na pojedinca i za koje bi bilo razumno očekivati da će on smatrati intimnim ili osjetljivim i

stoga bi htio ograničiti njihovo prikupljanje, korištenje ili dijeljenje. Definicija osobnih podataka Europske unije (EU) je da: „Osobni" podaci znače sve informacije koje se odnose na identificiranu ili prepoznatljivu fizičku osobu („subjekt podataka"); osoba koja se može identificirati je ona osoba koja može identificirati, izravno ili neizravno, osobito pozivanjem na identifikacijski broj ili na jedan ili više čimbenika specifičnih za njezin fizički, fiziološki, mentalni, ekonomski, kulturni ili društveni identitet. (https://ec.europa.eu/info/policies/justice-and-fundamental-rights_en, 1995.)

Kada govorimo o privatnosti, ključna terminologija koju uz nju vežemo je pojam kontrolora podataka, obrađivača podataka i ispitanika.
Kontrolor podataka - subjekt (fizička ili pravna osoba, javno tijelo, agencija ili drugo tijelo) koji sam ili zajednički s drugima određuje svrhe i način na koji se obrađuju osobne informacije.
Obrađivač podataka – subjekt koji obrađuje podatke u ime i na način određen od strane kontrolora podataka.
Ispitanik – osoba na koju se odnose osobni podaci, bilo da je identifikacija te osobe izravna ili neizravna (npr. pozivanjem na identifikacijski broj ili na jedan ili više čimbenika specifičnih za fizički, fiziološki, mentalni, ekonomski, kulturni ili društveni identitet).

Važno je još spomenuti i načela zaštite podataka koje navodi Data Protection Commission (n.d.):

- *Zakonitost, pravičnost i transparentnost* - Svaka obrada osobnih podataka trebala bi biti zakonita i poštena. Pojedincima bi trebalo biti transparentno da se osobni podaci koji se odnose na njih prikupljaju, koriste, konzultiraju ili na drugi način obrađuju te u kojoj se mjeri osobni podaci obrađuju ili će se obraditi. Načelo transparentnosti zahtijeva da sve informacije i komunikacija u vezi s obradom tih osobnih podataka budu lako dostupne i razumljive te da se koristi jasan jezik.
- *Ograničenje svrhe* - Osobne podatke treba prikupljati samo u određene, izričite i legitimne svrhe, a ne dalje obrađivati na način koji je nespojiv s tim

svrhama. Konkretno, posebne svrhe u koje se obrađuju osobni podaci trebaju biti eksplicitne i legitimne i utvrđene u vrijeme prikupljanja osobnih podataka.

- *Minimiziranje podataka* - Obrada osobnih podataka mora biti odgovarajuća, relevantna i ograničena na ono što je potrebno u odnosu na svrhe u koje se obrađuju. Osobne podatke treba obrađivati samo ako se svrha obrade ne može razumno ispuniti na druge načine. To zahtijeva, osobito, osiguravanje da je razdoblje za pohranu osobnih podataka ograničeno na strogi minimum.
- *Točnost* - Kontrolori obrade moraju osigurati da su osobni podaci točni i, prema potrebi, ažurirani; poduzimajući sve razumne korake kako bi se osiguralo da se osobni podaci koji su netočni, s obzirom na svrhe u koje se obrađuju, bez odlaganja izbrišu ili isprave. Konkretno, kontrolori bi trebali točno zabilježiti informacije koje prikupljaju ili primaju i izvor tih informacija.
- *Ograničenje pohrane* - Osobni se podaci trebaju čuvati samo u obliku koji dopušta identifikaciju ispitanika onoliko dugo koliko je potrebno za svrhe u koje se osobni podaci obrađuju. Kako bi se osiguralo da se osobni podaci ne čuvaju dulje nego što je potrebno, kontrolor obrade trebao bi odrediti rokove za brisanje ili za povremenu provjeru.
- *Integritet i povjerljivost* - Osobne podatke treba obrađivati na način koji osigurava odgovarajuću sigurnost i povjerljivost osobnih podataka, uključujući zaštitu od neovlaštenog ili nezakonitog pristupa ili uporabe osobnih podataka i opreme koja se koristi za obradu te od slučajnog gubitka, uništenja ili oštećenja, koristeći odgovarajuće tehničke ili organizacijske mjere.
- *Odgovornost* - kontrolor je odgovoran za podatke i mora biti u mogućnosti dokazati svoju usklađenost sa svim gore navedenim načelima zaštite podataka.

3.2. Sigurnost

Kada govorimo o sigurnosti, mislimo na informacijsku sigurnost. U tom smislu, sigurnost možemo definirati kao „očuvanje povjerljivosti, integriteta i dostupnosti informacija; osim toga, mogu se uključiti i druga svojstva kao što su autentičnost, odgovornost,

neporecivost i pouzdanost.“ (ISO: 27001: Information Security Management, 2005.) Sigurnost je neophodan, ali ne i dovoljan uvjet za privatnost. Sigurnost je zapravo jedno od temeljnih načela privatnosti. Uobičajeno je prema zakonu da ako tvrtka povjeri rukovanje osobnim podacima ili povjerljivim podacima drugoj tvrtki, ima izvjesnu odgovornost pobrinuti se da vanjski suradnik koristi „razumnu sigurnost“ za zaštitu tih podataka.

Kako bi osigurali sigurnost obrade podataka, kontrolori podataka moraju provesti odgovarajuće tehničke i organizacijske mjere kako bi ih zaštitili od:

- *neovlaštenog pristupa ili otkrivanja* - može dovesti do slučajnog ili nezakonitog gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima osobito tamo gdje obrada uključuje prijenos podataka putem mreže;
- *uništavanja* - slučajno ili protupravno uništenje ili gubitak;
- *izmjena* - neprikladna izmjena osobnih podataka;
- *neovlaštena upotreba* - svi drugi nezakoniti i nedopušteni oblici uporabe osobnih podataka.

Mehanizmi za to uključuju procjenu rizika, korištenje programa za sigurnost informacija i uvođenje učinkovitih, razumnih i odgovarajućih zaštitnih mjera koje pokrivaju fizičke, administrativne i tehničke aspekte sigurnosti.

4. Pitanja privatnosti u računarstvu u oblaku

Suočavamo se s velikim izazovom kada govorimo o dijeljenju resursa u računarstvu u oblaku i zaštiti privatnosti korisnika. S rastom računalstva u oblaku, zabrinutost za privatnost također postaje sve važnija. U nastavku razmatramo aspekte koji najbolje ilustriraju pitanje privatnosti.

4.1. Nedostatak korisničke kontrole

Kada govorimo o oblaku, potpuna korisnička kontrola nad podacima čini se nemoguća. Govoreći o SaaS uslugama, pružatelj usluga oblaka postaje odgovoran za

pohranjivanje podataka čime se vidljivost i kontrola podataka ograničeni. Pearson i Yee (2012.) navode glavne čimbenike manjka kontrole nad podacima:

1. *Vlasništvo i kontrola nad infrastrukturom* – u računarstvu u oblaku, korisnički se podaci obrađuju u oblaku na strojevima koje korisnik ne posjeduje ili kojima ne upravlja, te postoji prijetnja krađe, zlouporabe (osobito u različite svrhe od onih o kojima su prvotno obavijestili potrošača i koje su dogovorene s njima) ili neovlaštene preprodaje.
2. *Pristup i transparentnost* – može postojati nedostatak transparentnosti o tome gdje se podaci nalaze, tko ih posjeduje i što se s njima radi.
3. *Kontrola nad životnim ciklusom podataka* – pružatelj usluga oblaka možda neće udovoljiti zahtjevu za brisanje podataka.
4. *Promjena pružatelja usluga oblaka* – može biti teško vratiti podatke iz oblaka
5. *Obavijesti i pravna pomoć* – nesigurnosti u vezi s obavještavanjem, uključujući povrede privatnosti i mogućnost dobivanja naknade. Teško je znati da je došlo do povrede privatnosti i utvrditi tko je kriv u takvim slučajevima.
6. *Prijenos prava na podatke* – nije jasno koja će prava nad podacima steći obrađivači podataka i njihovi podizvođači te jesu li ona prenosiva na druge treće strane nakon stečaja, preuzimanja ili spajanja.

4.2. Nedostatak obuke i stručnosti

Nedostatak obučenog osoblja može biti problem sa sigurnosnog stajališta. Također, ljudima može nedostajati razumijevanje o utjecaju odluka koje donose na privatnost. Osim ako postoje odgovarajući postupci upravljanja, postoji opasnost da zaposlenici mogu prijeći na korištenje računalstva u oblaku bez odgovarajućeg razmatranja posljedica i rizika za tu određenu situaciju.

4.3. Neovlaštena sekundarna upotreba

Postoji opasnost da se podaci pohranjeni ili obrađeni u oblaku neovlašteno koriste. Dio je standardnog poslovnog modela računalstva u oblaku da pružatelj usluga može ostvariti prihod od dopuštene sekundarne upotrebe podataka korisnika, najčešće

ciljajući oglase. Međutim, neke sekundarne uporabe podataka bile bi vrlo nepoželjne za vlasnika podataka (poput, primjerice, preprodaje detaljnih podataka o prodaji njihovim konkurentima).

4.4. Složenost usklađenosti s propisima

Zbog globalne prirode računalstva u oblaku i brojnih zakona koji su na snazi u cijelom svijetu, može biti složeno i teško osigurati poštivanje svih zakona koji se mogu primijeniti u datom slučaju. Postavljanje podataka u oblak može utjecati na prava, obveze i status privatnosti. Pravna zaštita se može umanjiti i utjecati na poslovne tajne. Lokacija je važna s pravnog gledišta jer se mogu primjenjivati različiti zakoni ovisno o tome gdje postoje informacije, ali u računalstvu u oblaku informacije se ponekad mogu nalaziti na više mjesta istovremeno; možda je teško znati točno gdje se nalaze ili su u tranzitu. Osim toga, moguće je i kršenje lokalnih zakona pri prijenosu podataka pohranjenih u oblaku.

