UNIVERZITET U SARAJEVU
EKONOMSKI FAKULTET

ZAVRŠNI RAD

SIGURNOSNI ASPEKTI CLOUD COMPUTING

Sarajevo, juli 2024. NEJRA DERVIŠEVIĆ

U skladu sa članom 54. Pravila studiranja za I, II ciklus studija, integrisani, stručni i specijalistički studij na Univerzitetu u Sarajevu, daje se

IZJAVA O AUTENTIČNOSTI RADA

Ja, Nejra Dervišević, student drugog (II) ciklusa studija, broj index-a 4092, na programu Menadžment, smjer Menadžment i informacione tehnologije, izjavljujem da sam završni rad na temu:

SIGURNOSNI ASPEKTI CLOUD COMPUTING

pod mentorstvom prof.dr. Save Stupara izradila samostalno i da se zasniva na rezultatima mog vlastitog istraživanja. Rad ne sadrži prethodno objavljene ili neobjavljene materijale drugih autora, osim onih koji su priznati navođenjem literature i drugih izvora informacija uključujući i alate umjetne inteligencije.

Ovom izjavom potvrđujem da sam za potrebe arhiviranja predala elektronsku verziju rada koja je istovjetna štampanoj verziji završnog rada.

Dozvoljavam objavu ličnih podataka vezanih za završetak studija (ime, prezime, datum i mjesto rođenja, datum odbrane rada, naslov rada) na web stranici i u publikacijama Univerziteta u Sarajevu i Ekonomskog fakulteta.

U skladu sa članom 34. 45. i 46. Zakona o autorskom i srodnim pravima (Službeni glasnik BiH, 63/10) dozvoljavam da gore navedeni završni rad bude trajno pohranjen u Institucionalnom repozitoriju Univerziteta u Sarajevu i Ekonomskog fakulteta i da javno bude dostupan svima.

Sarajevo, 09. 01. 2024. Potpis studenta/studentice: Nejra Dervšević

SAŽETAK

Cloud computing pruža računarske i komunikacijske mogućnosti putem Interneta. Od obrade i pohranjivanja informacija i aplikacija, do mogućnosti pristupa s bilo kojeg mjesta i u bilo koje vrijeme, Cloud computing predstavlja proboj u načinu na koji ljudi i kompanije rade i komuniciraju putem Interneta. Posljednjih godina Cloud computing bilježi konstantan porast u svim svojim aspektima. Razvojem ICT tehnologija (na globalnom nivou) ograničenja u pružanju cloud usluga više ne postoje i tržište se ne može posmatrati na lokalnom nivou. Potrebno je razmotriti globalnu sliku i ponudu usluga u Cloudu koja dolazi od globalnih pružatelja usluga u Cloudu. U ovom radu prikazana je situacija u Bosni i Hercegovini po pitanju Cloud computinga.

Napredak informaciono-telekomunikacijske tehnologije omogućio je velikim i malim kompanijama pristup najsavremenijim tehnologijama zahvaljujući kojima mogu povećati profitabilnost i konkurentnost uz smanjenje troškova poslovanja. Pojedine kompanije baziraju svoje poslovanje na cloud tehnologiji, ali većina kompanija ima hardverske resurse na temelju kojih kreira platformu potrebnu za rad jednog ili više informacionih sistema.

Uprkos mnogim prednostima i sve većoj popularnosti, Cloud computing ima problem zbog povjerenja. Utvrđeno je da je povjerenje jedan od glavnih izazova za usvajanje Cloud computinga, s obzirom da nepovjerenje utiče na odluku korisnika da ga usvoje. Povjerenje i sigurnost su dvije od najkritičnijih prepreka za usvajanje i rast Cloud computinga danas. Stoga, da bi se privukle kompanije da implementiraju Cloud computing, potrebno je rješenje za sigurnost podataka i povjerenje.

Ključne riječi: Cloud computing, cloud usluge, tehnologija, digitalizacija, sigurnost, povjerenje.

ABSTRACT

Cloud computing provides computing and communication capabilities via the Internet. From processing and storing information and applications, to the possibility of access from anywhere and at any time, Cloud computing represents a breakthrough in the way people and companies work and communicate via the Internet. In recent years, Cloud computing has seen a constant increase in all its aspects. With the development of ICT technologies (on a global level), limitations in the provision of cloud services no longer exist and the market cannot be observed at the local level. It is necessary to consider the global picture and the Cloud service offering coming from global Cloud service providers. This paper presents the situation in Bosnia and Herzegovina regarding Cloud computing.

The progress of information and telecommunications technology has enabled large and small companies to access the most modern technologies thanks to which they can increase profitability and competitiveness while reducing business costs. Some companies base their business on cloud technology, but most companies have hardware resources on the basis of which they create the platform necessary for the operation of one or more information systems.

Despite its many advantages and growing popularity, Cloud computing has a trust problem. Trust has been found to be one of the main challenges to cloud computing adoption, with mistrust influencing users' decision to adopt it. Trust and security are two of the most critical

barriers to cloud computing adoption and growth today. Therefore, to attract companies to implement Cloud computing, a solution for data security and trust is needed.

Keywords: Cloud computing, cloud services, technology, digitization, security, trust.

SADRŽAJ

POPIS SLIKA

POPIS TABELA

POPIS GRAFIKONA

POPIS PRILOGA

1. UVOD

Svakodnevni i poslovni život danas je jednostavno nezamisliv bez upotrebe Interneta i novih tehnologija. Informacije su dostupne u svakom trenutku bez obzira gdje se čovjek nalazi Informacione tehnologije imaju posebno intenzivan razvoj posljednjih godina. Kompanije daju sve veći značaj svojim informacionim resursima.

Savremene kompanije sve više primjenjuju informatiku u svim segmentima svog poslovanja. Sadašnje i buduće doba je doba informacionih tehnologija (IT). Informaciona tehnologija (IT) i poslovanje, uvijek usko povezani, postaju praktično neodvojivi. Krećući se sa svoje tradicionalne uloge pokretača organizacione efektivnosti i efikasnosti, IT odjeli danas često preuzimaju vodeće uloge kako bi usmjerili kompanije u nove industrije i tržišta. Sve veći broj kompanija stavlja naglasak na iskorištavanje svojih IT investicija i njihovo usklađivanje s organizacionim ciljevima. Za današnje online poslovanje neuspjeh njihovih IT sistema je poslovni neuspjeh. Za te poslove je potrebno mnogo rigoroznije IT upravljanje. Upravljanje IT-om više nije samo IT pitanje, već pitanje poslovnog upravljanja od velikog interesa koje je na vrhu prioriteta većine kompanija širom svijeta. Gotovo sve moderne kompanije se u velikoj mjeri oslanjaju na kompjuterske informacione sisteme za obradu podataka potrebnih za vođenje njihovog poslovanja, za zadatke kao što su upravljanje podacima zaposlenih, praćenje prodaje i zaliha, angažovanje u razvoju proizvoda, predviđanje buduće potražnje i održavanje informacija o kupcima.

S obzirom da smo svjedoci svakodnevnog razvoja informacione nauke, skoro pa svakoga dana informatika nam pruža nove mogućnosti. Između ostalog jedan od najvećih razvoja u informacionoj nauci je razvoj Interneta koji se koristi u različitim dijelovima svijeta za različite namjene. Uz brojne svrhe korištenja Interneta jedna od svakako zanimljivijih i novijih usluga koje nam pruža Internet je sve veća mobilnost podataka. Cijeli taj sistem doživio je veliki napredak u posljednjih nekoliko godina, a naziva se Cloud computing ili računarstvo u oblaku. To je tehnologija u kojoj korisnici sve radnje obavljaju preko Interneta, a za to im je isključivo potreban uređaj, Internet veza i pretraživač.

Prema Dhiman i Joshi (2014), računarstvo u oblaku je model koji omogućuje sveprisutan, praktičan mrežni pristup na zahtjev zajedničkom skupu konfigurabilnih računarskih resursa uključujući mrežu, poslužitelj, pohranu, aplikaciju i usluge, uz minimalan napor upravljanja ili interakciju pružatelja usluga.

Cloud computing se najjednostavnije može definisati kao pohranjivanje, obrada i upotreba podataka na udaljenim računarima kojima se pristupa putem Interneta. To znači da korisnici ne moraju vršiti velika kapitalna ulaganja za ispunjavanje njihovih potreba i da do svojih podataka mogu doći bilo gdje gdje ima internetska veza. Bitno je istaći da Cloud computing može smanjiti troškove IT-a, ali isto tako može omogućiti razvijanje mnogih novih usluga. Poput Interneta, i Cloud computing prati tehnološki razvoj koji traje već neko vrijeme, te se

i dalje nastavlja razvijati. Za razliku od weba, Cloud computing je još uvijek u relativno ranoj fazi.

Računarstvo u oblaku je postalo značajan i dobro poznat pojam u kratkom vremenskom periodu. Cloud računarstvo je brzo i uspješno dobilo ključnu ulogu u informacionim tehnologijama, a time i u načinu na koji organizacije danas upravljaju svojim IT odjelima. Njegove mnoge prednosti privlače organizacije da implementiraju rješenje u oblaku. Uprkos značajnom rastu, računarstvo u oblaku i dalje ima svoje nedostatke. Jedan od njegovih problema se pojavio kao sigurnosni problem, što je dovelo do toga da su mnoge kompanije odlučile da ne implementiraju rješenje u oblaku i umjesto toga zadrže svoj tradicionalni sistem.

Utvrđeno je da je povjerenje jedan od glavnih izazova za usvajanje računarstva u oblaku, jer nepovjerenje utiče na odluku korisnika da ga usvoje, posebno onih korisnika koji nemaju direktnu kontrolu nad svojim podacima koji leže u oblaku. Stoga je vrednovanje povjerenja i njegovog uticaja postalo kritično pitanje. Povjerenje i sigurnost su dvije od najkritičnijih prepreka za usvajanje i rast računarstva u oblaku danas (Rathi, Kumari, 2015). Stoga ovo istraživanje istražuje faktore koji utiču na percipirano povjerenje prema usvajanju aplikacija temeljenih na pohrani u oblaku u Bosni i Hercegovini.

Napredak informaciono-telekomunikacijske tehnologije i sve veća primjena cloud tehnologija utiče na kreiranje novih servisa i poslovnih rješenja što istovremeno uzrokuje i kreiranje novih rizika u informacionim sistemima, međutim simultano se kreiraju i nova rješenja i potrebni sistemi zaštite.

1.1. Obrazloženje teme

U ovom radu će biti obrađena tema savremenih rizika i izazova u informacionim sistemima što podrazumijeva analizu tradicionalnih rješenja, korištenje informacionih sistema i njihovih rizika sa aspekta sigurnosti u odnosu na pojavu i korištenje novih tehnologija.

Također, moguće je uočiti nove trendove u pogledu generisanja velike količine podataka u jedinici vremena što predstavlja nove zahtjeve u pogledu rizika poslovanja kompanija. Podaci kompanija koji se generišu iz većeg broja informacionih sistema predstavljaju resurs kompanije koji pravilnim korištenjem može unaprijediti poslovanje i vrijednost kompanije. Međutim, povećana ovisnost od informacionih sistema sa aspekta korištenja podataka na bilo kojem mjestu u bilo kojem trenutku sa bilo kojeg uređaja kreira nove trendove i izazove zaštite podataka i informacionih sistema. Nerijetko, savremeni sistemi zašite informacionih sistema i povećanja stepena sigurnosti zahtijevaju korištenje savremenih tehnologija koje je nerijetko moguće ostvariti jedino korištenjem cloud usluga.

Kada govorimo o novim trendovima i izazovima u sigurnosti neizostavan dio je i definisanje savremenih tehnologija čija implementacija često zahtijeva značajne promjene unutar kompanija koje se mogu posmatrati i kao proces digitalne transformacije.

Korištenje savremenih tehnologija, ali i svijest o rizicima istih je povećana u posljednjem periodu, naročito tokom pandemije kada su kompanije, zbog eksternih uticaja, bile primorane u značajnoj mjeri prilagoditi svoje poslovanje što je uglavnom značilo promjenu lokacije rada zaposlenih. Nova promjena u poslovanju kompanija je predstavljala priliku ulaska u proces digitalne transformacije, korištenja novih tehnologija, ali i istovremeno prijetnju novih sigurnosnih rizika koji mogu značajno uticati na poslovanje i imidž kompanije.

Ovaj rad će sagledati mogućnost implementacije Cloud computinga u preduzećima u Bosni i Hercegovini, a putem istraživačkog dijela rada će se odrediti nivo zastupljenosti ove savremene tehnologije u našoj zemlji, koja se već intenzivno koristi u razvijenim zemljama.

1.2. Problem i predmet istraživanja

Sigurnosni problemi u računarstvu u oblaku vide se kao prepreka i stoga su jedan od glavnih razloga zbog kojih su današnje kompanije spriječene da usvoje rješenje u oblaku i umjesto toga nastavljaju koristiti tradicionalni sistem. Da bi se privukao veći broj kompanija da počnu koristiti računarstvo u oblaku, potrebno je rješenje za sigurnost podataka i povjerljivost (Karnwal, Sivakumar i Aghila 2011).

Ogigau-Neamtiu (2012) dalje objašnjava da postoje dodatni problemi koji se javljaju u vezi sa podacima; navedeni problemi su sastavljeni u životnom ciklusu sigurnosti podataka, koji se odnosi na kontrolu podataka. Problemi uključuju kreiranje, pohranu, modifikaciju, sigurnosno kopiranje i uklanjanje podataka. Ciklus se može naći u okruženju u oblaku i u okruženju koje nije u oblaku, ali faze u okruženju oblaka imaju tendenciju da budu složenije sa većim sigurnosnim rizicima i stoga je pažljiviji menadžment od suštinskog značaja.