4.5. Rješavanje ograničenja prekograničnog protoka podataka

Nepoznavanje kojim će rutama ići transnacionalni promet otežava razumijevanje posebnih zakona koji će se primjenjivati. Čak i ako tranzit podataka nije relevantan za razmatranje, i dalje je teško primijeniti propise o prekograničnom protoku podataka u oblaku. Računarstvo u oblaku može pogoršati problem poznavanja geografskog položaja na kojem se događaju aktivnosti u računalstvo u oblaku, jer to zbog svoje dinamičke prirode može biti izuzetno teško otkriti.

4.6. Pravna nesigurnosti

Pravni okviri su ključni za zaštitu osobnih i osjetljivih podataka korisnika. Oni se mogu razlikovati prema sektorima, informacijama ili zemljopisnom području. Pravne okvire – zajedno s povezanim alatima, savjetima i nacionalnim zakonodavstvom – potrebno je stalno ažurirati i prilagođavati imajući na umu trenutne i buduće tehnologije. Dinamička priroda računalstva u oblaku, potencijalno u kombinaciji s interakcijama među

nadležnostima, uvodi pravne aspekte koje je potrebno pažljivo uzeti u obzir pri obradi podataka. Budući da se tehnologija u oblaku razvila, postoji velika pravna nesigurnost u pogledu prava na privatnost u oblaku i teško je predvidjeti što će se dogoditi kada se postojeći zakoni primijene u okruženjima u oblaku. Područja neizvjesnosti o kojima se još uvijek raspravlja uključuju da se postupak anonimizacije ili šifriranja osobnih podataka može smatrati reguliranom „obradom“ koja zahtijeva pristanak, te nije jasno je li ta obrada u svrhu poboljšanja privatnosti korisnika izuzeta od zahtjeva za zaštitu privatnosti.

5. Pitanja sigurnosti u računarstvu u oblaku

Kada se govori o oblaku, sigurnost je često jedan od glavnih razloga zabrinutosti za korisnike. Postoje mnogi sigurnosni problemi vezani za oblak, oni uvelike ovise i o pružatelju usluga i modelu implementacije, npr. privatni oblaci mogu u određenoj mjeri jamčiti sigurnost, ali su ekonomski troškovi povezani s ovim modelom relativno visoki. Pearson i Yee (2012.) navode iduće: nedostatak u sigurnosti, neovlašteni pristup, neadekvatno brisanje podataka, kompromis sučelja za upravljanje, ranjivosti sigurnosnih kopija, neuspjeh izolacije, manjak povjerenja i transparentnosti, neadekvatno praćenje, usklađenost i revizija.

5.1. Nedostatak u sigurnosti

Općenito, sigurnosne kontrole za oblak iste su kao i one koje se koriste u drugim IT okruženjima. Rizik ovisi i o korištenom modelu, korisnik IaaS modela mora brinuti o sigurnosti jer je on sam odgovoran za nju, dok u SaaS modelu sigurnosne kontrole i njihov opseg ulaze u ugovor o uslugama. U slučaju Iaas i PaaS modela, pružatelj usluga oblaka treba specificirati kakvi oblici zaštite se očekuju od korisnika. U SaaS modelu o zaštiti se brine pružatelj usluga oblaka, ali se od korisnika ipak očekuje da će osigurati kontrolu pristupa putem svojih vlastitih sustava npr. koristeći lokalnu aplikaciju za kontrolu pristupa.

5.2. Neovlašteni pristup

Za zaštitu sigurnosti resursa mora postojati odgovarajuća razina kontrole pristupa u oblačnom okruženju. Računarstvo u oblaku zapravo može povećati rizik pristupa povjerljivim informacijama. Kao i kod drugih računalnih modela, postoji rizik od neovlaštenog i neželjenog pristupa podacima koji može biti iznimno problematičan ako su subjekti uključeni u lanac usluga koji imaju neadekvatne sigurnosne mehanizme. Rizik od neovlaštenog pristupa postoji u mnogo oblika, od strane zaposlenika pružatelja usluga oblaka, od strane hakera koji provaljuju u strojeve pružatelja usluga ili čak od korisnika iste usluge ako dijele isti stroj, a nisu adekvatno odvojeni podaci u oblaku. Podaci mogu biti pohranjeni u oblaku dug period pa je i vremenska izloženost podataka mnogo veća.

5.3. Neadekvatno brisanje podataka

Idući problem je osiguravanje da kupac ima kontrolu nad životnim ciklusom svojih podataka, a posebno njihovim brisanjem – u smislu kako biti siguran da se podaci koje treba izbrisati doista brišu i da ih pružatelj usluga oblaka ne može oporaviti. Trenutačno nema načina da se to dokaže jer se oslanja na povjerenje, a problem se pogoršava u oblaku jer može postojati mnogo kopija podataka (potencijalno u posjedu različitih entiteta, a neki možda i nisu dostupni) ili zato što možda nije moguće uništiti disk jer pohranjuje podatke drugih korisnika. Rizik je veći za korisnika ako se hardverski resursi ponovno koriste nego ako se koristi namjenski hardver.

5.4. Kompromis sučelja za upravljanje

Sučelja za upravljanje oblakom dostupna su preko interneta. To predstavlja povećan rizik u usporedbi s tradicionalnim pružateljima usluga hostinga jer se mogu uvesti ranjivosti daljinskog pristupa i web preglednika, a uz to povećan je i rizik pristupa sučelju. Ovaj povećani rizik prisutan je čak i ako se pristup kontrolira lozinkom.

5.5. Ranjivosti sigurnosnih kopija

Davatelji usluga u oblaku izrađuju više kopija podataka i postavljaju ih na različita mjesta kako bi osigurali visoku razinu pouzdanosti i performansi. Ovo služi kao oblik sigurnosne kopije, iako može dovesti do dodatnih obaveza i prijetnji od strane napadača. Poznati su slučajevi u kojima je korisnicima ponuđena sigurnosna kopija kao dodatak uz uslugu pohrane, a nekorištenje te usluge rezultiralo je potpunim gubitkom podataka korisnika koji uslugu nisu platili.

5.6. Neuspjeh izolacije

Višenamjensko korištenje izaziva sigurnosnu zabrinutost da jedan korisnik može utjecati na operacije ili pristup podacima drugih korisnika koji rade na istom oblaku. Ako se koristi SaaS model, softver je dizajniran za virtualnu podjelu podataka i konfiguraciju tako da svaka organizacija klijenta radi s prilagođenom instancom virtualne aplikacije. Postoji rizik da mehanizmi koji razdvajaju pohranu, memoriju ili usmjeravanje između različitih korisnika mogu otkazati pa bi, na primjer, drugi korisnici mogli pristupiti osjetljivim podacima.

5.7. Manjak povjerenja i transparentnosti

Korisnici oblaka moraju dobiti uvjerenje od pružatelja usluga u oblaku da će njihovi podaci biti pravilno zaštićeni. Oni također mogu zahtijevati da budu obaviješteni o incidentima u vezi sa sigurnošću i privatnošću. Neki pružatelji usluga u oblaku pružaju informacije o svojim postupcima rukovanja podacima, sigurnosnim mehanizmima i nude s tim povezana jamstva.

5.8. Neadekvatno praćenje, usklađenost i revizija

Postoje brojna pitanja koja se odnose na održavanje i dokazivanje usklađenosti pri korištenju računarstva u oblaku. Ako se korisnik preseli u oblak, njihovo prethodno ulaganje u sigurnosnu certifikaciju može biti dovedeno u pitanje ako pružatelj usluge

oblaka ne može pružiti dokaze o svojoj usklađenosti s relevantnim zahtjevima i ne omogućuje korisniku oblaka reviziju njegove obrade podataka korisnika. Nadalje, može biti teško procijeniti kako računalstvo u oblaku utječe na usklađenost s unutarnjim sigurnosnim politikama. Pružatelji usluga oblaka moraju provoditi interne kontrole nadziranja usklađenosti, uz proces vanjske revizije.

Pitanja privatnosti	Pitanja sigurnosti
- nedostatak kontrole	- nedostatak u sigurnosti i neovlašteni pristup
- nedostatak obuke i stručnosti	- neadekvatno brisanje podataka
- neovlaštena sekundarna upotreba	- neadekvatno praćenje, usklađenost i revizija
- pravna nesigurnost	- ranjivost sigurnosnih kopija
- složenost usklađenosti s propisima	- manjak povjerenja i transparentnosti
- prekogranični protok podataka	- kompromis sučelja za upravljanje

Tablica 2. Pitanja privatnosti i sigurnosti računarstva u oblaku

6. Prijetnje i ranjivosti

„Prijetnja je svaki događaj koji, ako se ostvari, može uzrokovati štetu sustavu i stvoriti gubitak povjerljivosti, dostupnosti ili integriteta. Prijetnje mogu biti zlonamjerne, poput namjerne izmjene osjetljivih podataka, ili mogu biti slučajne - poput pogreške u izračunu transakcije ili slučajnog brisanja datoteke.

Ranjivost je slabost u sustavu koja se može iskoristiti prijetnjom. Smanjenjem ranjivog aspekta sustava može se smanjiti rizik i utjecaj prijetnji na sustav. Na primjer - alat za generiranje lozinki koji pomaže korisnicima u odabiru robusnih lozinki, smanjuje vjerojatnost da će korisnici odabrati loše lozinke (ranjivost) i otežava razbijanje lozinke (prijetnja vanjskog napada).“ (Ponnusamy, n.d.)

6.1. Klasifikacija sigurnosnih prijetnji u računarstvu u oblaku

Sigurnosne prijetnje računarstvu u oblaku možemo svrstati u sljedeće tri kategorije:

1. Tradicionalna sigurnosna pitanja
2. Problemi s dostupnošću
3. Problemi vezani uz kontrolu podataka od trećih strana

6.1.1. Tradicionalna sigurnosna pitanja

Ovi sigurnosni problemi su omogućeni ili olakšani prelaskom u računarstvo u oblaku i uključuju upade ili napade na računalo i mrežu. Oni uključuju iduće:

- napadi na razini VM (virtualne mašine) – napad u kojem se iskorištavaju potencijalne ranjivosti hipervizora, haker preuzima kontrolu nad hipervizorom;
- phishing oblak – obično se koristi u e-porukama ili društvenim mrežama. Pod krinkom računarstva u oblaku želi natjerati korisnike da kliknu zlonamjerne veze;
- proširena površina napada mreže – pokriva sva područja organizacije koja su podložna napadu; korisnik oblaka mora zaštititi infrastrukturu koja se koristi za povezivanje i interakciju s oblakom;
- autentifikacija i autorizacija – autentifikacija i autorizacija pojedine organizacije se ne proširuju na oblak; organizacija mora spojiti svoje sigurnosne mjere i pravila s onima u oblaku.

6.1.2. Problemi s dostupnošću

Ove zabrinutosti usredotočene su na kritične aplikacije i podatke koji su dostupni. Poznati incident prekida rada oblaka uključuje jednodnevni prekid rada Gmaila sredinom listopada 2008. godine. Osiguravanje da pružatelj usluga oblaka daje valjane rezultate i osigurava računalni integritet, održavanje neprekidnog rada, sprječavanje rada uskraćivanjem usluge samo su neki od glavnih fokusa u ovoj kategoriji prijetnji.

6.1.3. Problemi vezani uz kontrolu podataka od trećih strana

Postoji potencijalni nedostatak kontrole i transparentnosti kada treća strana drži podatke. Pravne posljedice podataka i aplikacija koje posjeduje treća strana složene su i ne razumiju se dobro. Sen (n.d.) u svom radu navodi iduće probleme koje treba riješiti:

- dubinska analiza – postavljaju se pitanja kao što su može li korisnik biti siguran da je pružatelj usluga oblaka na njegov zahtjev trajno obrisao podatke, hoće li na zahtjev isporučiti podatke i hoće li to biti u odgovarajućem roku;
- revizija – poteškoće s revizijom još su jedna nuspojava nedostatka kontrole u oblaku; postavlja se pitanje postoji li dovoljna transparentnost u radu pružatelja usluga za potrebe revizije;
- ugovorne obveze – jedan od problema korištenja infrastrukture druge tvrtke osim neizvjesnog usklađivanja interesa je taj što bi moglo doći do iznenađujućih pravnih implikacija;
- špijunaža pružatelja usluga oblaka – može postojati zabrinutost u vezi krađe vlasničkih podataka tvrtke od strane pružatelja usluga oblaka;
- tranzitivna priroda ugovora - druga moguća zabrinutost je da bi ugovoreni davatelj usluga oblaka mogao sam koristiti kooperante, nad kojima korisnik oblaka ili nema kontrolu ili ima vrlo malu kontrolu.

6.1.4. Nove sigurnosne prijetnje podacima u oblaku

Sen (n.d.) navodi neke od dodatnih sigurnosnim prijetnji koje su relevantne za računalstvo u oblaku:

- napad bočnih kanala (side-channel attack) – pojavljujuća zabrinutost za modele isporuke u oblaku koji koriste platforme za virtualizaciju je rizik od napada bočnih kanala koji uzrokuju curenje podataka u su-rezidentnim instancama virtualnih strojeva; taj se rizik razvija, iako se trenutno smatra da je u začetcima, kako tehnologije virtualnih strojeva sazrijevaju;
- napadi uskraćivanja usluge (DoS) – dostupnost je primarna briga korisnika u oblaku i kao takva zabrinjava i pružatelje usluga koji moraju osmisliti rješenja

za ublažavanje ove prijetnje. Uskraćivanje usluge se veže s napadima u kojima se preplavljuje infrastrukturu s prekomjernim prometom kako bi došlo do trošenja svih raspoloživih resursa ili otkazivanja komponenti;

- napadi na društvene mreže – s povećanom popularnošću poslovnih i osobnih društvenih mreža povećava se rizik od napada; sustavi računalstva u oblaku ciljani su zbog velikih skladišta podataka o korisnicima;
- napadi na mobilne uređaje – upotreba pametnih telefona se povećala i povezivanje u oblak sada više nije ograničeno na prijenosna ili stolna računala. Danas se pojavljuju napadi koji su usmjereni na mobilne uređaje i oslanjaju se na značajke koje se tradicionalno povezuju s prijenosnim i stolnim računalima. Crvi, špijunski softveri itd. su primjeri napada na mobilne uređaje koji su potencijalno manje rizična meta za napadača koji želi ostati neotkriven. To podupire činjenica da većina mobilnih uređaja nema omogućene ekvivalentne sigurnosne značajke kao stolna i prijenosna računala, ili u nekim slučajevima nisu dostupne. Zrele tehnologije zaštite od zlonamjernog softvera, anti-virusi ili potpuna šifriranja diska nisu rasprostranjeni na trenutačno dostupnim pametnim telefonima;
- unutarnja prijetnja i prijetnja organiziranog kriminala – pružatelji usluga oblaka pohranit će niz različitih vrsta podataka, uključujući informacije o kreditnim karticama i druge financijske i osobne podatke. Svi ti podaci mogu se prikupiti od više kupaca i stoga biti iznimno vrijedni za kriminalce. Postoji opasnost da članovi oblaka namjerno koriste pristup podacima o korisnicima i sustavima ispitivanja kako bi pomogli vanjskim napadačima koji zahtijevaju dodatne informacije kako bi izvršili složene napade;
- analiza podataka – pojavom računalstva u oblaku stvoreni su ogromni skupovi podataka koje se mogu unovčiti pomoću aplikacija poput oglašavanja. Google, na primjer, koristi svoju infrastrukturu u oblaku za prikupljanje i analizu podataka o potrošačima za svoju oglasnu mrežu. Prikupiti i analizirati podatke sada je lako moguće, čak i za tvrtke kojima nedostaju Googleovi resursi. Dostupnost podataka i jeftine tehnike rudarenja podataka ima veliki utjecaj na privatnost korisničkih podataka. Napadači imaju

velike, centralizirane baze podataka dostupne za analizu, a također i sirovu računalnu moć za miniranje ovih baza podataka;

- isplativa obrana dostupnosti – dostupnost se također mora razmatrati u kontekstu protivnika čiji su ciljevi sabotiranje aktivnosti. Takvi protivnici postaju sve realniji kako se politički sukobi prenose na web;
- povećani zahtjevi za autentifikacijom – razvoj računalstva u oblaku može, u krajnjem slučaju, dopustiti upotrebu tankih klijenata na strani korisnika. Umjesto kupnje licence i instaliranja softvera na strani klijenta, korisnici će se autentificirati kako bi mogli koristiti aplikaciju u oblaku. U takvom modelu postoje neke prednosti, poput otežavanja softverskog piratstva i prikladnijeg centraliziranog praćenja. Također može pomoći u sprječavanju širenja osjetljivih podataka na nepouzdane klijente. Ova arhitektura također podržava poboljšanu mobilnost korisnika, ali zahtijeva robusnije protokole provjere autentičnosti. Štoviše, kretanje prema povećanom 'hostiranju' podataka i aplikacija u oblaku te manje oslanjanje na određene korisničke strojeve vjerojatno će povećati prijetnju od krađe identiteta i krađu podataka za pristup;

Slika 7. Sigurnosne prijetnje oblaku
Izvor: https://searchcloudsecurity.techtarget.com/tip/Top-cloud-security-challenges-and-how-to-combat-them

7. Pravne i kriminalne prijetnje podacima pohranjenim u oblaku

U ovom poglavlju navodimo opseg pravnih i kriminalnih prijetnji podacima pohranjenim u oblaku.

7.1. Pravne prijetnje

Wheeler i Winburn (2015.) navode sljedeće izvore pravnih prijetnji podacima pohranjenim u oblaku:

- Uvjeti korištenja pružatelja usluga oblaka
- Autorska prava i dijeljenje datoteka
- Građanske parnice
- Pravni nalozi
- Lokalni zakoni s obzirom na lokaciju
- Lokalni zakoni za podatkovni centar za pohranu u oblaku

Davatelji usluga pohrane podataka u oblaku mogu imati uvjete korištenja koji im mogu omogućiti široki pristup metapodacima i podatkovnom sadržaju. Uvjeti korištenja mogu imati dvosmislen jezik koji čini povjerljivost nejasnom. Pravna nejasnoća mogla bi značiti odlazak na sud radi zaštite privatnosti i sigurnosti podataka, dug i skup proces bez jamstva za uspjeh.

Korištenjem oblaka postavlja se pitanje i dijeljenju sadržaja s autorskim pravima. Autorski sadržaj se prodaje jednoj osobi na korištenje. Ukoliko ta osoba sadržaj kopira i prosljeđuje ili prodaje, uskraćuje nositelja autorskih prava materijalne dobiti.

Građanske parnice mogu drugima omogućiti pristup podacima u oblaku. Zahtjevi za pristup podacima pohranjenim u oblaku se šalju pružatelju usluga tog oblaka koji će udovoljiti legitimnom zakonskom zahtjevu za pristup.