Chowdhury (2014) objašnjava da se smanjenje rasta usvajanja računarstva u oblaku uglavnom veže za sigurnosne probleme. Zissis i Lekkas (2010) objašnjavaju da je za identifikaciju jedinstvenih izazova i prijetnji važno da se razumiju informacioni sistem (IS). Kada se sa sigurnosti Cloud computinga upravlja na pravi način, bitno je navesti dvije stavke, odnosno sigurnosnu identifikaciju prijetnji i povjerenje. Identifikacija se odnosi na povjerljivost, privatnost, integritet i dostupnost. Kroz ove faktore lakše je postići percepciju i razumijevanje sigurnosti oblaka.

Važnost usvajanja oblaka i njegovih korisnih karakteristika povećala je interesovanje među kompanijama. Kompanije danas, uglavnom mala i srednja preduzeća, postaju sve svjesnije korisnosti usluga koje se pružaju. Prednosti se odnose na brz pristup nekim od najboljih aplikacija i usluga koje će drastično promijeniti kompanijinu infrastrukturu, odnosno usvajanje oblaka za njihov posao, uz zanemarljiv trošak.

Danas su mnoge kompanije u iskušenju sa tehnikama virtualizacije oblaka sa ciljem poboljšanog korištenja resursa i smanjenja obima posla. Uloga oblaka u IT svijetu i njegova važnost za kompanije je od suštinskog značaja s obzirom na kontinuiran rast. Postojeća

istraživanja i studije ističu da su glavni problemi zbog kojih kompanije odlučuju da ne implementiraju računarstvo u oblaku nedostatak sigurnosti, povjerenja i privatnosti.

Pitanje sigurnosti je jedna od najvećih zabrinutosti iz perspektive kupaca, koja se vidi kao motiv za neusvajanje rješenja u oblaku. Problemi su uglavnom naglašeni zajedno sa vrstama sigurnosnih okvira koje treba primijeniti kao korisnik. Ako postoje identifikovani sigurnosni aspekti koje zahtijevaju organizacije, oni mogu biti povezani sa osnovnim razlozima zbog kojih se ne usvajaju rješenja u oblaku. Ovi temeljni razlozi su bitni jer rezultiraju odlukom da se ne uđe u cloud okruženje.

1.3. Hipoteze istraživanja

Na osnovu problema prikazanih u diskusiji problema, utvrđeno je da su sigurnosni problemi jedan od glavnih razloga zašto organizacije odlučuju da ne usvoje računarstvo u oblaku u svom poslovanju. Studije i istraživanja ilustruju prednosti prelaska na oblak. Ali čak i ako su kompanije svjesne ovih prednosti, mnoge od njih i dalje upotrebljavaju tradicionalni sistem. Važno je shvatiti stavove organizacija u vezi sa ovim pitanjima.

Navode se sljedeće hipoteze istraživanja:

- H1: Dostupnost je pozitivno povezana sa sigurnošću u Cloud computingu.
- H2: Dugoročna održivost je pozitivno povezana sa sigurnošću u Cloud computingu.
- H3: Backup i Recovery su pozitivno povezani sa sigurnošću u Cloud computingu.
- H4: Sigurnost je pozitivno povezana s povjerenjem korisnika Cloud computinga.
- H5: Pouzdanost je pozitivno povezana sa sigurnošću Cloud computinga.
- H6: Pouzdanost je pozitivno povezana s povjerenjem korisnika Cloud computinga.

1.4. Ciljevi istraživanja

Glavni cilj ovog istraživačkog rada je identifikovati i razumjeti sigurnosne probleme koji utiču na performanse Cloud computinga. Također, bitno je razumijevanje sigurnosnih tehnika koje se koriste za ublažavanje ovih sigurnosnih problema.

Ostali ciljevi ovog istraživanja su:

- Identifikovati sigurnosne izazove koji se očekuju u budućnosti Cloud computinga.
- Predložiti neke mjere za buduće izazove sa kojima se treba suočiti Cloud computing.

Dakle, cilj rada je istražiti probleme sigurnosti i istražiti metode zaštite podataka u Cloud computingu.

1.5. Metodologija istraživanja

Metode kojima će se koristiti u ovom radu su metoda deskripcije, metoda sinteze i analize, i metoda komparacije. Korištene kroz cijeli rad, ove metode pogodne su za predmetno istraživanje jer istovremeno omogućavaju navođenje obrađene literature i kritički stav prema ključnim pitanjima teme. Metode prikupljanja podataka su one metode koje se koriste prilikom prikupljanja podataka. Često, kada se misli na prikupljanje podataka, to se odnosi na klasifikaciju i obradu podataka sve do izvođenja potrebnih zaključaka na osnovu tih podataka. U metode prikupljanja se ubrajaju neke od sljedećih metoda: ispitivanje, studija slučaja, posmatranje, analiza dokumenata, eksperimentisanje, test i biografska metoda. U ovom master radu za prikupljanje podataka je najviše korištena metoda analize dokumenata. Metoda analize dokumenata obuhvata prikupljanje, selekciju i proučavanje postojećih izvora, kao što su teorije i prakse iz udžbenika, knjiga, radova, te slične literature nabavljene iz različitih izvora. Svakako da je najbolji i najveći izvor informacija Internet. Najviše literature za ovaj rad dolazi upravo s Interneta kao najrasprostranjenijeg medija. S ovom istraživačkom metodom je obuhvaćen pogled i na stranu i na domaću literaturu. Potrebno je istaknuti da je u domaćoj literaturi o ovoj temi jako teško pronaći adekvatan materijal koji je moguće iskoristiti. Veoma malo populacije u regiji se bavi tematikom Cloud computinga i samim tim, obim literature na regionalnim jezicima je jako oskudan.

Metode obrade podataka su u principu grupa metoda. Praksa u istraživanju pokazuje da se ove metode najviše pojavljuju kao dijelovi nekih općih metoda istraživanja ili kao produžeci tih metoda. Na primjer, razne vrste analize podataka, kada nema istraživanja samo su varijante analize kao osnovne metode. Isto tako je i sa metodama zaključivanja.

Svrha ovog istraživanja je da se razvije i poveća znanje o tome koji su to sigurnosni aspekti koje organizacije imaju prema različitim rješenjima u oblaku, uključujući i pružanje znanja o poznatim sigurnosnim pitanjima koja mogu biti povezana sa sigurnosnim aspektima. Pregledom istraživanja pokazalo se da brojna dosadašnja istraživanja preciziraju da se bezbjednosna pitanja posmatraju kao veliki problem i objašnjavaju kao jedan od glavnih faktora zašto kompanije odlučuju da ne prelaze na oblak.

Cloud computing ima veliku ulogu u IT današnje industrije, a korisne usluge mogu biti osnovni razlog njegovog brzog rasta. Da bi se industrija unaprijedila, potrebno je identifikovati i riješiti probleme. Identifikovanjem sigurnosnih aspekata koje su istakle same kompanije, može se doći „korak bliže“ prema dugoročnom procesu pronalaženja i pružanja odgovarajućih rješenja.

Istraživanje će obuhvatati aspekt tehnlogija i servisa koji mogu i koji jesu predmet sigurnosnog rizika, poput načina pristupa cloud resursima, mrežnim komponentama cloud servisa, zaštite podataka, autentifikacije i verifikacije i drugih aspekata koji se na direktan ili indirektan način koriste za prevencije ili zaštitu od savremenih sigurnosnih rizika. Dio

istraživanja će sadržavati i analizu vrsta sigurnosnih izazova i preporuka za eliminaciju ili umanjenje sigurnosnih rizika.

2. TEORIJSKE OSOBINE CLOUD COMPUTINGA

2.1. Pojam Cloud computinga

Računarstvo u oblaku (engl. Cloud computing) kao savremeni pojam u informacionom društvu se najjednostavnije definiše kao koncept kod kojeg krajnji korisnik može bilo gdje držati svoje podatke, može koristiti bilo koju aplikaciju, bilo koju infrastrukturu i platformu (Davidović, 2011). Dakle, njemu nije potreban posebni hardver za spremanje svojih podataka jer su oni smješteni u tzv. oblak. Pri tome korisnik može računati na zaštitu od neovlaštenog pristupa, privatnost svojih podataka, brz pristup i dostupnost podacima te sveukupnu elastičnost.

Prema Kretschmeru (2012), Cloud computing pojednostavljeno se može shvatiti kao pohranjivanje, obrada i upotreba podataka sa različito lociranih računara kojima se pristupa putem Interneta. To znači da korisnici mogu narediti gotovo neograničen broj zahtjeva računaru, te ne moraju činiti velika kapitalna ulaganja za ispunjavanje njihovih potreba i da do svojih podataka mogu doći bilo gdje i u bilo kom trenutku putem internetske veze. Cloud computing kao isporuka različitih usluga putem Interneta, uključuje pohranu podataka, servere, baze podataka, umrežavanje i softver. Pohrana u oblaku postaje sve popularnija među pojedincima kojima je potreban veći prostor za pohranu i za kompanije koje traže efikasno rješenje za sigurnosnu kopiju podataka izvan lokacije. Na ovaj način se ostvaruje ušteda troškova, povećava produktivnost, brzina i efikasnost, performanse i sigurnost. Skladištenje u oblaku omogućava spremanje datoteka u udaljenu bazu podataka i njihovo preuzimanje na zahtjev. Sigurnost u oblaku postaje sve važnija oblast u IT-u.

Računarstvo u oblaku premješta sav posao obrade i održavanja podataka u ogromne kompjuterske klastere daleko u sajber prostoru. Internet postaje oblak, a naši podaci, posao i aplikacije dostupni su sa bilo kojeg uređaja s kojim se možemo povezati na Internet, bilo gdje u svijetu.

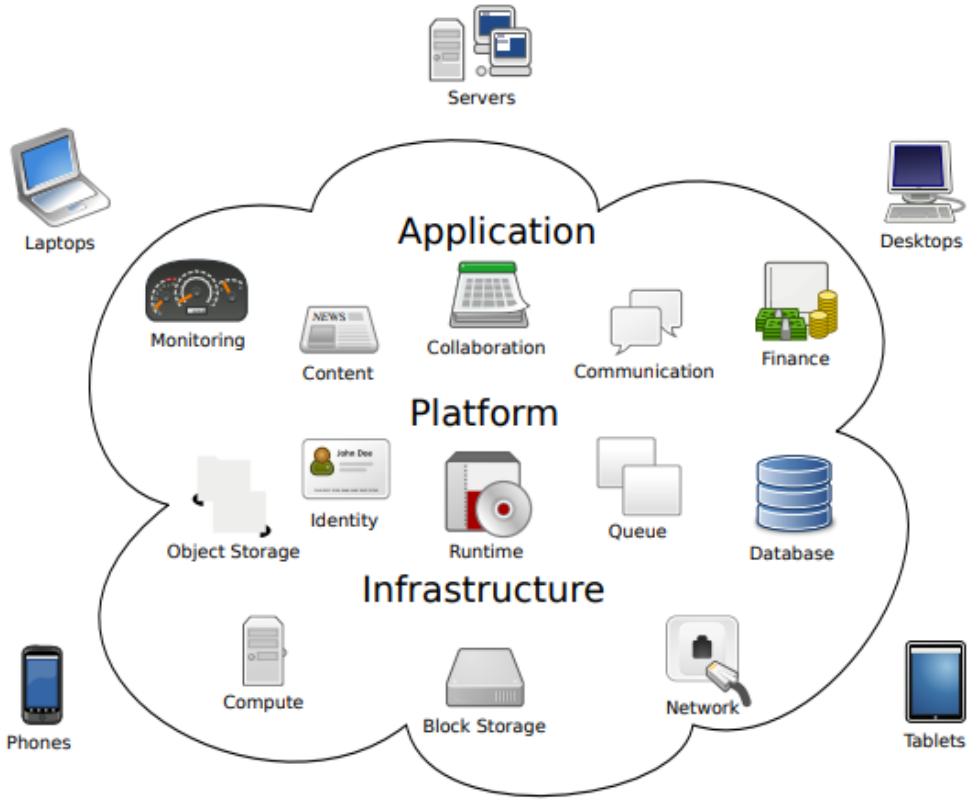
Računarstvo u oblaku može biti javno i privatno. Javni servisi u oblaku pružaju svoje usluge putem Interneta uz naknadu. Privatni cloud servisi, s druge strane, pružaju usluge samo određenom broju ljudi. Ove usluge su sistem mreža koje pružaju hostirane usluge. Postoji i hibridna opcija, koja kombinuje elemente javnih i privatnih usluga. Privatno ili javno, cilj računarstva u oblaku je da obezbijedi lak, skalabilan pristup računarskim resursima i IT uslugama.

Cloud computing je opći pojam za sve što uključuje isporuku hostiranih usluga putem Interneta. Ove usluge su podijeljene u tri glavne kategorije ili vrste računarstva u oblaku: infrastruktura kao usluga (IaaS), platforma kao usluga (PaaS) i softver kao usluga (SaaS).

Cloud infrastruktura uključuje hardverske i softverske komponente potrebne za pravilnu implementaciju modela računarstva u oblaku. Računarstvo u oblaku se također može smatrati pomoćnim računarstvom ili računarstvom na zahtjev. Poput Interneta, Cloud computing podrazumijeva tehnološki razvoj koji traje već neko vrijeme i nastaviti će se razvijati. Za razliku od weba, računarstvo u oblaku je još uvijek u relativno ranoj fazi. Danas se sve više nastoji omogućiti i olakšati brže usvajanje Cloud computinga u svim sektorima privrede što može smanjiti troškove informaciono-komunikacijske tehnologije i može povećati produktivnost, rast i radna mjesta.

Računarstvo u oblaku funkcioniše tako što omogućava klijentskim uređajima da pristupe podacima i aplikacijama u oblaku preko Interneta sa udaljenih fizičkih servera, baza podataka i računara. Internetska mrežna veza povezuje prednji kraj, koji uključuje pristup klijentskom uređaju, pretraživaču, mreži i softverskim aplikacijama u oblaku, sa back end, koji se sastoji od baza podataka, servera i računara. Pozadinska strana funkcioniše kao spremište, pohranjujući podatke kojima pristupa prednji kraj.

Slika 1. Cloud computing



Izvor: (Balwinder, 2017)

Tabela 1. Odnos tradicionalnog računarstva i računarstva u oblaku

TRADICIONALNI COMPUTING	CLOUD COMPUTING
File Serveri	Google docs, Dropbox
MS Outlook, Apple mail	Gmail, Yahoo!, MSN
SAP CRM / Oracle CRM / Siebel	SalesForce.Com
Quicken / Oracle Financials	Intacct / NetSuite
Microsoft Office / Lotus Notes	Google Apps
Stellent	Valtira
Off – site backup	Amazon S3
Server, racks i firewall	Amazon EC2m GoGrid, Mosso

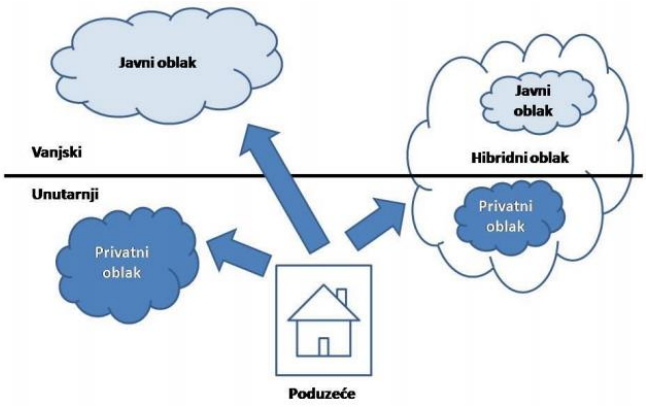
Izvor: (Chen, et.al., 2013)

Prema Ambrust, *et.al.* (2009), računarstvo u oblaku nije nova ideja, ali je evolucija neke stare paradigme za distribuirano računarstvo. Pojava entuzijazma za računarstvo u oblaku je rezultat nedavnog tehnološkog trenda i poslovnih modela.

2.2. Modeli implementacije Cloud computinga

Ogrizek, Biškupić i Banek (2014), navode četiri modela implementacije računarstva u oblaku, a to su: privatni oblak (engl. Private Cloud), javni oblak (engl. Public Cloud), hibridni oblak (engl. Hybrid Cloud), oblak zajednice (engl. Community Cloud).

Slika 2. Modeli implemntacije Cloud computinga



Izvor: (Ogrizek, Biškupić, Banek, 2014)

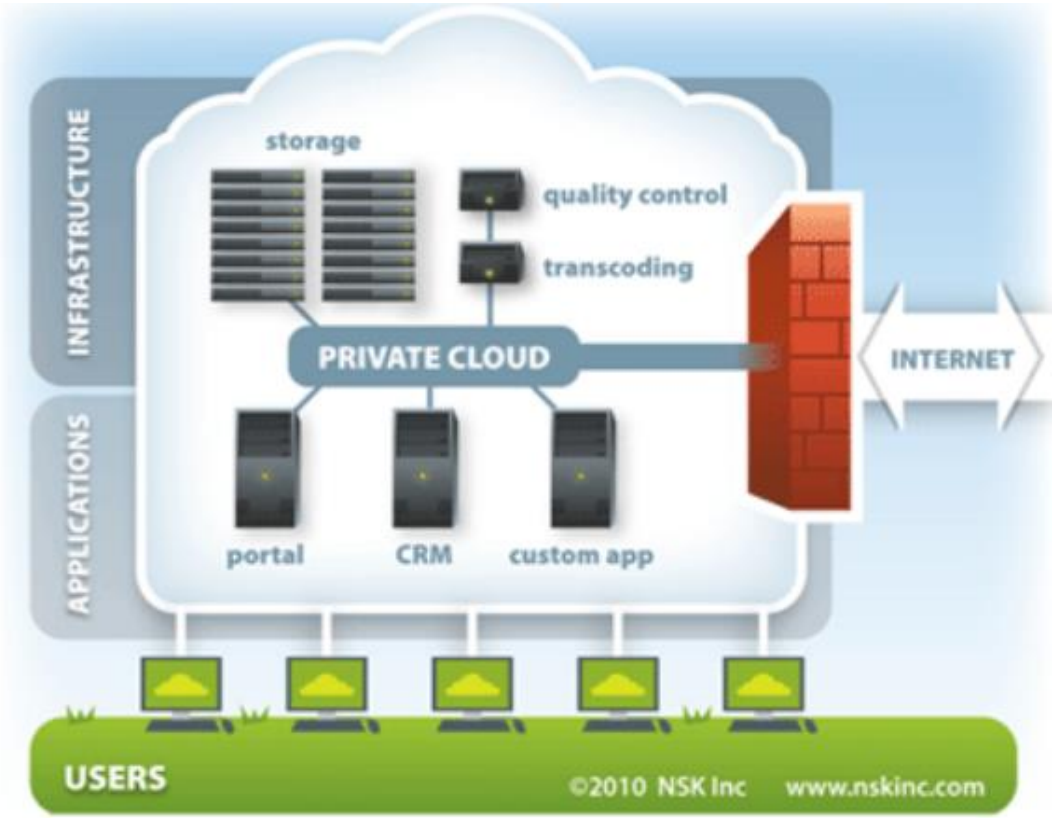
2.2.1. Privatni Cloud

Privatni Cloud održava se unutar organizacije i koristi isključivo za svoju unutrašnju svrhu. Mnoga preduzeća kreću u pravcu ove postavke i stručnjaci smatraju da je ovo prvi korak kada organizacija prelazi u oblak. Sigurnost, propusnost mreže nisu kritični problemi za privatni oblak. Ovaj se oblak sastoji od hostinga privatnih aplikacija, pohrane. U privatnom oblaku, računarske usluge se nude preko privatne IT mreže za namjensku upotrebu jedne

organizacije. Također nazvan interni, poslovni ili korporativni oblak, privatnim oblakom se obično upravlja putem internih resursa i nije dostupan nikome izvan organizacije. Privatno računarstvo u oblaku pruža sve prednosti javnog oblaka, kao što su samoposluživanje, skalabilnost i elastičnost, zajedno sa dodatnom kontrolom, sigurnošću i prilagođavanjem.

Privatni oblaci pružaju viši nivo sigurnosti putem zaštitnih zidova kompanije i internog hostinga kako bi se osiguralo da osjetljivi podaci organizacije nisu dostupni dobavljačima trećih strana. Nedostatak privatnog oblaka je, međutim, u tome što organizacija postaje odgovorna za cjelokupno upravljanje i održavanje podatkovnih centara, što se može pokazati kao prilično zahtjevno za resurse. Privatni oblak (eng. Private Cloud), kao što i sam naziv kaže, oblikovan je iz postojeće IT infrastrukture računarskog centra te služi organizaciji unutar vlastitog poslovnog vatrozida (Brumec, 2011). Ovakva vrsta oblaka se obično implementira u samom centru organizacije a njime upravljaju zaposleni (administratori). Privatni Cloud uobičajeno sadrži sve resurse kompanije kao što su npr. podaci o transakcijama ili podaci o klijentima. Na ovaj način kompanija otklanja mnoga sigurnosna i pravna pitanja o kojima bi morala voditi računa kada bi pohranjivanje svojih resursa povjerila trećoj strani.

Slika 3. Prikaz Privatnog Clouda



Izvor:https://info.focustsi.com/it-services-boston/resources/blog/cloud-computing-101-public-vs-private-clouds (pristupljeno: 10.05.2023. godine)

2.2.2. Javni Cloud

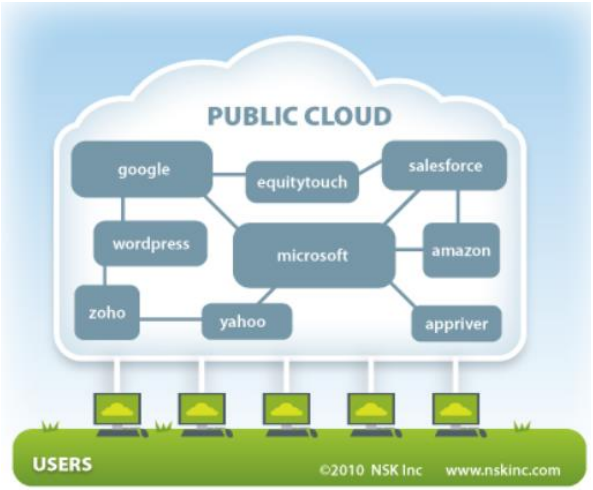
Javni Cloud iznajmljuje cloud usluge pružatelja na zahtjev. Bitno je istaći da se usluge pružaju korisnicima pomoću modela uslužnog računarstva. Javni oblak poznat je i kao vanjski oblak. Dakle, u oblaku su podaci mnogih korisnika, ali se naravno ne može pristupiti informacijama drugih. Javni oblak je Cloud computing platforma koja je dostupna svima, neovisno radi li se o pojedincu ili organizaciji. Javni oblak je u vlasništvu kompanije koja prodaje cloud uslugu. Aplikacije koje korisnici koriste često se nalaze na istim poslužiteljima. Oni čine privremeno zakupljenu infrastrukturu organizacija (Nicoletti, 2013). Ovaj oblak je još nazvan i potrošački oblak gdje korisnici putem Interneta, preko poslužitelja koriste računarske resurse, uslužne aplikacije, resurse poput društvenih mreža, blogova, e-pošte, pohrane podataka ili slika itd.

Javni oblak se odnosi na računarske usluge koje nude provajderi trećih strana preko Interneta. Za razliku od privatnog oblaka, usluge u javnom oblaku dostupne su svima koji ih žele koristiti ili kupiti. Javni oblaci mogu pomoći preduzećima da uštede na kupovini, upravljanju i održavanju lokalne infrastrukture jer je dobavljač usluga u oblaku odgovoran za upravljanje sistemom. Oni također nude skalabilnu RAM memoriju i fleksibilnu propusnost, što olakšava preduzećima da skaliraju svoje potrebe za skladištenjem.

Jedna od prednosti javnog oblaka je to što oni mogu biti puno veći nego što su privatni oblaci. Na taj način Javni Cloud nudi mogućnost povećavanja ili smanjivanja zakupljenog dijela oblaka i prebacivanja odgovornosti i to u slučaju da se pojave nenadani rizici. Kada se govori o dijelovima Javnog Clouda, oni mogu biti pod upotrebom samo jednog korisnika te na taj način stvaraju privatni podatkovni centar (datacentar). Javni Cloud je višeupotrebna infrastruktura i da bi je koristio, korisnik treba da, prije svega, sklopi ugovor sa pružateljem usluge o samom nivou usluge te da se utvrde prava i obaveze sa obje strane. Tek poslije sklapanja ugovora, moguće je koristiti resurse oblaka.

Plaćanje same usluge je na bazi “plati koliko potrošiš”. Kao primjeri Javnog Clouda mogu se navesti Amazon Elastic Compute Cloud, Sun Cloud, Google AppEngine. Danas postoji mnogo servisa koje koristimo u svakodnevnom životu, kao što su Facebook, Twitter, Gmail, Google Docs, Windows Live, Dropbox itd. Sigurnost i upravljanje podacima predstavljaju najvažniji problem ovog modela.

Slika 4. Prikaz Javnog Clouda



Izvor:https://info.focustsi.com/it-services-boston/resources/blog/cloud-computing-101-public-vs-private-clouds (pristupljeno: 10.05.2023. godine)

Tabela 2. Razlike između Javnog i Privatnog Clouda

	Javni Cloud	**Privatni Cloud**
Infrastruktura i vlasništvo	izvan institucije – usluga poslužitelja	unutar institucije
Skalabilnost	neograničeno na zahtjev	ograničena oprema instaliranoj infrastrukturi
Kontrola i menadžment	manipuliše se samo virtualnim uređajima, što zahtijeva malo opterećenje	visok stepen kontrole nad izvorima, zahtijeva više stručnosti za upravljanje
Troškovi	niski	visoki: uključuju i prostor, hlađenje, potrošnju električne energije i hardver
Izvedba	nepredvidivo okruženje koje teže garantuje uspješnosti	zagarantovana uspješnost
Sigurnosti	upitnost očuvanja privatnosti podataka	iznimno sigurno

Izvor: Autor rada

2.2.3. Hibridni Cloud

Hibridni Cloud sastoji se od više unutrašnjih ili vanjskih oblaka. To je scenarij kada se organizacija kreće u javni oblak računarstva iz domene unutrašnjeg privatnog oblaka. To je kombinacija javnog i privatnog oblaka. Organizacija može imati dio usluge u vlastitoj infrastrukturi, ali i u javnom oblaku. Dobra je opcija kada želimo imati svoje podatke ili aplikacije na lokalnom nivou i ne želimo previše ulagati u infrastrukturu (Bhaskar, Choi, Lumb, 2009). Hibridni oblak (eng. Hybrid Cloud) podrazumijeva kombinaciju privatnog i javnog oblaka uzimajući najbolje od oba. Privatni oblak zadržava veliki stepen funkcionalnosti te se povezuje sa javnim oblakom za potrebe velikog radnog opterećenja ili poteškoća sa hardverom.