Pravni nalozi mogu značajnu količinu podataka pohranjenih u oblaku učini dostupnima javnim ili privatnim agencijama koje su zadužene za analizu podataka. To znači da će drugi imati pristup podacima bez znanja pojedinca i jamstva kako će se i od koga ti podaci koristiti.

Lokalni zakoni s obzirom na lokaciju mogu omogućiti policijska zaustavljanja ili sigurnosne kontrolne punktove koji daju jamstvo za pristup podacima u oblaku.

Lokalni zakoni koji vrijede za fizičku lokaciju pojedinca i fizičku lokaciju podataka utječu na sigurnost tih podataka. Ako su podaci fizički smješteni na jednom mjestu, a pojedinac putuje na drugo mjesto, zakoni u drugoj zemlji mogu od njega zahtijevati da pokaže podatke spremljene u oblak putem uređaja.

7.2. Kriminalne prijetnje

Wheeler i Winburn (2015.) navode iduće kriminalne motive za napad na podatke i pohranu u oblaku:

- Iskorištavanje – podaci vrijedni za pojedinca, mogu imati vrijednost i drugima
- Uskraćivanje – privremeno sprječavanje pojedinca da dođe do svojih podataka, može nekome biti od koristi
- Uništavanje – trajno uništavanje podataka može nekome koristiti
- Obmana – suptilne promjene podataka koje mogu ostati nezamijećene sve dok ne izazovu problem
- Prisvajanje – drugi mogu koristiti pohranu pojedinca u vlastite svrhe, npr. za skrivanje ilegalnog sadržaja

Osobni podaci mogu imati vrijednosti za druge iz mnogo razloga. Npr. cyberstalkeri koriste osobne podatke kako bi uspostavili osobni odnos i komunikaciju s pojedincem, cyber-nasilnici ih mogu koristiti za sramoćenje ili ucjene, podaci mogu služiti i za krađu identiteta itd.

Poslovno iskustvo može biti slično onom od pojedinca. Industrijska špijunaža se događa kada kriminalci dobiju informacije o poslovnoj strategiji, ugovorima, podacima o upravljanju odnosima s korisnicima ili drugom intelektualnom vlasništvu i te informacije koriste ili prodaju.

Izraz „doxing“ odnosi se na objavljivanje osobnih informacija ili osjetljivih sadržaja o pojedincu ili organizaciji u svrhu sramoćenja, iznude, prisile, uznemiravanja itd.

8. Dijeljenje podataka u oblaku

Osim pohrane podataka u oblaku, trebamo spomenuti i pojam dijeljenja podataka u oblaku. Dijeljenje podataka s drugima predstavlja dodatni sigurnosni rizik za pojedince koji pohranjuju podatke samo za osobnu upotrebu. Dijeljenje podataka u oblaku uključuje društvene mreže, zajedničku pohranu datoteka ili kolaborativni radni prostor. Pojedinci ga mogu koristiti za dijeljenje fotografija, razmišljanja, videa itd. s

poznanicima. Organizacije najčešće dijele podatke sa zaposlenicima kako bi im omogućili rad na daljinu.
Wheeler i Winburn (2015.) navode iduća pitanja koja treba razmotriti kada razmišljamo o dijeljenju podataka u oblaku:

1. *Povjerenje u članove* – kada dijelimo svoje podatke s drugima, postajemo ranjiviji jer smo izloženi njihovoj greški ili lošoj namjeri. Oslanjamo se na pojedince s kojima dijelimo podatke da će se ponašati odgovorno, da neće dijeliti podatke s osobama koje nisu članovi grupe, da neće učitavati neprikladan ili ilegalan sadržaj. Povjerenje je jedan od najvećih izazova kada se radi o dijeljenju podataka u oblaku.
2. *Kontrola pristupa* – označava mogućnost dopuštanja i opoziva pristupa podacima. Opoziv dozvole pristupa može značiti promjenu lozinke za sve članove, a zatim dojavljivanje lozinke članovima kojima želimo dopustiti pristup putem alternativnog sigurnog kanala.
3. *Mehanizam dijeljenja* – implementirani mehanizmi dijeljenja podataka su sigurnosni rizik koji pružatelj usluga mora razmotriti. Npr. korisnik oblaka može podijeliti datoteku s pojedincem na način da mu pošalje URL za pristup. Problem se javlja kada Internet preglednici pohranjuju taj URL u povijest pretraživanja i omogućuju pojedincu ne samo pristup, već i dijeljenje URL-a s drugima.

Primjeri pružatelja usluga oblaka koji se koriste za dijeljenje podataka su Dropbox, Box i OneDrive.

8.1. Dropbox

„Kada se pretplatite na Dropbox, dodjeljuje vam se određena količina prostora za pohranu na mrežnom poslužitelju poznatom kao "oblak". Nakon instaliranja aplikacije Dropbox na računalo, mobilni uređaj ili oboje, sve datoteke koje lokalno pohranite u Dropbox bit će kopirane i na Dropbox poslužitelj. Ako promijenite ove datoteke na jednom mjestu, ažuriranja se automatski preslikavaju posvuda. Sinkroniziranjem vaših Dropbox datoteka lokalno i na mreži možete jednostavno pristupiti tim datotekama bilo

gdje i lakše ih dijeliti s drugima. Jedan od ključnih razloga korištenja Dropboxa je koliko je usluga jednostavna za dijeljenje datoteka. Možete kontrolirati razine dopuštenja i dijeliti datoteke i mape s određenim osobama pomoću veze ili učiniti datoteke javnim kako bi svatko s odgovarajućom vezom mogao pristupiti vašim podacima. To je prikladan način za slanje datoteka bez upotrebe privitaka e-pošte. Dropbox čak uključuje i neke alate za suradnju, poput Dropbox Spaces, koji timovima omogućuje zajednički rad na dokumentima, dijeljenje bilješki i uređivanje u stvarnom vremenu.“ (Johnson, 2021.)

8.2. Box

„Koristeći pristup sličan Dropboxu po pitanju pohrane u oblaku, Box postavlja određenu mapu na vašem Windows ili macOS računalu, a zatim održava sav njezin sadržaj sinkroniziran s oblakom zajedno sa svim drugim uređajima s instaliranim Boxom. Dijeljenje datoteka i mapa jednostavan je i jasan zadatak, bilo da treba surađivati s drugim ljudima na nečemu ili samo za stvaranje veze koja će se distribuirati svima kojima je to potrebno.“ (Pickavance, Nield, DeMuro, 2021.)

8.3. OneDrive

„Jedna od mnogih prednosti usluge OneDrive je mogućnost dijeljenja datoteka s drugim ljudima. Datoteke možete dijeliti izravno s lokalnog računala ili s web mjesta za pohranu. Datoteke možete dijeliti s jednom ili više osoba putem e-pošte ili putem veze. Također možete odrediti želite li da drugi ljudi mogu uređivati vaše datoteke na usluzi OneDrive ili ih samo pregledavati.“ (Whitney, 2020.)

Slika 8. Dropbox, Box i OneDrive logotipi

9. Koraci koje treba uzeti u obzir pri prelasku na računarstvo u oblaku

Kalluri i Rao (2014.) navode da će primjenjivanje idućih smjernica pomoći u zaštiti korisnika u računarstvu u oblaku. Sigurnosni mehanizmi se mogu podijeliti u dvije različite kategorije – zasnovani na partnerima (sigurnost za SaaS, PaaS i IaaS) ili korisnički (na bazi klijenta):

- *strateško planiranje sigurnosti u oblaku* - uzimanje u obzir sigurnosti tijekom početne faze planiranja stvara čvrste temelje. Potrebno je pažljivo razmotriti kako se korporativno radno opterećenje treba isporučiti krajnjim korisnicima;
- *odabir pružatelja usluga oblaka* - ključno je odabrati pružatelja usluga oblaka koji može zaštititi osjetljive podatke ili informacije. Prije odabira pružatelja usluga oblaka provjerite imaju li iskustva u IT i sigurnosnim uslugama te jamstva o učinkovitosti strateških usluga;
- *pronalazak pisanog dokumenta o sigurnosnim mjerama koje nudi pružatelj usluga oblaka* - to znači dobivanje uvjerenja zapisanog u ugovoru od pružatelja usluga oblaka. Dokument mora sadržavati aplikacije, infrastrukturu, konfiguracije, politike, pravila i propise;
- *provjera tko će nadzirati podatke* - provjera tko će imati pristup podacima te zašto i kada im pristupaju;

- *plan za sigurnosne probleme* - mora se provjeriti koju odgovornost pružatelj usluga oblaka obećava i koje će radnje poduzeti tijekom i nakon sigurnosnog problema;
- *provjera kontrola pristupa koje se koriste* - važno je definirati uloge i odgovornosti kako bi se osiguralo da čak i privilegirani korisnici ne mogu izbjeći testiranje i odgovornost;
- *nadziranje sustava* - pružatelj usluga oblaka mora kontinuirano nadzirati podatke u oblaku. Potrebno je uspostaviti mjerne podatke o performansama u oblaku i redovito ih testirati.