U modelu hibridnog oblaka, kompanije plaćaju samo za resurse koje koriste privremeno umjesto kupovine i održavanja resursa koji se možda neće koristiti tokom dužeg perioda. Ukratko, hibridni oblak nudi prednosti javnog oblaka bez sigurnosnih rizika. U Hibridnom Cloudu najčešće se radi na način da preduzeće zadržava važne podatke i aplikacije unutar vlastitog vatrozida dok one manje važne pohranjuje na javni oblak. Hibridni oblak može biti jako koristan u situacijama kada kompanija želi koristiti nekakav vanjski softver ali je brine sigurnost sistema. Jedna od prednosti je da kompanija može osigurati javni oblak za svoje klijente dok na vlastitom privatnom drži svoj informacioni sistem.

Slika 5. Prikaz Hibridnog Clouda

Izvor: https://www.stablenet.net/solutions/cloud-computing/hybrid-cloud/ (pristupljeno: 10.05.2023. godine)

2.3. Ključne karakteristike Cloud computinga

Postoji nekoliko ključnih karakteristika Cloud computinga. Ponude usluga najčešće se stavljaju na raspolaganje specifičnim potrošačima i malim preduzećima koji vide korist od toga što im je kapitalni izdatak minimiziran. Ovo služi za smanjenje prepreka ulasku na tržište, budući da je infrastruktura korištena za pružanje tih ponuda u vlasništvu pružatelja usluga oblaka i ne moraju je kupiti. Kako korisnici nisu vezani za određeni uređaj (potreban im je samo pristup internetskoj mreži) i kako Internet omogućava neovisnost lokacije, korištenje clouda omogućava kupcima pružatelja usluga računarstva u oblaku pristup sistemima koji omogućava cloud bez obzira na to gdje se nalaze i omogućava dijeljenje resursa i troškova među velikim brojem korisnika (Farber, 2010).

Performanse se veoma često poboljšavaju u okruženjima računarstva u oblaku jer pružatelji usluga koriste više redudantnih mjesta. Ovo je privlačno za preduzeća zbog kontinuiteta poslovanja i obnove od katastrofe. Međutim, nedostatak je što IT menadžeri mogu učiniti vrlo malo kada dođe do prekida rada.

Još jedna prednost koja cloud usluge čini pouzdanijima je ta što se skalabilnost može dinamički razlikovati na temelju promjenjivih potreba korisnika. Budući da provajder servisa upravlja potrebnom infrastrukturom, sigurnost se poboljšava. Kao rezultat centralizacije podataka, povećava se usredotočenost na zaštitu korisničkih resursa koje održava pružatelj usluga. Kako bi osigurali da su njihovi podaci sigurni, pružatelji usluga oblaka brzo ulažu u posvećeno sigurnosno osoblje. To se uglavnom smatra korisnim, ali također je izražena zabrinutost zbog gubitka kontrole korisnika nad osjetljivim podacima.

Za razliku od tradicionalnog pristupa, poslovanje koje se temelji na korištenju usluga zasnovanih na računarstvu u oblaku uvodi modele korištenja resursa koji nisu u vlasništvu kompanije (Tomac, 2013). Sirća i Spremić (2000), navode da se najveće razlike između tradicionalnog pristupa IT infrastrukture i računarstva u oblaku temelje kroz sljedeće karakteristike:

- Isporuka usluga na zahtjev - Usluge Cloud computing često se isporučuju po modelu samoposluživanja, odnosno uz minimalnu interakciju sa isporučiteljem usluge. Bitno je istaći da je korisnicima olakšano korištenje resursa gdje ih mogu svojevoljno uključivati ili isključivati, prema potrebi.
- Brza elastičnost - Ova karakteristika omogućava krajnjim korisnicima da brzo, jednostavno i efikasno optimiziraju resurse koji su im potrebni uz ekonomično plaćanje koje se temelji na principu «plati koliko koristiš».
- Mjerena usluga - Sistemi koji koriste Cloud computing usluge automatski provjeravaju stepen iskorištenosti resursa, tako što se mjeri sposobnost apstrakcije pogodne za potreban tip usluge. Korištenje resursa se prati, provjerava i o tome se prave izvještaji, što omogućava transparentan uvid o pružateljima usluga i korisnicima.

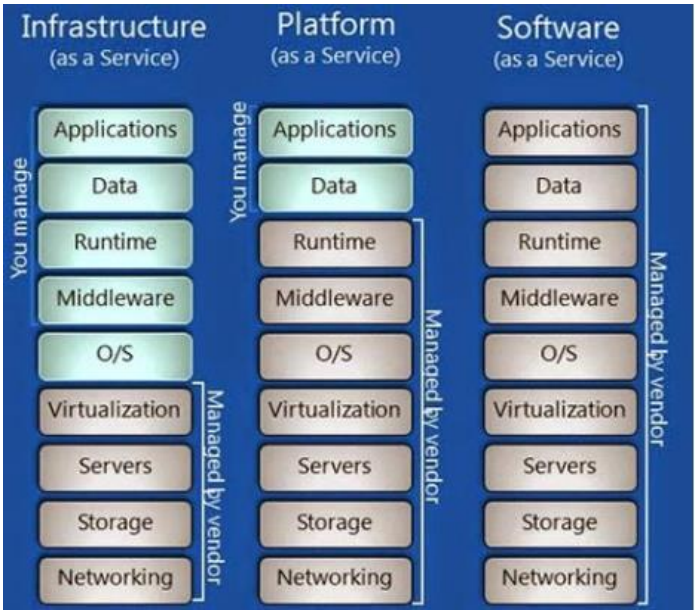
Konačno, računarstvo u oblaku vjerovatno će donijeti mase superračunanja. Yahoo, Google, Microsoft, IBM i drugi uključeni su u stvaranje mrežnih usluga kako bi svojim korisnicima omogućili čak i bolji pristup podacima u svakodnevnom životu kao što su zdravstvena zaštita, finansiranje, osiguranje, itd. (King, 2010).

2.4. Modeli pružanja usluge

Cloud Computing odnosi se i na aplikacije koje se isporučuju kao usluge putem Interneta kao i na hardverski i sistemski softver u podatkovnim centrima koji pružaju te usluge. Arhitektura Cloud computinga može se kategorizovati prema tri vrste modela isporuke usluge, a to su:

- Infrastruktura kao usluga (IaaS)
- Softver kao usluga (SaaS)
- Platforma kao usluga (PaaS)

Slika 6. Prikaz odgovornosti modela



Izvor: http://opensourceforgeeks.blogspot.com/2015/01/difference-between-saas-paas-and-iaas.html *(pristupljeno: 10.06.2023. godine)*

2.4.1. Infrastruktura kao usluga (IaaS)

Infrastruktura kao usluga ili IaaS je vrsta računarstva u oblaku u kojoj je provajder usluga odgovoran za obezbjeđivanje servera, skladištenja i umrežavanja preko virtualnog interfejsa. U ovoj usluzi korisnik ne treba da upravlja infrastrukturom oblaka, ali ima kontrolu nad skladištem, operativnim sistemima i implementiranim aplikacijama. Umjesto korisnika, dobavljač treće strane „ugošćuje“ hardver, softver, servere, skladište i druge komponente infrastrukture. Dobavljač također hostuje korisničke aplikacije i održava rezervnu kopiju. IaaS može imati mnoge prednosti za organizacije, kao što je potencijalno brža, lakša, fleksibilnija i isplativija radna opterećenja.

Najčešći slučajevi upotrebe za IaaS implementacije uključuju sljedeće:

- Okruženja za testiranje i razvoj - IaaS organizacijama nudi fleksibilnost kada su u pitanju različita testna i razvojna okruženja. Mogu se lako povećati ili smanjiti prema potrebama.
- Hosting web stranica namijenjenih korisnicima - To može učiniti hostiranje web stranice pristupačnijim u poređenju s tradicionalnim načinima hostinga web stranica.
- Pohrana podataka, backup i oporavak - IaaS može biti najlakši i najučinkovitiji način za organizacije da upravljaju podacima kada je potražnja nepredvidljiva ili se može stalno povećavati. Nadalje, organizacije mogu zaobići potrebu za obimnim naporima usmjerenim na upravljanje, zakonske zahtjeve i zahtjeve usklađenosti pohrane podataka.

- Web aplikacije - Infrastrukturu potrebnu za hostiranje web aplikacija osigurava IaaS. Stoga, ako organizacija hostira web aplikaciju, IaaS može osigurati potrebne resurse za pohranu, poslužitelje i umrežavanje. Implementacije se mogu izvršiti brzo, a infrastruktura oblaka može se lako povećati ili smanjiti prema zahtjevima aplikacije.
- Računarstvo visokih performansi (HPC) - Određena radna opterećenja mogu zahtijevati računarstvo na nivou HPC-a, kao što su naučna izračunavanja, finansijsko modeliranje i dizajn proizvoda.
- Skladištenje podataka i analitika velikih podataka - IaaS može pružiti potrebnu računarsku i procesorsku snagu za pročešljavanje velikih skupova podataka (Moreno, et al., 2013).

Organizacije biraju IaaS jer je često lakše, brže i isplativije upravljati radnim opterećenjem bez potrebe za kupovinom, upravljanjem i podrškom temeljne infrastrukture. Uz IaaS, preduzeće može jednostavno unajmiti ili iznajmiti tu infrastrukturu od drugog preduzeća.

Općenito, IaaS korisnici plaćaju po korištenju, obično po satu, sedmici ili mjesecu. Neki IaaS pružatelji također naplaćuju korisnicima na temelju količine prostora virtualnog stroja koji koriste. Ovaj pay-as-you-go model eliminiše kapitalne troškove postavljanja internog hardvera i softvera. Kada preduzeće ne može koristiti pružatelje usluga treće strane, privatni oblak izgrađen u prostorijama i dalje može ponuditi kontrolu i skalabilnost IaaS-a - iako se isplativost troškova više ne primjenjuje. Uprkos svom fleksibilnom, pay-as-you-go modelu, IaaS naplata može biti problem za neka preduzeća. Naplata u oblaku posebno je granularna i raščlanjena kako bi odražavala preciznu upotrebu usluga. Uobičajeno je da korisnici dožive šok od naljepnica - ili otkriju da su troškovi veći od očekivanih - kada pregledaju račune za svaki resurs i uslugu uključenu u implementaciju aplikacije. Korisnici bi trebali pažljivo pratiti svoja IaaS okruženja i račune kako bi razumjeli kako se IaaS koristi i kako bi izbjegli naplatu neovlaštenih usluga.

Budući da IaaS pružatelji usluga posjeduju infrastrukturu, detalji o konfiguraciji njihove infrastrukture i izvedbi rijetko su transparentni IaaS korisnicima. Ovaj nedostatak transparentnosti može korisnicima otežati upravljanje i nadzor sistema (Clark, 2005).

Korisnici IaaS-a također su zabrinuti zbog otpornosti usluge. Dostupnost i performanse radnog opterećenja značajno ovise od pružatelja usluga. Ako pružatelj usluge IaaS doživi mrežna uska grla ili bilo koji oblik internog ili vanjskog prekida rada, to će uticati na radna opterećenja korisnika. Osim toga, budući da je IaaS arhitektura s više „stanara“, problem „bučnog susjeda“ može negativno uticati na radna opterećenja korisnika (Clark, 2005).

Kada se želi implementirati IaaS proizvod, potrebno je uzeti u obzir važna pitanja. Slučajevi upotrebe IaaS-a i potrebe za infrastrukturom trebaju biti strogo definisani prije nego što se razmotre različiti tehnički zahtjevi i pružatelji usluga. Tehničke potrebe i potrebe za pohranom koje treba razmotriti za implementaciju IaaS-a uključuju:

- Umrežavanje - Kada se fokusiraju na implementaciju oblaka, organizacije moraju postaviti određena pitanja kako bi osigurale da se osiguranoj infrastrukturi u oblaku može pristupiti na učinkovit način.
- Skladištenje - Organizacije bi trebale razmotriti zahtjeve za tipove pohrane, potrebne nivoe performansi pohrane, mogući potreban prostor, opskrbu i potencijalne opcije kao što je pohrana objekata.
- Sigurnost - Sigurnost podataka trebala bi biti od najveće važnosti pri ocjenjivanju usluga i pružatelja usluga u oblaku. Pitanjima o enkripciji podataka, certifikatima, usklađenosti i regulativi te sigurnim radnim opterećenjima trebalo bi se detaljno pozabaviti.
- Oporavak od katastrofe - Specifičnosti i opcije oporavka od katastrofe još su jedno ključno područje vrijednosti za organizacije u slučaju prestanka rada na nivou VM-a, poslužitelja ili web-mjesta.
- Veličina poslužitelja - Opcije za veličine servera i VM-a, koliko CPU-a može biti postavljeno na poslužitelje i druge pojedinosti o CPU-u i memoriji.
- Propusnost mreže - Brzina između VM-ova, podatkovnih centara, pohrane i Interneta (Radić, 2011).