9.1. Zaštita podataka u oblaku

U nastavku su navedeni savjeti za osiguravanje podataka u oblaku:

- lokalna sigurnosna kopija – mogućnost gubitka ili brisanja podatak iz oblaka dobar je razlog za napraviti sigurnosne kopije svega što se pohranjuje u oblak, pogotovo ukoliko se radi o podacima ključnim za poslovanje;
- izbjegavanje pohranjivanja osjetljivih podataka – podatke koji bi ozbiljno mogli našteti pojedincu ili organizaciji u slučaju da su ukradeni nije preporučljivo pohranjivati u oblak;
- korištenje enkripcije – šifriranje podataka prije njihovog prijenosa u oblak odličan je oblik zaštite protiv hakera. Šifriranjem podataka svatko tko pristupi podacima bez ključa za dešifriranje ih neće moći pročitati;
- korištenje pouzdanih lozinka – lozinke ne bi trebale biti predvidljive i lako pamtljive. Korištenje jedinstvene lozinke je bolji odabir, kao i njeno redovno mijenjanje. Uz to, uvođenje postupka provjere u dva koraka povećava razinu sigurnosti. Čak i ako dođe do povrede u prvom sigurnosnom koraku, drugi i dalje štiti podatke;
- dodatne sigurnosne mjere – oblak bi trebao biti zaštićen antivirusnim programima, administratorskim kontrolama i drugim značajkama koje pospješuju njegovu sigurnost;

- testiranje sigurnosti – testiranje može uključivati ispitivanje oblaka kako bi se uvidjeli koliko se dobro ponaša u skladu sa sigurnosnim postavkama. Također moguće je unajmiti etičke hakere kako bi se testirala razina sigurnosti sustava.

Na primjer, svako rješenje za e-poštu u oblaku treba imati sljedeće:

• Antivirus
• Anti-spam, tj. kontrolu protiv neželjenog sadržaja
• Kontrola curenja informacija
• Mogućnost stvaranja posebnih pravila za blokiranje sadržaja, uključujući privitke
• Praćenje prometa e-poštom

Dok bi bilo koje Cloud aplikacijsko rješenje trebalo imati sljedeće mogućnosti

• Alati za otkrivanje upada
• Vatrozid aplikacije
• Vatrozid nove generacije
• Alati za ublažavanje DDoS napada
• Dnevnik prijave
• Mreža za isporuku sadržaja

9.2. Dizajn sigurnosne arhitekture

Kao što tvrde Rittinghouse i Ransome (2010.), okvir sigurnosne arhitekture trebao bi se uspostaviti uzimajući u obzir procese (autentifikacija i autorizacija poduzeća, kontrola pristupa, povjerljivost, integritet, nepoštivanje, upravljanje sigurnošću itd.), operativne procedure, tehničke specifikacije, upravljanje ljudima i organizacijom te usklađenost i izvještavanje o sigurnosnim programima. Treba razviti dokument o sigurnosnoj arhitekturi koji definira načela sigurnosti i privatnosti kako bi se ispunili poslovni ciljevi. Dokumentacija je potrebna za upravljačke kontrole i metrike specifične za klasifikaciju i

kontrolu imovine, fizičku sigurnost, kontrolu pristupa sustavu, upravljanje mrežom i računalom, razvoj i održavanje aplikacija, kontinuitet poslovanja i usklađenost. Program projektiranja i provedbe također bi trebao biti integriran u službeni životni ciklus razvoja sustava kako bi uključio poslovni slučaj, definiciju zahtjeva, dizajn i provedbene planove. Treba uključiti tehnologiju i metode projektiranja, kao i sigurnosne procese potrebne za pružanje sljedećih usluga u svim tehnološkim slojevima:

- Autentifikacija
- Autorizacija
- Dostupnost
- Povjerljivost
- Integritet
- Odgovornost
- Privatnost

10. Upravljanje rizikom od strane pružatelja usluga oblaka

Kao što navodi Vacca (2017.), pružatelji usluga oblaka razvijaju arhitekture u oblaku i grade usluge u oblaku koje uključuju temeljne funkcije i operativne značajke, uključujući kontrole sigurnosti i privatnosti koje zadovoljavaju osnovne zahtjeve. Njihova rješenja imaju za cilj zadovoljiti potrebe velikog broja korisnika oblaka na način koji zahtijeva minimalnu prilagodbu. Odabir i primjena davatelja usluga u oblaku i njegove kontrole sigurnosti i privatnosti uzimaju u obzir njihovu djelotvornost, učinkovitost i ograničenja na temelju primjenjivih zakona, direktiva, politika, standarda ili propisa kojih se davatelj usluga u oblaku mora pridržavati. Pružatelji usluga oblaka imaju značajnu fleksibilnost u određivanju onoga što čini uslugu u oblaku, a time i njezine granice, ali u trenutku kada je sustav projektiran i implementiran, oni mogu samo pretpostaviti prirodu podataka koje će generirati njihovi korisnici oblaka. Stoga su kontrole sigurnosti i privatnosti koje odabere i provodi pružatelj usluga oblaka skupovi koji zadovoljavaju potrebe velikog broja potencijalnih potrošača. Centralizirana priroda usluge oblaka omogućuje pružatelju usluga oblaka da izradi visoko-tehnička, specijalizirana sigurnosna rješenja

koja mogu pružiti viši sigurnosni položaj nego u tradicionalnim IT sustavima. Primjena standardiziranih ili provjerenih pristupa upravljanju rizicima u oblačnim uslugama ključna je za uspjeh cijelog ekosustava u oblaku i njegovih podržanih informacijskih sustava. Budući da ponuđenom uslugom oblaka izravno upravlja i kontrolira pružatelj usluga oblaka, primjena okvira upravljanja rizicima ne zahtijeva dodatne zadatke osim onih klasičnog IT sustava. Važno je napomenuti da je sigurnosni položaj ekosustava u oblaku jak koliko i najslabiji podsustav ili funkcionalni sloj. Budući da reputacija i kontinuitet poslovanja davatelja usluga u oblaku ovise o nesmetanom radu i visokim performansama rješenja njihovih potrošača, prilikom primjene okvira upravljanja rizicima pružatelj usluga u oblaku nastoji nadoknaditi moguću slabost u rješenjima svojih korisnika oblaka.

11. Upravljanje rizikom od strane korisnika

Vacca (2017.) navodi kako je organizacijama lakše prihvatiti rizik kada imaju veću kontrolu nad procesima i opremom koja je u to uključena. Visok stupanj kontrole omogućuje organizacijama da odmjere alternative, odrede prioritete i odlučno djeluju u svom najboljem interesu kada se suoče s incidentom. Za uspješno usvajanje rješenja informacijskog sustava temeljenog na oblaku, korisnik oblaka mora biti u stanju jasno razumjeti karakteristike sustava specifične za oblak, arhitektonske komponente za svaku vrstu usluge i modela implementacije te uloge aktera u oblaku u uspostavljanju sigurnog ekosustava oblaka. Za poslovne korisnike oblaka i kritične procese jako je bitno da mogu: identificirati kontrole sigurnosti i privatnosti prilagođene riziku i specifične za oblak; zahtijevati od pružatelja usluga oblaka da je provedba kontrole sigurnosti i privatnosti njihova odgovornost gdje je to moguće; procijeniti provedbu navedene kontrole sigurnosti i privatnosti; kontinuirano pratite sve identificirane kontrole sigurnosti i privatnosti.

Budući da korisnici oblaka izravno upravljaju i kontroliraju funkcionalnim sposobnostima koje primjenjuju, primjena okvira upravljanja rizicima na ove funkcionalne slojeve ne zahtijeva dodatne zadatke ili operacije različite od onih u klasičnom IT sustavu. Uz

usluge temeljene na oblaku, neki podsustavi ili komponente podsustava ne spadaju pod izravnu kontrolu organizacije korisnika oblaka. Budući da usvajanje rješenja temeljenog na oblaku inherentno ne pruža istu razinu sigurnosti i usklađenost s mandatima u tradicionalnom IT modelu, mogućnost sveobuhvatne procjene rizika ključna je za izgradnju povjerenja u sustav temeljen na oblaku kao prvi korak u odobravanju njegovog rada.

Karakteristike ekosustava oblaka uključuju:

- Širok pristup mreži
- Smanjena vidljivost i kontrola od strane korisnika oblaka
- Dinamične granice sustava i nadolazeće uloge/odgovornosti između korisnika oblaka i pružatelja usluga oblaka
- Zajedničko korištenje
- Lokalizacija podataka
- Procjena usluga
- Značajno povećanje opsega (na zahtjev), dinamike (elastičnost, optimizacija troškova) i složenosti (automatizacija, virtualizacija)

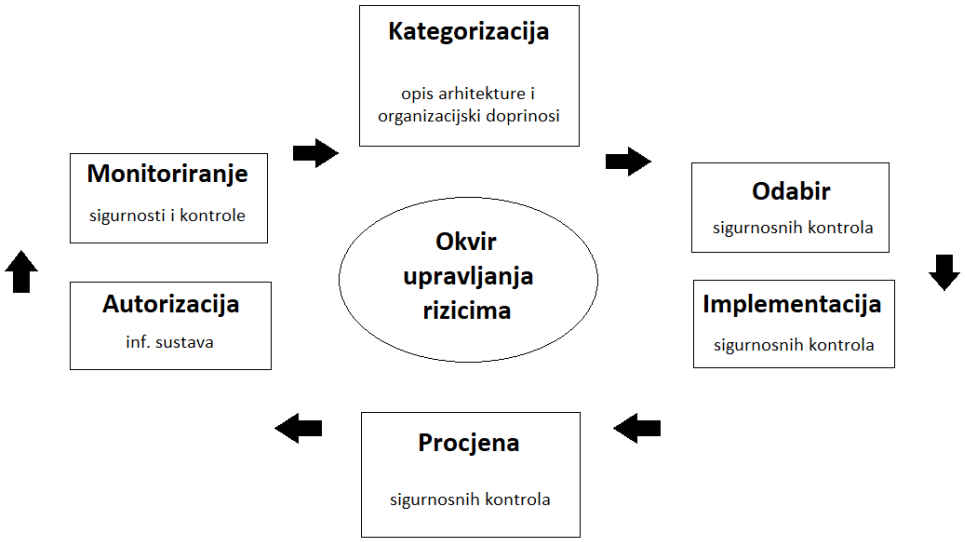
Ove karakteristike često predstavljaju za korisnika oblaka sigurnosne rizike koji se razlikuju od onih u tradicionalnim rješenjima informacijske tehnologije. Kako bi očuvali razinu sigurnosti svog informacijskog sustava i podataka u rješenju temeljenom na oblaku, korisnici oblaka trebaju moći unaprijed identificirati sve sigurnosne karakteristike i rizike prilagođene oblaku. Također trebaju zahtijevati od pružatelja usluga oblaka, putem ugovornih sredstava, da se identificiraju sve komponente sigurnosti i privatnosti te da se njihove kontrole u potpunosti i točno provedu.