2.4.2. Platforma kao usluga (PaaS)

Platforma kao usluga ili PaaS je vrsta računarstva u oblaku koja pruža okruženje za razvoj i implementaciju u oblaku koje omogućava korisnicima da razvijaju i pokreću aplikacije bez složenosti izgradnje ili održavanja infrastrukture. Korisnicima pruža resurse za razvoj aplikacija zasnovanih na oblaku. U ovoj vrsti usluge, korisnik kupuje resurse od dobavljača po principu pay-as-you-go i može im pristupiti preko sigurne veze. PaaS ne zahtijeva od korisnika da upravljaju osnovnom infrastrukturom, tj. mrežom, serverima, operativnim sistemima ili pohranom, ali im daje kontrolu nad implementiranim aplikacijama. Ovo omogućava organizacijama da se fokusiraju na implementaciju i upravljanje svojim aplikacijama oslobađajući ih odgovornosti za održavanje softvera, planiranje i nabavku resursa.

Jedna od osnovnih prednosti platforme kao usluge je ekonomičnost, jer se plaćaju samo resursi koji se koriste. Kao još jedna prednost ove usluge može se navesti brz vremenski period pokretanja softvera ili aplikacije, gdje se korisnik ne mora baviti optimizacijom resursa i održavanjem platforme, već se njima bavi pružatelj usluge. Na taj način se skraćuje vrijeme potrebno za pokretanje aplikacije u klasičnoj IT infrastrukturi koje ovisi od brzine IT tehničara i njegove dostupnosti te količine resursa sa kojom on raspolaže. Sa druge strane, ovaj tip usluge ima i određene nedostatke kao što su: brzina, čija prednost ne mora uvijek biti izražena u brzini virtualnih poslužitelja i hardvera, već ovisi i od brzine mreže što može biti izraženije u ovisnosti od lokacije sa koje se pristupa usluzi. Drugi nedostatak se vezuje za zakon o pohrani podataka, jer različite zemlje imaju različite zakone koji se tiču lokacije fizičke pohrane podataka.

Neki od primjera ovog modela su: Google – AppEngine, Amazon Web Service – Elastic Beanstalk, Microsoft – Windows Azure, VMWare Cloud Foundry, Salesforce – AppForce (Radić, 2011).

2.4.3. Softver kao usluga (SaaS)

Softver kao usluga (SaaS) je model koji se koristi za isporuku aplikacija preko Interneta kao jedna usluga. Jedna od velikih prednosti SaaS modela prema korisnicima je ta što ne zahtijeva nikakvu kupovinu softvera, hardvera, bilo kakvu instalaciju, održavanje ili nadogradnju. Korištenje aplikacije je veoma jednostavno, a potrebna je samo Internet konekcija. Softver kao usluga (SaaS) predstavlja najpoznatiji model Cloud computinga, jer većina populacije koristi takav tip usluge svakodnevno. Najpoznatiji primjer SaaS nudi informaciona kompanija Google pod nazivom Google Apps. Asortiman Googe Apps paketa se sastoji od: Google Docs, Gmail, Calendar, Google Drive, Docs i sl.

SaaS ili softver kao usluga omogućava korisnicima pristup softveru dobavljača u oblaku na osnovu pretplate. U ovoj vrsti Cloud computinga, korisnici ne moraju instalisati ili preuzimati aplikacije na svojim lokalnim uređajima. Umjesto toga, aplikacije se nalaze na udaljenoj mreži u oblaku kojoj se može direktno pristupiti putem weba ili API-ja. U SaaS modelu, dobavljač usluga upravlja hardverom, aplikativnim softverom i sigurnošću.

Bitno je istaći da ovaj model veoma pojednostavljuje način rada za krajnjeg korisnika. Također, svi podaci se čuvaju u cloudu što rješava problem čuvanja podataka na posebnim diskovima velikih kapaciteta. Što se tiče plaćanja, korisnik ima mogućnost mjesečnog najma licenci prema potrebi, u čiju cijenu se uključuje i održavanje aplikacijskog softvera.

2.5. Prednosti i nedostaci Cloud computinga

Jedna od najvećih prednosti Cloud computinga je korištenje po potrebi. Također, najam opreme i resursa na pretplatu ili na duži vremenski period posebno je pogodan kod malih preduzeća koja tek započinju svoje poslovanje jer tako mogu izbjeći nabavu skupe opreme za obavljanje određenih poslova. Sa druge strane, neki od nedostataka Cloud computinga su nedostupnost i nesigurnost. Poslovanje korisnika vođeno na uslugama koje su smještene na tuđoj infrastrukturi može izazvati probleme ukoliko dođe do nekakvih poteškoća kod davatelja usluga. Upravo zbog ovoga potrebno je uspostaviti jedan odnos od povjerenja između korisnika i davatelja usluge.

Aymerich, Fenu i Surcis, (2008), definiraju niz prednosti Cloud computing kao što su:

- hardver (računari, uređaji za pohranu) je u vlasništvu pružatelja računarskih usluga u oblaku, a ne u vlasništvu korisnika koji s njim komunicira putem Interneta
- upotreba hardvera dinamički se optimizira u mreži računara

- pružatelji usluga oblaka često premještaju radna opterećenja svojih korisnika (npr. s jednog računara na drugi ili iz jednog podatkovnog centra u drugi)
- daljinski hardver pohranjuje i obrađuje podatke i čini ih dostupnima, npr. kroz aplikacije (kako bi kompanija mogla koristiti računarstvo utemeljeno na oblaku u potpuno istim uslovima na način na koji potrošači već danas koriste svoje račune putem web pošte)
- organizacije i pojedinci mogu pristupiti svom sadržaju i koristiti svoj softver kada i gdje im treba, npr. na stolnim računarima, prenosnim računarima, tabletima i pametnim telefonima
- postavljanje oblaka sastoji se od slojeva: hardvera, srednjeg softvera ili platforme i aplikacije softvera; standardizacija je važna posebno na srednjem sloju jer se omogućava programerima da se obraćaju širokom krugu potencijalnih kupaca i pružaju korisnicima izbor
- korisnici obično plaćaju korištenje, izbjegavajući velike unaprijed i fiksne troškove koji su potrebni za upravljanje sofisticiranom računarskom opremom
- istovremeno korisnici mogu vrlo lako izmijeniti količinu hardvera koji koriste (npr. donijeti novi kapacitet pohrane na mreži u nekoliko sekundi s nekoliko klikova mišem).

Aymerich, Fenu i Surcis, (2008), navode da prednosti upotrebe Cloud usluga mogu biti tehničke, arhitektonske, poslovne, itd.

Sa stanovišta dobavljača:

- Većina podatkovnih centara danas se ne koristi. Ovim podatkovnim centrima su potrebni rezervni kapaciteti. Velike kompanije, ako imaju te podatkovne centre, mogu lako iznajmiti računarske snage drugima organizacijama, te iz toga ostvariti profit, a također imaju sve potrebne resurse za pravilno funkcionisanje podatkovnog centra (poput snage).
- Kompanije koje imaju velike centre podataka već su iskoristile resurse, a za pružanje usluga u oblaku trebat će im vrlo malo ulaganja.

Sa stanoviša korisnika oblaka:

- Korisnici oblaka ne trebaju brinuti o hardveru i softveru koji koriste, odnosno ne moraju brinuti oko održavanja. Korisnici više nisu vezani za jedan tradicionalni sistem.
- Tehnologija virtualizacije
- Korisnici oblaka mogu resurse koristiti na zahtjev i platiti koliko ih koriste. Tako korisnici mogu dobro planirati smanjenje upotrebe kako bi sveli izdatke na najmanju moguću mjeru.
- Skalabilnost je jedna od glavnih prednosti korisnika oblaka. Korisnici dobijaju onoliko resursa koliko imaju potreba (Aymerich, Fenu, Surcis, 2008).

3. SIGURNOSNI ASPEKTI CLOUD COMPUTINGA

3.1. Sigurnost Cloud computinga

U društvu danas postoji zabrinutost oko sigurnosti računarstva u oblaku. Jedan od rizika koji ljudi vide jest da pružatelji usluga moraju upravljati potencijalno milionima kupaca, a to predstavlja izazov (Ohlman, Eriksson i Rembarz, 2009). Ovo pokazuje da su mnogi ljudi zabrinuti da se pružatelji usluga u oblaku neće moći nositi s velikim obimom ili da se infrastruktura neće moći ispravno skalirati s velikim količinama korištenja. Privatnost je važna za organizacije, posebno kada se pohranjuju lični podaci pojedinca ili osjetljivi podaci, ali još nije potpuno jasno hoće li infrastruktura računarstva u oblaku moći podržati pohranjivanje osjetljivih podataka, a da organizacije ne budu izložene riziku od kršenja propisa privatnosti.

Šifriranje nije uvijek potpuni dokaz za zaštitu podataka, ponekad se mogu pojaviti mali problemi i podaci se ne mogu dešifrovati, ostavljajući podatke oštećenima i neupotrebljivima za korisnike i pružatelja usluga u oblaku. Resursi oblaka također se mogu zloupotrijebiti jer pružatelji usluga oblaka ponovno dodjeljuju IP adrese kada korisnik više ne treba IP adresu. Nakon što IP adresa više nije potrebna jednom korisniku nakon određenog vremena, postaje dostupna drugom korisniku za korištenje. Pružatelji usluga oblaka štede novac i ne trebaju toliko IP adresa ako ih ponovo koriste, stoga im je u interesu da to i čine. Previše ovih neaktivnih/korištenih IP adresa može ostaviti pružatelja usluga oblaka otvorenim za zloupotrebu njegovih resursa.

Većina korisnika neće znati gdje pružatelj usluga oblaka pohranjuje njihove podatke. Ovo stvara niz problema, posebno ako su informacije važne ili vrijedne. Korisnici koji su zabrinuti za sigurnost trebali bi pitati svog pružatelja usluga u oblaku gdje se drže fizički poslužitelji, koliko često se održavaju i koje su vrste fizičkih sigurnosnih mjera poduzete (npr. biometrijski ili PIN pristup) da bi se ograničio pristup resursima poslužitelja. Postoji mogućnost da će se podaci čuvati u drugoj zemlji, što znači da bi lokalni zakon i nadležnost bili drugačiji i mogli bi stvoriti drugačiji sigurnosni rizik, jer podaci koji bi mogli biti sigurni u jednoj zemlji možda nisu sigurni u drugoj (Staten, 2009). Posmatrajući različite poglede na privatnost podataka između SAD-a i EU-a, ovaj sigurnosni rizik postaje očitiji budući da SAD ima vrlo otvoren pogled na privatnost podataka. Američki Patriot Act daje vladi i drugim agencijama gotovo neograničene ovlasti za pristup informacijama uključujući one koje pripadaju kompanijama, dok bi u EU ova vrsta podataka bila mnogo sigurnija, tako da lokalni zakoni i nadležnost mogu imati veliki uticaj na sigurnost i privatnost podataka unutar oblaka (Mikkilineni i Sarathy, 2009).

Za oblak se vezuje niz sigurnosnih problema, koji uglavnom ovise od izbora pružatelja usluga i modela implementacije. Tako npr. privatni oblak garantuje sigurnost do određenog nivoa, ali ekonomski troškovi ovog modela nisu uopće zanemarljivi. Mikkilineni i Sarathy

(2009) ističu niz problema: manjak sigurnosti, neadekvatno brisanje podataka, neovlašteni pristup, ranjivosti sigurnosnih kopija, nedovoljno povjerenje i transparentnost.

3.1.1. Manjak sigurnosti

Računarstvo u oblaku sa sobom donosi i mnoge jedinstvene sigurnosne probleme i izazove. U oblaku se podaci pohranjuju kod dobavljača treće strane i pristupa im se putem Interneta. To znači da je vidljivost i kontrola nad tim podacima ograničena. Također se postavlja pitanje kako se podaci mogu pravilno osigurati. Imperativ je da svatko razumije svoju ulogu i sigurnosna pitanja svojstvena računarstvu u oblaku. Pružatelji usluga u oblaku tretiraju sigurnosna pitanja i rizike u oblaku kao zajedničku odgovornost.

U ovom modelu pružatelj usluga u oblaku pokriva sigurnost samog oblaka, a korisnik pokriva sigurnost onoga što u njega stavlja. U svakoj usluzi u oblaku – od softvera kao usluge (SaaS) kao što je Microsoft 365 do infrastrukture kao usluge (IaaS) kao što je Amazon Web Services (AWS) – korisnik računarstva u oblaku uvijek je odgovoran za zaštitu svojih podataka od sigurnosnih prijetnji i kontrolisanja pristupa njemu (Staten, 2009). Većina sigurnosnih rizika računarstva u oblaku povezana je sa sigurnošću podataka u oblaku. Bilo da se radi o nedostatku vidljivosti podataka, nemogućnosti kontrole podataka ili krađi podataka u oblaku, većina problema dolazi od podataka koje korisnici stavljaju u oblak.

Bitno je istaći da se sigurnosne kontrole za oblak ne razlikuju od kontrola koje se koriste za druga IT okruženja. Rizik ovisi od modela koji se koristi, pa je tako korisnik IaaS modela sam odgovoran za sigurnost i o njoj se brine, dok se kod SaaS modela sigurnost reguliše u ugovoru o uslugama. U IaaS i PaaS modelu, pružatelj usluga oblaka precizno definiše kakva se zaštita očekuje od korisnika. Sa druge strane, u SaaS modelu zaštita je obaveza i odgovornost pružatelja usluga oblaka, ali i korisnik treba kontrolisati pristup pomoću svojih vlastitih sistema, npr. uz pomoć lokalne aplikacije za kontrolu pristupa.

Navodi se deset najčešćih sigurnosnih problema u oblaku SaaS:

- nedostatak vidljivosti podataka koji se nalaze unutar aplikacija u oblaku
- krađa podataka iz aplikacije u oblaku od strane zlonamjernog aktera
- nepotpuna kontrola nad tim tko može pristupiti osjetljivim podacima
- nemogućnost praćenja podataka u prenosu do i iz aplikacija u oblaku
- aplikacije u oblaku koje se osiguravaju izvan IT vidljivosti (npr. IT u sjeni)
- nedostatak osoblja s vještinama upravljanja sigurnošću za aplikacije u oblaku
- nemogućnost sprečavanja zlonamjerne unutrašnje krađe ili zloupotrebe podataka
- napredne prijetnje i napadi na pružatelja aplikacija u oblaku
- nemogućnost procjene sigurnosti rada pružatelja aplikacije u oblaku
- nemogućnost održavanja usklađenosti s propisima (Rajaraman, 2014).

SaaS sigurnosni problemi u oblaku prirodno su usredotočeni na podatke i pristup jer većina modela zajedničke sigurnosne odgovornosti ostavlja to dvoje kao isključivu odgovornost za SaaS korisnike. Odgovornost je svake organizacije razumjeti koje podatke stavlja u oblak, tko im može pristupiti i koji su nivo zaštite primijenili (i pružatelj usluga oblaka).

Navodi se deset najčešćih sigurnosnih problema u oblaku IaaS:

- radna opterećenja u oblaku i računi koji se stvaraju izvan IT vidljivosti (npr. IT u sjeni)
- nepotpuna kontrola nad tim tko može pristupiti osjetljivim podacima
- krađa podataka smještenih u infrastrukturi oblaka od strane zlonamjernog aktera
- nedostatak osoblja s vještinama za osiguranje infrastrukture oblaka
- nedostatak uvida u podatke koji se nalaze u oblaku
- nemogućnost sprečavanja zlonamjerne unutrašnje krađe ili zloupotrebe podataka
- nedostatak dosljednih sigurnosnih kontrola nad okruženjima s više oblaka i lokalnim okruženjima
- napredne prijetnje i napadi na infrastrukturu oblaka
- nemogućnost praćenja ranjivosti sistema radnog opterećenja oblaka i aplikacija
- lateralno širenje napada s jednog opterećenja oblaka na drugo (Potdar, *et.al*., 2015).

Zaštita podataka ključna je u IaaS-u. Kako se odgovornost korisnika proteže na aplikacije, mrežni promet i operativne sisteme, uvode se dodatne prijetnje. Organizacije bi trebale razmotriti nedavnu evoluciju napada koji se protežu izvan podataka kao središta IaaS rizika. Zlonamjerni akteri provode neprijateljsko preuzimanje računarskih resursa za rudarenje kriptovalute i ponovo koriste te resurse kao vektor napada protiv drugih elemenata poslovne infrastrukture i trećih strana.

Potdar, *et.al*. (2015) navodi pet najčešćih sigurnosnih problema u privatnom oblaku:

- nedostatak dosljednih sigurnosnih kontrola koje obuhvataju tradicionalne poslužiteljske i virtualizovane privatne infrastrukture oblaka
- sve veća složenost infrastrukture zahtijeva više vremena/napora za implementaciju i održavanje
- nedostatak osoblja s vještinama za upravljanje sigurnošću za softverski definisan podatkovni centar (npr. virtualni računar, mreža, pohrana)
- nepotpuna vidljivost nad sigurnošću za softverski definisan podatkovni centar (npr. virtualni računar, mreža, pohrana)
- napredne prijetnje i napadi.

Važan faktor u procesu donošenja odluka o dodjeli resursa javnom naspram privatnog oblaka je fino podešena kontrola dostupna u okruženjima privatnog oblaka. U privatnim oblacima dodatni nivoi kontrole i dodatne zaštite mogu kompenzovati druga ograničenja

implementacije privatnog oblaka i mogu doprinijeti praktičnom prelazu s monolitnih podatkovnih centara temeljenih na poslužitelju.

3.1.2. Neovlašteni pristup

Za računarstvo u oblaku je važno obezbijediti adekvatnu kontrolu pristupa povjerljivim informacijama, kako bi se zaštitila njihova sigurnost. Neovlašten pristup je značajan problem, ako ne postoje odgovarajući sigurnosni mehanizmi. Neovlašteni pristup može biti od strane zaposlenih pružatelja usluga oblaka, hakera, korisnika istog servisa na zajedničkom serveru, a podaci nisu na odgovarajući način odvojeni u oblaku. S obzirom da se podaci mogu pohraniti u oblaku u dužem vremenskom razdoblju, povećava se i njihova vremenska izloženost.

Neovlašteni pristup je najveća prijetnja sigurnosti Clouda. Novi izvještaji o sigurnosti u oblaku pokazuju da 53% anketiranih organizacija vidi neovlašteni pristup kroz zloupotrebu zaposlenih i neodgovarajuće kontrole pristupa kao najveću prijetnju sigurnosti u oblaku. A 96% anketiranih organizacija ima neke ili sve svoje aplikacije u oblaku. Kao što izvještaj navodi, dobra vijest je da se kontrola pristupa može riješiti putem sigurnosnih rješenja u oblaku u kombinaciji s politikama upravljanja identitetom i pristupom (Ryan, 2013).

Preduzeća danas sve više traže podatke i aplikacije kojima se može pristupiti s bilo kojeg uređaja, bez obzira na platformu. Iako je teoretski moguće, sigurnost računarstva u oblaku suštinski je izazovna. Postavlja se pitanje šta kompanije mogu učiniti kako bi iskoristile prednosti računarstva u oblaku i istovremeno zaštitile svoje podatke. Identifikovanje problema prvi je korak u pronalaženju rješenja koje nam odgovara. Sljedeći korak je izbor pravih sigurnosnih proizvoda u oblaku i pružatelja usluga.

Prvi izazov su DDoS i DoS napadi. Kako se sve više preduzeća i funkcija seli u oblak, pružatelji usluga u oblaku postaju sve ranjiviji. Događa se sve veći broj DDoS napada. U prvom kvartalu 2021. najčešće ciljane industrije bile su platforme u oblaku (PaaS) i SaaS (Srnivasan, 2012). DDoS napadi imaju za cilj nadvladati poslužitelje web stranice kako bi osujetili legitimne zahtjeve korisnika. Ovisno od jačine DDoS napada, web stranica može biti nedostupna danima ili čak sedmicama. Kao rezultat toga, povjerenje kupaca i pouzdanost u marku mogu biti narušeni.

Drugo, postoje povrede podataka, a hakiranje je najčešći uzrok. Čuvanje privatnih podataka važnije je nego ikad. IT stručnjaci tradicionalno su bili zaduženi za mrežnu arhitekturu i fizički hardver koji štiti privatne podatke. Neke od tih sigurnosnih kontrola (privatne, javne ili hibridne) prenose se pouzdanom partneru u oblaku, što dovodi do sigurnosnih problema. Od ključne je važnosti raditi s kompanijom koja ima dokazane rezultate u implementaciji snažnih sigurnosnih mjera.

Osim toga, postoji rizik od gubitka podataka. Mnoge kompanije zabrinute su za sigurnost svojih najpovjerljivijih podataka kada su pohranjeni u oblaku. Gubitak podataka u oblaku u

slučaju prirodne katastrofe mogao bi biti katastrofalan za preduzeće. DDoS napadi obično se koriste za krađu ili brisanje osjetljivih podataka. Preduzeća koja se bave ovim problemom moraju imati planove za oporavak od katastrofe i integrisanu strategiju za borbu protiv kibernetičkih napada. Sigurnosno rješenje u oblaku također mora štititi sloj aplikacije.

Sigurnost računarstva u oblaku izgrađena je na čvrstim temeljima znanja o sigurnosti i otvorenoj komunikaciji o prijetnjama. Kao dio sveobuhvatne strategije sigurnosti podataka, administratori web stranica i aplikacija trebali bi biti svjesni potencijalnih sigurnosnih problema. Neophodno je imati otvorene linije komunikacije u slučaju krize kako bi se šteta svela na minimum.

U svakom slučaju, sigurnosni problemi u računarstvu u oblaku mogu se riješiti, a s pravim pružateljem usluga u oblaku, tehnologijom i pripremom, kompanije mogu iskoristiti prednosti računarstva u oblaku.

3.1.3. Neadekvatno brisanje podataka

Jedan od najzahtjevnijih dijelova upravljanja podacima u oblaku je brisanje podataka. S jedne strane, to je proces koji treba učiniti nepovratno. S druge strane, administrator mora osigurati da nema preostalih sigurnosnih kopija. U slučajevima kada više korisnika dijeli infrastrukturu, podatke je potrebno obrisati bez mogućnosti ponovnog vraćanja. Nije dovoljno obrisati tvrdi disk i nadati se najboljem.

Naehrig, et. al. (2011), tvrdi da nepotpuno brisanje podataka može dovesti do nenamjernog ili unaprijed pripremljenog izlaganja osjetljivih podataka. Troškovi povezani s takvim otkrivanjem su visoki i uključuju finansijske gubitke (i za korisnike i za pružatelje, npr. kroz regulatorne kazne) i gubitak ugleda. Na primjer, sistem pružatelja usluga nije uspio očistiti diskove prije nego što ih je preraspodijelio na nove korisnike. Međutim, važno je napomenuti da garantovano brisanje u oblaku nije samo važno korisnicima, već je ono također važno pružateljima usluga. Iz perspektive korisnika, bitno je dobiti garancije da će podaci biti uništiti prema dogovoru. Sa perspektive pružatelja usluge oblaka, takve su garancije potrebne za usklađenost s podacima, propisima raznih zemalja i regija te je također nužno adresirati zahtjeve i očekivanja korisnika. Nadalje, garancije za brisanje stvaraju diferenciranost na tržištu između pružatelja usluga oblaka.

Uloženi su značajni napori u raznim područjima kako bi se korisnicima oblaka pružile garancije kao što su dokaz o dostupnosti podataka, integritet podataka, lokacija podataka i šifriranje. Ponekad su takve garancije uključene u ugovore ali i dalje zahtijevaju povjerenje pružatelju bez ikakvog tehničkog dokaza. Tehničke garancije i dokaz o brisanju na zahtjev, mogu stvoriti povjerenje korisnika o tome kako se postupa s njihovim vanjskim podacima i kako se povlače iz upotrebe (Benson, *et.al.*, 2011).

3.1.4. Ranjivost sigurnosnih kopija

Sigurnosno kopiranje u oblaku, također je poznato kao mrežno sigurnosno kopiranje ili strategija za slanje kopije fizičke ili virtualne datoteke ili baze podataka na sekundarnu lokaciju izvan lokacije radi očuvanja u slučaju kvara opreme, katastrofe na lokaciji ili ljudske prevare (Benson, *et.al.,* 2011). Poslužitelj rezervnih kopija i sistemi za pohranu podataka obično su smješteni kod treće strane u oblaku ili SaaS pružatelju usluga koji korisniku rezervne kopije naplaćuje ponavljajuću naknadu na temelju korištenog prostora za pohranu ili kapaciteta, propusnosti prenosa podataka, broja korisnika, broja poslužitelja ili broja puta dohvaćanja podataka.

Implementacija sigurnosne kopije podataka u oblaku može pomoći u jačanju zaštite podataka organizacije, kontinuiteta poslovanja i strategija usklađenosti s propisima bez povećanja radnog opterećenja IT osoblja. Prednost uštede rada može biti značajna i dovoljna za nadoknadu nekih dodatnih troškova povezanih sa sigurnosnim kopiranjem u oblaku, kao što su troškovi prenosa podataka.

Što se tiče sigurnosnih kopija podataka, zahtijeva se potpuna vidljivost mjesta čuvanja. U oblaku ne bi smjele biti pohranjene nenadzirane kopije jer bi ti podaci s vremenom mogli pronaći put do hakera. Ipak, u većini slučajeva brisanje podataka mora slijediti procedure pružatelja usluga oblaka, tako da će to vjerovatno biti zajednički napor, iako neki pružatelji usluga u oblaku mogu imati drugačije zahtjeve.

Postoje različiti pristupi sigurnosnom kopiranju u oblaku, s dostupnim uslugama koje se lako mogu uklopiti u postojeći proces zaštite podataka u organizaciji. Varijante sigurnosne kopije u oblaku uključuju sljedeće:

- Sigurnosno kopiranje direktno u javni oblak. Jedan od načina pohranjivanja organizacionih radnih opterećenja je dupliciranje resursa u javnom oblaku. Ova metoda uključuje pisanje podataka direktno pružateljima usluga oblaka, kao što su AWS, Google Cloud ili Microsoft Azure. Organizacija koristi vlastiti softver za sigurnosno kopiranje za izradu kopije podataka za slanje u uslugu pohrane u oblaku. Usluga pohrane u oblaku zatim pruža odredište i sigurno čuvanje podataka, ali ne pruža posebno aplikaciju za sigurnosno kopiranje. U ovom je scenariju važno da softver za sigurnosno kopiranje može komunicirati s uslugom pohrane u oblaku. Osim toga, s opcijama javnog oblaka, IT stručnjaci će možda trebati razmotriti dodatne postupke zaštite podataka, kao što je enkripcija podataka, kao i upravljanje identitetom i pristupom kako bi osigurali sigurnosne kopije podataka.
- Sigurnosno kopiranje davatelju usluga. U ovom scenariju organizacija zapisuje podatke u uslugu u oblaku ili SaaS davatelju koji nudi usluge sigurnosnog kopiranja u upravljanom podatkovnom centru. Softver za izradu sigurnosnih kopija koji kompanija koristi za slanje svojih podataka usluzi može biti dostavljen kao dio

usluge ili usluga može podržavati određene komercijalno dostupne aplikacije za izradu sigurnosnih kopija.