Razumijevanje odnosa i međuovisnosti između različitih modela implementacije računalnog oblaka i modela usluga ključno je za razumijevanje sigurnosnih rizika uključenih u računarstvo u oblaku. Razlike u metodama i odgovornostima za osiguravanje različitih kombinacija usluga i modela implementacije predstavljaju značajan izazov za korisnike oblaka. Moraju provesti temeljitu procjenu rizika, kako bi

točno identificirali kontrole sigurnosti i privatnosti potrebne za očuvanje razine sigurnosti njihovog okoliša u sklopu procesa tretiranja rizika, te nadgledali operacije i podatke nakon migracije u oblak kao odgovor na svoje potrebe kontrole rizika.

Korisnik koji prihvaća rješenje zasnovano na oblaku mora slijediti ove korake:

- Opisati uslugu ili aplikaciju za koju se može koristiti rješenje temeljeno na oblaku
- Identificirati sve funkcionalne sposobnosti koje se moraju implementirati za navedenu uslugu ili aplikaciju
- Utvrditi zahtjeve sigurnosti i privatnosti te sigurnosne kontrole potrebne za zaštitu usluge ili aplikacije



Slika 9. Okvir upravljanja rizicima

12. Primjeri povreda podataka u oblaku

Kao što tvrde Hill i Swinhoe (2021.) u današnjem svijetu koji se temelji na podacima, povrede podataka mogu istodobno utjecati na stotine milijuna ili čak milijarde ljudi. Digitalna transformacija povećala je ponudu podataka u pokretu, a povrede podataka su se time povećale jer napadači iskorištavaju ovisnost svakodnevnog života o podacima.

Koliko bi veliki cyber napadi u budućnosti mogli postati, ostaje nagađati, ali kao što ćemo vidjeti u idućim primjerima, oni su već dosegli ogromne razmjere.

- Yahoo – 2013. godine, utjecaj na 3 milijarde računa. Tvrtka je prvi put javno objavila incident – za koji je rekla da se dogodio 2013. – u prosincu 2016. U to vrijeme je procijenjeno da je hakerska grupa pristupila podacima o računu više od milijarde njegovih korisnika. Manje od godinu dana kasnije, Yahoo je objavio da je stvarna brojka izloženih korisničkih računa 3 milijarde. To je i dalje najrazornija povreda podataka uzme li se u broj pogođenih računa;
- Alibaba – studeni 2019. godine, utjecaj na 1.1 milijardu korisničkih računa. Tijekom razdoblja od osam mjeseci, razvojni programer koji je radio za afilijacijskog oglašivača sakupljao je podatke o klijentima, uključujući korisnička imena i brojeve mobilnih telefona, s kineske Alibaba web stranice za kupnju 'Taobao', koristeći softver za indeksiranje koji je stvorio;
- LinkedIn – lipanj 2021. godine, utjecaj na 700 milijuna korisnika. S vodeće stranice za profesionalno umrežavanje LinkedIn u lipnju 2021. godine objavljeni su na tamnom webu podaci povezani sa 700 milijuna korisnika, što utječe na više od 90% njegove baze korisnika;
- Sina Weibo – ožujak 2020. godine, utjecaj na 538 milijuna računa. S više od 600 milijuna korisnika, Sina Weibo jedan je od najvećih kineskih društvenih medija. U ožujku 2020. tvrtka je objavila da je napadač dobio dio njihove baze podataka, što je utjecalo na 538 milijuna korisnika Weiba i njihove osobne podatke, uključujući prava imena, korisnička imena web mjesta, spol, lokaciju i telefonske brojeve. Navodi se da je napadač tada prodao bazu podataka na tamnom webu za 250 dolara;
- Facebook – travanj 2019. godine, utjecaj na 533 milijuna korisnika. U travnju 2019. otkriveno je da su dva skupa podataka iz Facebook aplikacija bila izložena javnom internetu. Podaci su se odnosili na više od 530 milijuna korisnika Facebooka i uključivali su telefonske brojeve, nazive računa i Facebook ID-ove. Međutim, dvije godine kasnije (travanj 2021.) podaci su objavljeni besplatno, što ukazuje na nove i stvarne kriminalne namjere koje okružuju podatke;

- MySpace – 2013. godine, utjecaj na 360 milijuna korisnika. Iako je odavno prestao biti moćno mjesto kao nekada, web stranica MySpace našla se na naslovnicama 2016. nakon što je 360 milijuna korisničkih računa procurilo na LeakedSource.com i stavljeno na prodaju na tamnom web tržištu 'The Real Deal' s traženom cijenom od 6 bitcoina (tada oko 3000 dolara).

13. Budućnost računarstva u oblaku

13.1. Trenutna ograničenja računarstva u oblaku

Kao što su naveli Sehgal, Bhatt i Acken (2020.) postoji nekoliko trenutnih ograničenja oblaka:

- Kretanje podataka – budući da se poslužitelji nalaze u udaljenom podatkovnom centru, svi ulazni podaci potrebni za računanje moraju se premjestiti tamo, a rezultati se moraju vratiti iz njih. Takve I/O (input-output) transakcije koštaju dodatni novac u većini javnih oblaka i povećavaju kašnjenje u usporedbi s računanjem na lokalnim poslužiteljima
- Gubitak kontrole – kada se e-poruke korisnika pohranjuju u oblaku, roboti ih često pregledavaju, a zatim odlučuju o prikazivanju relevantnih oglasa, kako bi generirali prihod davateljima usluga e-pošte, poput Googleovog Gmaila. Međutim, ovo postavlja pitanje tko je vlasnik sadržaja e-pošte i tko joj može pristupiti. Na primjer, ako postoji pravni slučaj i sudski pozivi davatelju usluga e-pošte da predaju e-poštu, davatelju usluga bit će teško reći ne. Na kraju, ako korisnik želi posjedovati sadržaj i držati ga privatnim, poput slika ili drugih poslovnih podataka, tada ga treba čuvati na lokalnom računalu.
- Percepcija sigurnosti u oblaku – iako više ljudi može pristupiti podatkovnom centru u oblaku, to možda nije ništa manje sigurno od podatkovnog centra u poduzeću. Zbog gubitka kontrole, kako je ranije spomenuto, postoji percepcija da je javni oblak manje siguran što ne mora nužno biti točno.
- Neizvjesne performanse – pružatelji usluga oblaka zarađuju dijeljenjem iste hardverske infrastrukture s mnogim korisnicima. Iako njihovi virtualni strojevi

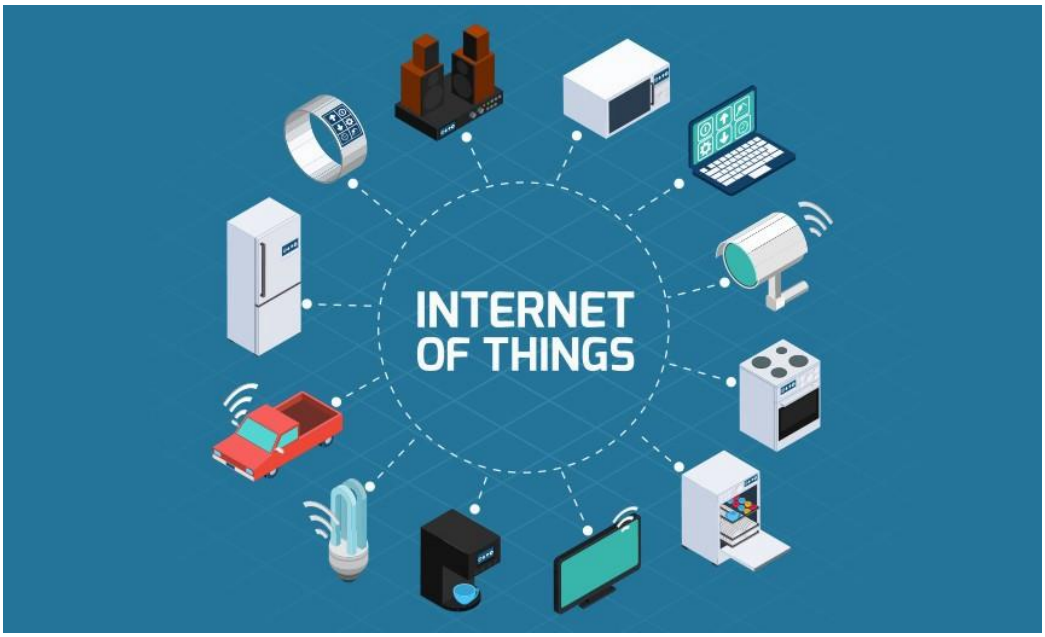
(VM) mogu biti izolirani u memoriji i raditi na različitim jezgrama poslužitelja, postoje i drugi dijeljeni resursi, poput memorijskog kontrolera i mrežne kartice kroz koje moraju proći podaci svakog VM-a. To stvara uska grla slična prometnim gužvama u podatkovnom centru na ulaznim i izlaznim mjestima, kao i ulasku i izlazu na zajedničke poslužitelje.