- Izbor sigurnosne kopije iz oblaka u oblak (C2C). Ove su usluge među najnovijim ponudama u areni sigurnosnog kopiranja u oblaku. Specijalizovane su za sigurnosno kopiranje podataka koji već žive u oblaku, bilo kao podaci stvoreni pomoću SaaS aplikacije ili kao podaci pohranjeni u usluzi sigurnosnog kopiranja u oblaku. Kao što joj ime govori, C2C backup usluga kopira podatke iz jednog oblaka u drugi oblak. Usluga sigurnosnog kopiranja iz oblaka u oblak obično „ugošćuje" softver koji upravlja ovim procesom.
- Korištenje online sistema za sigurnosno kopiranje u oblaku. Postoje i hardverske alternative koje olakšavaju sigurnosno kopiranje podataka u uslugu sigurnosnog kopiranja u oblaku. Ovi su uređaji sve-u-jednom strojevi za sigurnosno kopiranje koji uključuju softver za sigurnosno kopiranje i kapacitet diska, zajedno s poslužiteljem za sigurnosno kopiranje. Uređaji su približno bliski plug-and-playu kao što je sigurnosno kopiranje, a većina njih također pruža besprijekornu vezu s jednom ili više usluga sigurnosnog kopiranja u oblaku ili pružatelja usluga u oblaku. Popis dobavljača koji nude uređaje za sigurnosno kopiranje koji uključuju sučelja u oblaku je dugačak, a u ovoj su „areni" aktivni Quantum, Unitrends, Arcserve, Rubrik, Cohesity, Dell EMC, StorageCraft i Asigra. Ovi uređaji obično zadržavaju najnoviju sigurnosnu kopiju lokalno, uz kopiranje u pružatelja sigurnosne kopije u oblaku, tako da se svi potrebni oporavci mogu izvršiti iz lokalne sigurnosne kopije, štedeći vrijeme i troškove prenosa (Subashini, Kavitha, 2011).

3.1.5. Manjak povjerenja i transparentnosti

Pružatelj usluga u oblaku mora dati uvjerenje korisnicima oblaka da će se njihovi podaci pravilno zaštititi. Također, korisnici moraju biti obavješteni o nastalim incidentima vezanim za sigurnost i privatnost. Određeni pružatelji usluga u oblaku informišu korisnike o načinu rukovanja sa podacima, sigurnosnim sistemima i s tim u vezi davanjem garancija.

Almanea (2014) tvrdi da se obično transparentnost računarstva u oblaku svodi na deklarisanje jasnih pragova usluge. Vrijeme neprekidnog rada, dostupnost sistema, vrijeme odziva i rješavanje problema samo su neki od faktora koji zahtijevaju otvorenu i poštenu izjavu o ograničenju. Od politika do cijena, sve treba biti transparentno.

Prema Shimba (2010), sigurnosne kontrole koje se koriste u računarstvu u oblaku općenito su slične onima koje se primijenjuju u tradicionalnim IT postavkama. S druge strane, računarstvo u oblaku može donijeti različite rizike za organizacije u odnosu na tradicionalno okruženje. To je zbog vrste oblaka, modela koji se koriste, operativnih modela i tehnologija za postavljanje usluge u oblaku. Štaviše, u računarstvu u oblaku odgovornost za implementaciju sigurnosne kontrole su odvojene između pružatelja usluga oblaka i potrošača oblaka, ovisno od modela isporuke (tj. SaaS, PaaS ili IaaS).

Transparentnost i povjerenje bitne su komponente svakog poslovnog odnosa i oni postaju posebno važni pri odabiru clouda. Pojam reputacije usko je povezan s pouzdanošću. Reputacija se definiše kao uvjerenja ili mišljenja koja se općenito drže o nekome ili nečemu. Jedna od preporuka koja bi mogla povećati pouzdanost pružatelja usluga oblaka je njihova procjena na temelju detaljnih parametara kvaliteta usluge zajedno s povratnim informacijama potrošača, te daljnji specifični parametri vezani uz računarstvo u oblaku (Khan, Malluhi, 2010).

Zasad se čini da se transparentnost svodi na koristi za kupce i korisnike, ali to nije istina. Transparentnost računarstva u oblaku ima ključnu ulogu u budućnosti računarstva u oblaku. Uz sigurnost, transparentnost je najvažniji aspekt prilagodljivosti. Što su dobavljači oblaka transparentniji, to će preduzeća lakše polagati svoje povjerenje u oblak. Uz sve veći broj klijenata u oblaku, dobavljači u oblaku pronaći će više prilika za optimizaciju svoje usluge i potrošnje. Iako postoji mnogo toga što treba učiniti na strani dobavljača, korisnici bi također trebali biti oprezniji pri izboru dobavljača koji obećava transparentnost računarstva u oblaku i pruža je. Moguće je posjetite podatkovni centar i zatražiti izvještaje o reviziji usklađenosti ili pravila obavještavanja o kršenju. Veća transparentnost poboljšat će nivo povjerenja između prodavača i kupaca i na kraju oblikovati budućnost oblaka.

Izgradnja profila pouzdanosti za pružatelje usluga oblaka je važna, jer će pružiti mehanizam refleksije sigurnosnog profila pružatelja usluga oblaka na otkrivanje snaga i slabosti unutar pružatelja usluga oblaka. Mjerenje pouzdanosti pružatelja usluga u oblaku važno je pitanje. Kako se transparentnost smatrala preduslovom za izbor pružatelja usluga oblaka, metoda za procjenu pouzdanosti oblaka bila bi ključna za potencijalne kupce oblaka (Alhamad, Dillon, Chang, 2011).

3.2. Prijetnje i ranjivost

Svaka prijetnja koja se i dogodi, šteti sistemu i smanjuje povjerenje, dostupnost i integritet. Razlikuju se zlonamjerne prijetnje (npr. namjerno mijenjanje ključnih podataka) i slučajne prijetnje (npr. slučajno brisanje datoteke). Ranjivost je slabost sistema, koja „pomaže“ prijetnji. Ako se smanji ranjivost sistema, smanjit će se i mogućnost prijetnji sistemu. Na primjer, alat za kreiranje lozinki koji olakšava izbor robusnih lozinki, limitirat će mogućnost izbora loših lozinki (ranjivost) i otkrivanja lozinke (prijetnja spoljašnjeg napada).

Organizacije koje koriste tehnologije u oblaku i/ili biraju pružatelje usluga u oblaku i usluge ili aplikacije bez potpunog razumijevanja rizika izlažu se riziku od određenih komercijalnih, finansijskih, tehnoloških, pravnih problema i problema s usklađenošću. Računarstvo u oblaku je brzorastući sektor, a poslovi računarstva u oblaku imaju veliku potražnju. No, nažalost, prema studiji koju je proveo HelpNetSecurity, 93% organizacija ima veliku zabrinutost oko sigurnosti javnog oblaka (Alhamad, Dillon, Chang, 2011).

Usluge u oblaku promijenile su način na koji kompanije pohranjuju podatke i hostiraju aplikacije, istovremeno uvodeći nove sigurnosne izazove.

Upravljanje identitetom, autentifikacijom i pristupom – To uključuje neuspjeh u korištenju višefaktorske autentifikacije, pogrešno konfigurisane pristupne tačke, slabe lozinke, nedostatak skalabilnih sistema upravljanja identitetom i nedostatak tekuće automatizovane rotacije kriptografskih ključeva, lozinki i certifikata (Ogigau-Neamtiu, 2012).

Ranjivi javni API-ji – Od provjere autentičnosti i kontrole pristupa do enkripcije i praćenja aktivnosti, sučelja za programiranje aplikacija moraju biti dizajnirana za zaštitu od slučajnih i zlonamjernih pokušaja pristupa osjetljivim podacima (Ogigau-Neamtiu, 2012).

Preuzimanje računa – Napadači mogu pokušati prisluškivati korisničke aktivnosti i transakcije, manipulisati podacima, vraćati krivotvorene informacije i preusmjeravati korisnike na nelegitimne stranice.

Zlonamjerni insajderi – Sadašnji ili bivši zaposleni ili izvođač s ovlaštenim pristupom mreži, sistemima ili podacima organizacije može namjerno zloupotrijebiti pristup na način koji dovodi do povrede podataka ili utiče na dostupnost informacionih sistema organizacije.

Dijeljenje podataka – Mnoge usluge u oblaku osmišljene su kako bi olakšale dijeljenje podataka među organizacijama, povećavajući područje napada za hakere koji sada imaju više meta dostupnih za pristup kritičnim podacima.

Napadi uskraćivanjem usluge – Poremećaj infrastrukture oblaka može uticati na više organizacija istovremeno i omogućiti hakerima da naštete kompanijama bez pristupa njihovim računima usluga oblaka ili internoj mreži.

Napadači imaju dva načina napada kako bi ugrozili resurse oblaka (Potdar, *et.al*., 2015):

- Prvi je tradicionalni način, koji uključuje pristup sistemima unutar mrežnog vatrozida preduzeća, nakon čega slijedi izviđanje i eskalacija privilegija na administrativni račun koji ima pristup resursima u oblaku.

- Drugi uključuje zaobilaženje svega navedenog jednostavnim ugrožavanjem korisničkog imena/lozinke s administrativnog računa koji ima administrativne mogućnosti ili ima administrativni pristup pružatelja usluga u oblaku (CSP).

Kada je glavni administrativni račun ugrožen, to je mnogo štetnije za sigurnost mreže u oblaku. Uz pristup administrativnom računu, napadač ne treba eskalirati privilegije ili održavati pristup mreži preduzeća jer glavni administrativni račun može učiniti sve to i više.

Više nije dovoljno identifikovati sumnjivi pokušaj prijave da bi se zaštitila vlastita mreža u oblaku. Moderni, sofisticirani hakeri mogu pristupiti računu putem društvenog inženjeringa, kao što je phishing. Sada je bitno pratiti ponašanje računa koji su već prijavljeni i otkriti

svaku sumnjivu aktivnost. Čak i u oblaku, kompanije čine značajnu grešku kada misle da će oblak zaštititi njihova radna opterećenja i podatke od napada, krađe i drugog nedoličnog ponašanja. Dakle, i u oblaku nedostaci i potencijal za iskorištavanje su neizbježni.

Velika količina podataka koja teče između organizacija i pružatelja usluga u oblaku stvara prilike za slučajno i zlonamjerno curenje osjetljivih podataka nepouzdanim trećim stranama. Ljudska pogreška, prijetnje iznutra, zlonamjerni softver, slabe lozinke i kriminalne aktivnosti pridonose većini povreda podataka usluge oblaka. Zlonamjerni akteri, uključujući hakere koje sponzoriše čak država, nastoje iskoristiti sigurnosne ranjivosti usluge oblaka kako bi izvukli podatke iz mreže organizacije žrtve za profit ili druge nedopuštene svrhe.

3.2.1. Klasifikacija sigurnosnih prijetnji u Cloud computingu

3.2.1.1.Tradicionalne sigurnosne prijetnje

Tradicionalne sigurnosne prijetnje su olakšane korištenjem računarstva u oblaku, a odnose se na upade ili napade na računar i mrežu. Navode se sljedeći sigurnosni problemi:

- napadi na nivou virtualne mašine – haker koristi moguće ranjivosti hipervizora, kako bi preuzeo kontrolu nad njim
- phishing oblak – uglavnom se koristi u e-porukama ili društvenim mrežama, cilj je animirati korisnike da kliknu zlonamjerne veze
- proširena površina napada mreže – korisnik oblaka mora izvršiti zaštitu infrastrukture koju koristi za povezivanje i interakciju s oblakom
- autentifikacija i autorizacija – autentifikacija i autorizacija organizacija se ne proširuje na oblak, stoga organizacija treba da poveže svoje sigurnosne mjere i pravila sa onima koje su prisutne u oblaku (Subashini, Kavitha, 2011).

3.2.1.2.Problemi s dostupnošću

Problemi sa dostupnošću su fokusirani na kritične aplikacije i dostupnost podataka. Poznat je incident u oblaku koji se odnosio na jednodnevni prekid rada Gmaila polovinom oktobra 2008. godine. Neki od prioriteta, kada je riječ o ovoj vrsti prijetnji, odnose se na obaveze pružatelja usluga oblaka da daje verodostojne rezultate i obezbjeđuje računarski integritet, da održava kontinuirani rad i da ne uskraćuje usluge, što stvara smetnje u radu korisnika.

3.2.1.3.Problemi kontrole podataka od trećih strana

Postoji mogućnost nedostatka kontrole i transparentnosti, ako se podaci nalaze kod treće strane. Posjedovanje podataka kod treće strane može izazvati pravne posljedice, koje su složene i ne shvataju se baš najbolje. Sen (n.d.) navodi probleme koji moraju biti riješeni: - dubinska analiza (sigurnost korisnika u pružatelja usluga oblaka vezano za trajno brisanje

podataka na osnovu njegovog zahtjeva, isporuka podataka u dogovorenom roku od strane pružatelja usluga oblaka); - revizija (odgovarajuća transparentnost pružatelja usluga vezano za potrebe revizije); - ugovorne obaveze (korištenje tuđe infrastrukture može dovesti do nepodudarnosti interesa i niza pravnih učinaka); - špijunaža pružatelja usluga oblaka (pružatelj usluga oblaka može izvršiti krađu podatakakorisnika); - tranzitivna priroda ugovora (pružatelj usluga oblaka može imati i kooperante, koje korisnici oblaka ne mogu ili mogu simbolično kontrolisati).