13.2. Pojava Interneta stvari (IoT)

Kao što tvrde Sehgal, Bhatt i Acken (2020.) još jedan trend u nastajanju je oblak vođen stvarima u odnosu na trenutno računarstvo u oblaku koje uglavnom vode ljudi. Na primjeru transporta i automobila radi se o softverski definiranoj kabini u komercijalnom zrakoplovu ili autonomnom vozilu. Izraz "Internet stvari" prvi je put upotrijebio britanski tehnološki vizionar Kevin Aston 1999. godine. Njegova je percepcija bila misliti na "objekte u fizičkom svijetu povezane senzorima".

Četiri osnovna komunikacijska modela za IoT su:
1. Uređaj prema uređaju
2. Uređaj prema oblaku
3. Uređaj prema gatewayju
4. Pozadinski model dijeljenja podataka

Ove nove prilike donose i nove sigurnosne izazove. Na primjer, ako su ti uređaji spojeni na Internet, tada haker može potencijalno dobiti pristup za čitanje izlaznih podataka ili promijeniti konfiguracije uređaja kako bi izazvao neočekivane rezultate.

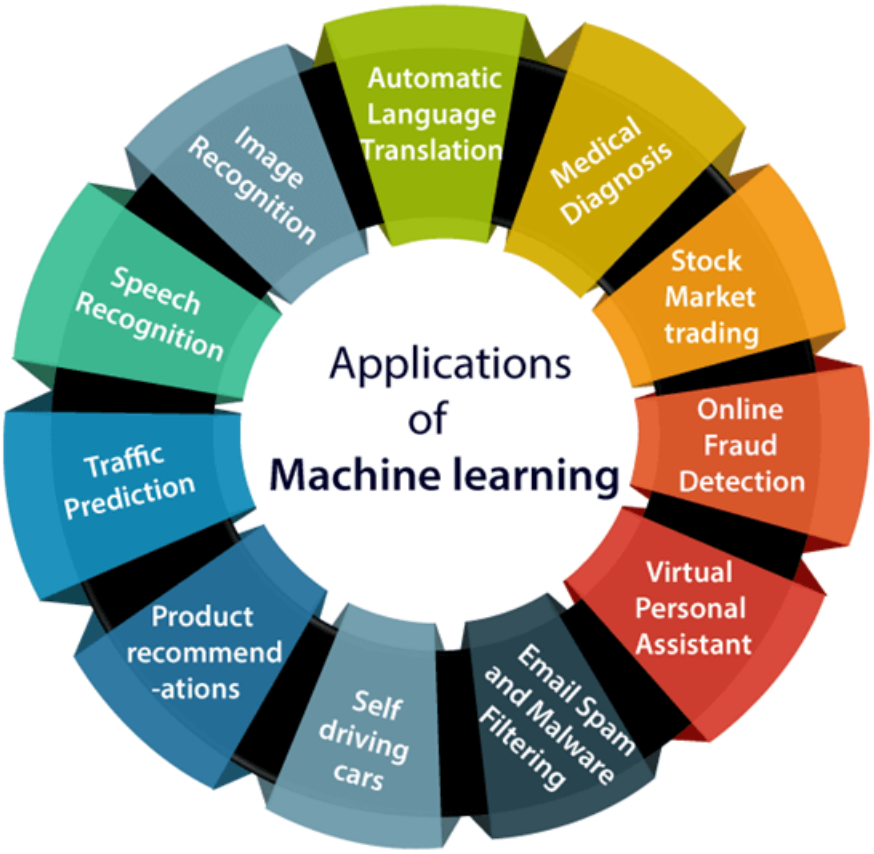


Slika 10. Internet of Things
Izvor: https://medium.com/agileinsider/internet-of-things-iot-101-7588a388ef70

13.3. Pojava strojnog učenja

Sehgal, Bhatt i Acken (2020.) navode primjer strojnog učenja gdje u kantini tvrtke s više radnih smjena i različitim brojem zaposlenika koji se poslužuju u različite dane, inteligentni hladnjak može provjeriti ima li preostalih zapakiranih namirnica, uključujući njihove datume isteka. Ako je cilj imati sastojke hrane u skladištu barem sljedeća dva dana, upravitelj kantine može se obavijestiti da ih po potrebi nadopuni. Dio strojnog učenja ne proizlazi iz nedostatka unaprijed određene zalihe, već iz samog učenja rješenja na temelju obrasca potrošnje zaposlenika. Ako je petak, a tvrtka je zatvorena sljedeća dva dana, tada će sustav tražiti potrebne zalihe do sljedećeg utorka. Također, u različite radne dane potrebni jelovnici i određene namirnice mogu varirati, pa zahtijevaju rješenje koje može inteligentno predvidjeti što je potrebno naručiti kako bi se smanjili troškovi i izbjeglo rasipanje hrane, a da se pritom osigura da bitni sastojci nikada neće teći. Općenito, takvi pametni uređaji nude željenu funkcionalnost i rade na energetski učinkovit način uz minimalnu računalnu snagu i memoriju dok su povezani s mobilnom aplikacijom i oblakom na stražnjoj strani. Sustavi strojnog učenja pokazali su se korisnima u maloprodaji jer dobavljači mogu pronaći artikle koje kupci kupuju ili ne, te

u skladu s tim izraditi sljedeći proizvodni nalog. Osim toga, mogu izraditi profile kupaca i predložiti dodatne artikle kupcima koji kupuju artikl, na temelju onoga što su drugi kupili nakon što su kupili isti predmet. To je pridonijelo ogromnom uspjehu internetskih trgovaca na malo kao što je Amazon.



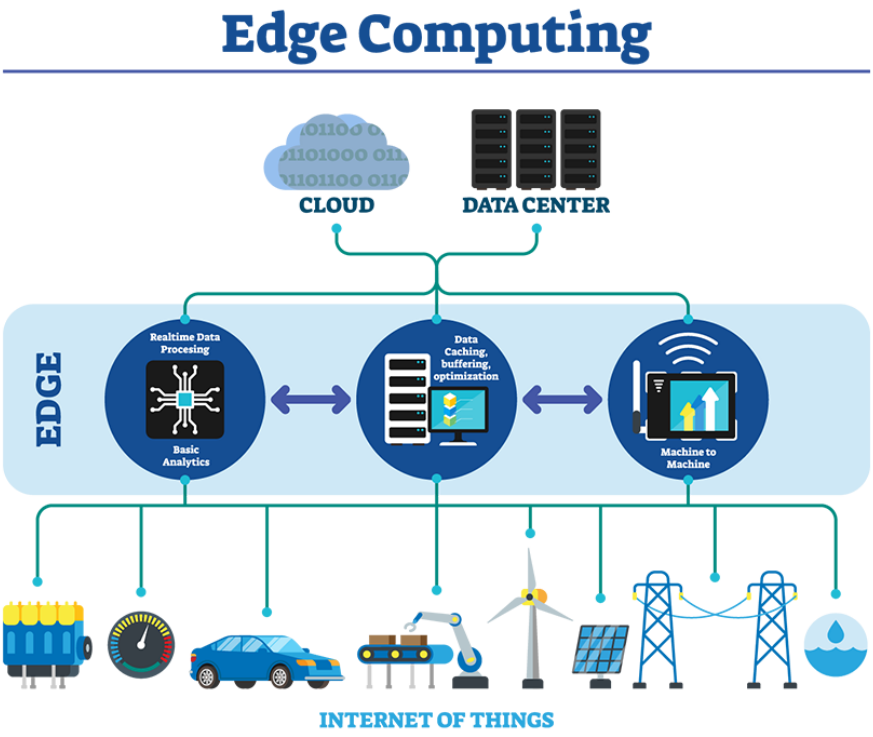
Slika 11. Svrhe u koje se može primjenjivati strojno učenje
Izvor: https://www.javatpoint.com/applications-of-machine-learning

13.4. Pojava rubnog računarstva

S mnogim IoT uređajima i slučajevima upotrebe imperativ je imati lokaliziranu računalnu snagu i pohranu podataka, kako navode Sehgal, Bhatt i Acken (2020.). Primjer je automobil. Sastoji se od ugrađenih kamera, IC senzora i podataka prikupljenih s motora, kočnica itd. Međutim, autonomni automobil ne može pauzirati poslužitelj u oblaku da donese odluku o ubrzanju ili kočenju. Stoga mu je potrebna dovoljna proračunska snaga u automobilu za sigurnu vožnju, a neki ga nazivaju "podatkovnim

centrom na kotačima". Može se sinkronizirati s udaljenim podatkovnim centrom u oblaku preko noći dok je parkiran, ali na cesti se mora usredotočiti na sigurnu vožnju uz donošenje odluka u stvarnom vremenu. Stoga se dio oblaka migrira iz udaljenog podatkovnog centra u polje, što se naziva rubno računanje. Slični primjeri mogu se naći i u drugim domenama primjene, poput pametnih kuća sa sigurnosnim kamerama, koje na licu mjesta mogu odlučiti je li uljez član obitelji ili stranac te u potonjem slučaju oglasiti alarm. Ipak, i ovdje se javljaju sigurnosni rizici. Čak i za jednostavan sustav kućne automatizacije, poput inteligentne brave na vratima, za sigurnost su potrebne sljedeće sigurnosne značajke:

1. Vatrozid za odvraćanje udaljenih hakera od autentifikacije za prijavu.
2. Za provjeru autentičnosti potrebna je identifikacija telefonskih brojeva, lozinke ili biometrije kao što su prepoznavanje lica, otisak palca, skeniranje mrežnice itd.



Slika 12. Rubno računanje
Izvor: https://forum.huawei.com/enterprise/en/edge-computing-a-cutting-edge-technology/thread/734895-893?page=1

Da bi se osiguralo povjerenje u rubno računanje, mora se početi s pouzdanim okruženjem, pouzdanim protokolima i komponentama zaštićenim od neovlaštenog pristupa. Dobavljači moraju za početak ponuditi "anti-tamper“ rješenja, tj. rješenja protiv ometanja rada. Nadogradnja softvera na terenu potrebna je za sve ispravke programskih pogrešaka tijekom vijeka trajanja rubnog računalnog uređaja. Sigurni kanal mora postojati za pružanje potpisanih binarnih paketa koji se prenose i instaliraju na terenu, na primjer, u automobilu ili na televizoru kod kuće. U našem primjeru vrata dobavljač mora pružiti antitamper rješenje kako bi spriječio da netko lokalno mijenja firmware ili postavke na neovlašten način. Čak i nadogradnje softvera na daljinu moraju biti provjerene. Inače, nezaštićeni kućanski aparati mogu se koristiti za pokretanje kibernetičkih napada.

14. Zaključak

Od 60-ih godina kada se postavljaju njegovi temeljni koncepti pa do danas, računarstvo u oblaku je doživjelo velike promjene. Rastom popularnosti računala i mobilnih uređaja, raste i njegov opseg, kao i količina podataka i informacija koje dijelimo i pohranjujemo. Obavljanjem naizgled bezopasnih radnji kao što su kupnja preko interneta, rezervacija hotela itd. ipak izlažemo svoje podatke sigurnosnim rizicima. Pohranjivanjem i dijeljenjem podataka koristeći oblak, pojedinac gubi određenu kontrolu nad svojim podacima te njihova sigurnost i privatnost ne ovise samo o njemu, već i o pružatelju usluge oblaka. Sigurnosnih rizika i prijetnji podacima u oblaku je mnogo, od neovlaštenog pristupa podacima do neadekvatnog brisanja podataka. Iz tog razloga i pojedinac i organizacije trebaju poduzeti prikladne mjere za zaštitu osobnih ili za poslovanje kritičnih podataka, a prije svega donijeti informiranu odluku pri izboru pružatelja usluge oblaka i odgovarajuće vrste i modela oblaka. Osim sigurnosnih rizika i prijetnji, postavlja se i pitanje privatnosti podataka. Transparentnost je jedna od primarnih briga, moraju se postaviti pitanja kao što su gdje se podaci nalaze, tko ima pristup tim podacima i što se s njima radi. Plan za sigurnosne mjere, kontrola pristupa i redovno nadziranje sustava neki su od koraka koje je moguće poduzeti kako bi se osigurala željena razina sigurnosti i privatnosti podataka.

15. Literatura

1. American Institute of Certified Public Accountants (AICPA) and CICA: Generally accepted privacy principles. Dostupno na: http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/generallyacceptedprivacyprinciples/downloadabledocuments/gapp_prac_%200909.pdf(2009.)

2. Bronzin, T., Adamec, D. (2011) Uzlet u oblake, Infotrend, 184, p. 25-27

3. Cert Carnet (2010.), Cloud Computing, dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-03-293.pdf

4. Coyne, L. et. al., (2018.) IBM Private, Public, and Hybrid Cloud Storage Solutions, Redbooks

5. Daniels, J. (2009.) Server virtualization architecture and implementation. Crossroads, 16(1):8–12

6. Data Protection Commission, Principles of Data Protection (n.d.) Dostupno na: https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection

7. Elmroth, E. et al. (2009.) Accounting and billing for federated cloud infrastructures. In Grid and Cooperative Computing, 2009. GCC'09. Eighth International Conference on, pages 268–275. IEEE

8. European Commission: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://ec.europa.eu/justice/policies/privacy/docs/95- 46-ce/dir1995-46_part1_en.pdf (1995.)

9. Goel A. Fleet telematics real-time management and planning of commercial vehicle operations. Operations Research/Computer Science Interfaces Series. 2008:40

10. Grossman, R. L., Gu, Y., Sabala, M., i Zhang, W. (2009.) Compute and storage clouds using wide area high performance networks. Future Generation Computer Systems, 25(2):179–183

11. Hill, M. i Swinhoe, D. (2021.) The 15 biggest data breaches of the 21st century,

dostupno na: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
12. ISO: 27001: Information Security Management – Specification with Guidance for Use. ISO, London (2005.)
13. Johnson, D. (2021.) 'What is Dropbox?': How to use the cloud-based file-storage service for collaboration, dostupno na: https://www.businessinsider.com/what-is-dropbox
14. Kalluri, R. i Rao, C. V. G. (2014.) Adressing the Security, Privacy and Trust Challenges of Cloud Computing
15. Kirschnick, J. et al. (2010.) Toward an architecture for the automated provisioning of cloud services. IEEE Communications Magazine, 48(12):124–131, 2010.
16. Kumar, V., Chaisiri, S., i Ko, R. (2017.) Data Security in Cloud Computing, Springer
17. Liotine, M. (n.d.) Integrating Cloud Computing with Next-Generation Telematics for Energy Sustainability in Vehicular Networks, University of Illinois at Chicago, Chicago, Illinois, USA
18. Mathur, S. (2019.) Top 15 Benefits of Cloud Computing, dostupno na: https://www.impigertech.com/resources/blogs/benefits-of-cloud-computing
19. Nissenbaum, H.: Privacy as contextual integrity. Washington Law Rev. 79 , 101–139 (2004.) 15.
20. Nissenbaum, H.: Privacy in Context: Technology, Policy and the Integrity of Social Life. Stanford University Press, Stanford (2009.)
21. Ohri, A. (2021.) Top 10 Disadvantages and Advantages of Cloud Computing, dostupno na: https://www.jigsawacademy.com/blogs/cloud-computing/advantages-of-cloud-storage/
22. Panian, Ž (2013.) Elektroničko poslovanje druge generacije
23. Pearson, S. i Yee, G. (2013.) Privacy and Security for Cloud Computing, Springer
24. Pickavance, M., Nield, D. i DeMuro, J. P. (2021.) Box cloud storage review, dostupno na: https://www.techradar.com/reviews/box
25. Ponnusamy, D. (n.d.) Cloud Computing Security Issues
26. Rittinghouse, J. W. i Ransome, J. F. (2010.) Cloud Computing, Implementation, Managment and Security, CRC Press

26. Sehgal, N. K. i P. Bhatt, P. C. (2018.) Cloud Computing, Concepts and Practices, Springer
27. Sehgal, N. K., P. Bhatt, P. C. i Acken J. M. (2020.) Cloud Computing With Security, Concepts and Practices, Springer
28. Sen, J. (n.d.) Security and Security and Privacy Issues in Cloud Computing
29. Solove, D.J.: A taxonomy of privacy. Univ. Pennsylvania Law Rev. 154 (3), 477 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622 (2006.)
30. Srinivasan, S. (2014.) Cloud Computing Basics, Springer
31. Sultan, N. (2010) Cloud computing for education: A new dawn?, International Journal of Information Management, dostupno na: https://www.sciencedirect.com/science/article/pii/S0268401209001170
32. Swire, P.P., Bermann, S.: Information Privacy: Official Reference for the Certified Information Privacy Professional, CIPP. International Association of Privacy Professionals, York (2007.)
33. Vacca, J. R. (2017.), Cloud Computing Security, Foundations and Challenges, CRC Press
34. Warren, S. i Brandeis, L. (1890.) The Right to Privacy, Harv. Law Rev. 4, 193.
35. Westin, A.: Privacy and Freedom. Atheneum, New York (1967.)
36. Wheeler, A. i Winburn, M. (2015.) Cloud Storage Security, A Practical Guide, Elsevier
37. Whitney, L. (2020.) How to share files using Microsoft OneDrive, dostupno na: https://www.techrepublic.com/article/how-to-share-files-using-microsoft-onedrive/

16. Popis slika

17. Popis tablica

18. Sažetak

Tema ovog diplomskog rada je „Privatnost i sigurnost podataka u oblaku, “ a cilj je istaknuti rizike sigurnosti i privatnosti podataka u računarstvu u oblaku što bi pomoglo u informiranom donošenju odluke o modelu i vrsti oblaka koji izabrati za pohranu podataka i informacija, pogotovo ako se radi o osjetljivim podacima ili podacima kritičnim za poslovanje organizacije. Opisani su i koraci koje treba uzeti u obzir pri prelasku u oblak i načini zaštite podataka u oblaku, kao i načini na koji pružatelj usluga oblaka i korisnici mogu upravljati rizikom. Nadalje, navedene su neke od najznačajnijih povreda podataka u oblaku na primjeru kojih je moguće vidjeti razmjere napada i njihov utjecaj na podatke pojedinaca.

Ključne riječi: računarstvo u oblaku, privatnost i sigurnost podataka, sigurnost računarstva u oblaku, privatnost podataka, prijetnje i ranjivosti podataka u oblaku, zaštita podataka

19. Abstract

The topic of this thesis is "Privacy and security of data in the cloud," and it aim to highlight the risks of security and privacy of data in cloud computing which would help make informed decisions about the model and type of cloud to choose for data and information storage, especially if it is sensitive data or data critical to the business of the organization. It also describes the steps to consider when moving to the cloud and how to protect data in the cloud, as well as how cloud providers and users can manage risk. Furthermore, some of the most significant data breaches in the cloud are listed on the example of which it is possible to see the scale of attacks and their impact on individuals data.

Keywords: cloud computing, data privacy and security, cloud computing security, data privacy, cloud data threats and vulnerabilities, data security