3.2.1.4. Nove sigurnosne prijetnje podacima u Cloudu

Sen ističe dodatne sigurnosne prijetnje u računarstvu u Cloudu**:**

- Napad bočnih kanala – Kod modela isporuke u oblaku kod kojeg se koristi virtualizacija, prisutna je prijetnja od napada bočnih kanala, što prouzrokuje curenje podataka. Iako je ovaj rizik još u svojim začecima, ipak doživljava svoj razvoj kako se razvija tehnologija virtualnih mašina.
- Napadi uskraćivanja usluge (DoS) – Korisnike usluga oblaka posebno brine dostupnost usluga, te je neophodno da pružatelj usluga minimizira navedene prijetnje. Uskraćivanje usluga može biti prouzrokovano napadima koji opterećuju infrastrukturu previše obimnim prometom, čime se preopterećuju raspoloživi resursi i otkazuju komponente.
- Napadi na društvene mreže – Uporedo sa naraslom popularnošću društvenih mreža, raste i rizičnost od napada. Računarstvo u oblaku je cilj napada, jer raspolaže sa velikim skladištima podataka o korisnicima.
- Napadi na mobilne uređaje – Pametni telefoni sve više zamjenjuju prenosne ili stolne računare, te se povezuju u oblak. Stoga su i mobilni uređaji postali česta "meta" napada. Crvi, špijunski softveri i sl. napadaju mobilne uređaje, koji ne posjeduju adekvatnu zaštitu. Odgovarajuće tehnologije zaštite, antivirusni programi ili kompletna šifriranja diska još uvijek nisu "zaživjeli" na današnjim pametnim telefonima.
- Unutrašnja prijetnja i prijetnja organizovanog kriminala **–** Pružatelji usluga oblaka pohranjuju različite vrste podataka, uključujući i podatke o kreditnim karticama i druge finansijske i lične podatke, koji su posebno važni za kriminalce. Postoji zabrinutost da članovi oblaka čak namjerno koriste pristupanje korisničkim podacima i sistemima ispitivanja, s ciljem pomaganja vanjskim napadačima kojima trebaju dodatne informacije za izvršavanje složenih napada.
- Analiza podataka **–** Pojava računarstva u oblaku dovela je do stvaranja ogromnih skupova podataka, koje je moguće unovčiti pomoću aplikacija, kao što je oglašavanje. Na primjer Google, koristeći svoju infrastrukturu u oblaku prikuplja i analizira podatke o potrošačima za svoju oglasnu mrežu. Privatnost korisničkih podataka je uveliko ugrožena usljed dostupnosti podataka i jeftinih tehnika rudarenja podataka. Danas napadači raspolažu sa velikim, centralizovanim bazama podataka

dostupnim za analiziranje, kao i sirovom računarskom moći za miniranje ovih baza podataka.

- Isplativa odbrana dostupnosti – Dostupnost se razmatra sa aspekta protivnika, koji želi sabotirati aktivnosti. Politički sukobi se prenose na web, stoga protivnici postaju realni.
- Povećani zahtjevi za autentifikacijom – Umjesto da kupuju licence i instaliraju softver, korisnici se odlučuju za autentifikaciju, da bi koristili aplikaciju u oblaku. U ovom modelu otežano je softversko piratstvo i olakšano je centralizovano praćenje, te se onemogućava širenje osjetljivih podataka ka nepouzdanim klijentima. Navedena arhitektura pomaže veću mobilnost korisnika, ali su potrebni robusniji protokoli za provjeru autentičnosti. Povećano "hostiranje" podataka i aplikacija u oblaku te manje fokusiranje na određene korisničke strojeve, povećava opasnost od krađe identiteta i podataka za pristupanje.

Slika 7. Sigurnosne prijetnje u Cloudu

Izvor: (Subashini, Kavitha, 2011)

3.3. Dijeljenje podataka u Cloudu

Pored pohranjivanja podataka u oblaku, važno je i njihovo dijeljenje. Dijeljenje podataka sa drugima je dodatni sigurnosni rizik, kada se pohranjuju podaci koji služe samo za ličnu upotrebu. Kada je riječ o kompanijama, one najčešće dijele podatke sa svojim zaposlenima, kako bi se mogao odvijati rad na daljinu.

Wheeler i Winburn (2015) preciziraju o čemu treba voditi računa prilikom dijeljenja podataka u oblaku:

- Povjerenje u članove – Kada odlučimo dijeliti svoje podatke sa drugima, moramo računati na njihove greške ili loše namjere, što čini da postajemo ranjivi. Očekujemo

od pojedinaca da budu odgovorni, u smislu da će dijeliti podatke samo sa članovima grupe, da neće učitavati neprikladan ili ilegalan sadržaj. Kada je riječ o dijeljenju podataka u oblaku, povjerenje je sigurno jedan od ključnih izazova.

- Kontrola pristupa – Odnosi se na mogućnost dozvole ili opoziva pristupanja podacima. Opoziv dozvole pristupanja podacima vrši se mijenjanjem lozinke za sve članove, da bi se poslije dojavila nova lozinka samo onim članovima kojima se želi dopustiti pristupanje podacima.
- Mehanizam dijeljenja – Primijenjeni mehanizmi dijeljenja podataka predstavljaju sigurnosni rizik o kojem pružatelj usluga mora voditi računa. Na primjer, korisnik oblaka može poslati URL za pristup drugom pojedincu, a problem nastaje kada Internet preglednici pohrane taj URL u historiju pretraga, te pojedinac ima ne samo pristup, nego i mogućnost dijeljenja URL sa drugima.

Pružatelji usluga oblaka koji se koriste za dijeljenje podataka su Dropbox, Box i OneDrive. Prilikom pretplate na Dropbox, dobija se određeni prostor za pohranjivanje na mrežnom poslužitelju, odnosno oblaku. Kada se izvrši instaliranje aplikacije Dropbox na mobilni uređaj, računar ili na oboje, datoteke koje su lokalno pohranjene u Dropbox, kopiraju se i na Dropbox poslužitelj. Promjena datoteka na jednom mjestu, dovodi do njihovog automatskog ažuriranja svuda. Osnovna prednost Dropboxa je jednostavno dijeljenje datoteka. Omogućeno je kontrolisanje nivoa dopuštenja i dijeljenja datoteka pomoću veze ili pravljenje javnih datoteka, čime se omogućava svakome sa adekvatnom vezom da pristupi podacima. Dropbox može sadržavati i određene alate za saradnju, npr. Dropbox Spaces, što olakšava timski rad sa dokumentima, dijeljenje zabilješki i sređivanje u stvarnom vremenu (Johnson, 2021).

Box koristi sličan pristup kao Dropbox, vezano za pohranjivanje u oblaku. Box postavlja određenu mapu na Windows ili macOs računar, te održava cjelokupan njen sadržaj sinhronizovan sa oblakom, zajedno i sa svim drugim uređajima koji imaju instalisan Box. Datoteke i mape se jednostavno dijele, kada je potrebna saradnja sa drugim osobama oko nečega ili je pak potrebno samo stvoriti vezu koja se distribuira onima kojima je potrebna (Pickavance, Nield, DeMuro, 2021).

One Drive ima mogućnost dijeljenja datoteka sa drugim osobama, koje se mogu dijeliti direktno sa lokalnog računara ili sa web mjesta za pohranjivanje. Datoteke se mogu dijeliti sa jednom ili više osoba pomoću e-pošte ili veze. Također, može se regulisati da li želimo da druge osobe mogu uređivati naše datoteke na OneDrive usluzi ili ih samo pregledati (Whitney, 2020).

3.4. Prelazak na Cloud computing – koraci

Navode se sljedeći koraci koje treba uzeti u obzir prije prelaska na Cloud computing:

- Arhitektura migracije – Prvi korak prije migracije u oblak je izgradnja robusne arhitekture migracije. Sistemska migracijska arhitektura odgovorna je za definisanje zahtjeva za oblak, planiranje resursa i dizajniranje strategija. Kako strategija migracije u oblak uključuje detaljno tehničko planiranje i strukturisano projektovanje, cjelokupna odgovornost je u rukama arhitekte migracije za donošenje kritičnih odluka kako bi se osigurao uspješan proces migracije u oblak.
- Procjena platforme u oblaku – Preduzećima je izuzetno teško odabrati platformu u oblaku za migraciju svojih kritičnih aplikacija. Optimizacija aplikacija na platformi u oblaku isključivo ovisi od API-ja i tehnologija koje se koriste tokom razvoja softvera. Prije nego se odluče za jednu platformu u oblaku ili platformu s više oblaka, organizacije moraju temeljito procijeniti preduslove svog poslovanja i tehnologiju koja se koristi u njihovim aplikacijama.
- Ukupni trošak – Odlučivanje o pristupačnom budžetu za korake migracije u oblak postaje ključni zadatak za svaku kompaniju. Preduzeća moraju procijeniti ukupnu cijenu resursa i također biti dobro informisana o modulu cijena platformi u oblaku. Kompanije moraju procijeniti svoju infrastrukturu i interne resurse prije ulaganja u pristup migracije u oblak. Postoje razni alati u oblaku i aplikacije trećih strana koji mogu pomoći u razvoju poslovanja i povećanju produktivnosti.
- Cloud Provider – Prije ulaganja u alate za migraciju u oblak vrlo je bitno izabrati pravog pružatelja usluga u oblaku. Kompanije bi trebale analizirati i pažljivo proučiti pružatelja usluga oblaka na temelju tehnologije, kompatibilnosti, međunarodnih standarda i vladajućih politika. Prikladan pružatelj usluga može učinkovito raditi s našim aplikacijama i ponuditi podršku 24/7 našoj kompaniji.
- Sigurnost – Podaci su najvažniji i najpovjerljiviji element svake kompanije. Svaka kompanija nastoji osigurati sigurnost i zaštitu svojih povjerljivih informacija pohranjenih u uređajima. Organizacije moraju temeljito proučiti sigurnosne politike i propise pružatelja usluga oblaka prije postavljanja svojih aplikacija na platformu u oblaku. Prema izvještajima istraživanja, više od 60% kompanija je zabrinuto zbog sigurnosnih mjera koje slijede pružatelji usluga oblaka.

Dok se odlučuju za novu infrastrukturu, kompanije moraju uzeti u obzir sve značajne faktore tokom migracije svojih aplikacija na platformu u oblaku. Pružatelj usluge Cloud Security trebao bi ponuditi visoke sigurnosne mjere kako bi osigurao zaštitu i sigurnost povjerljivih podataka svake kompanije. Migracija na oblak ključna je procedura, ali uz ispravne korake koje slijedi izabrani pružatelj usluge oblaka, prebacivanje na platformu u oblaku može biti pojednostavljen proces. Kalluri i Rao (2014) su naveli neke od smjernica za zaštitu korisnika računarstva u oblaku. Sigurnosni mehanizmi se dijele na dvije grupe – zasnovani na partnerima (sigurnost za SaaS, PaaS i IaaS) i korisnički (na bazi klijenta):

- Strateško planiranje sigurnosti u oblaku – Razmatranje sigurnosti u početnoj fazi planiranja je izuzetno važno. Potrebno je sagledati kako će se korporativno radno opterećenje isporučiti do krajnjih korisnika.

- Izbor pružatelja usluga oblaka – Najvažnije je da se izabere onaj pružatelj usluga oblaka koji će obezbijediti zaštitu osjetljivih podataka ili informacija. Prije samog izbora pružatelja usluga oblaka važno je provjeriti njihovo iskustvo u IT i sigurnosni aspekt , te garancije vezane za učinkovitost strateških usluga.
- Pisani dokument o sigurnosnim mjerama koje daje pružatelj usluga oblaka – Odnosi se na dobijanje uvjerenja koje se reguliše u ugovoru od strane pružatelja usluga oblaka. Dokument treba da sadrži aplikacije, infrastrukturu, konfiguracije, politike, pravila, propise.
- Nadziranje podataka – Ključno je provjeriti tko ima pristup podacima i zašto im i kada pristupa.
- Plan za sigurnosne probleme – Važno je znati koji nivo odgovornosti garantuje pružatelj usluga oblaka i koje aktivnosti će preduzeti u toku i poslije sigurnosnog problema.
- Provjera kontrole pristupa – Potrebno je definisati uloge i odgovornosti, kako bi se i privilegovani korisnici morali testirati i imati odgovornosti.
- Kontrola sistema – Pružatelj usluga oblaka kontinuirano vrši kontrolu podataka u oblaku, utvrđuju se mjerni podaci za performanse u oblaku i redovno se obavlja njihovo testiranje (Kalluri, Rao, 2014).

3.4.1. Zaštita podataka u Cloudu

U nastavku su navedeni savjeti za osiguravanje podataka u Cloudu:

- Lokalna sigurnosna kopija – S obzirom da se može desiti gubitak ili brisanje podataka iz oblaka, potrebno je napraviti sigurnosnu kopiju onoga što se pohranjuje u oblak, a posebno ako je riječ o ključnim podacima za poslovanje.
- Izbjegavanje pohranjivanja osjetljivih podataka – Osjetljive podatke, odnosno podatke koji mogu prouzrokovati štetu pojedincu ili organizaciji ako budu ukradeni, ne treba pohranjivati u oblak.
- Upotreba enkripcije – Šifriranje podataka, prije nego što se prenesu u oblak, predstavlja dobru zaštitu od hakera. U tom slučaju, pojedincu koji pristupi podacima bez posjedovanja ključa za dešifriranje, onemogućeno je njihovo čitanje.
- Upotreba pouzdanih lozinki – Lozinke trebaju biti nepredvidljive i teške za upamtiti. Upotreba jedinstvene lozinke je dobar izbor, uz redovnu promjenu. Pored toga, provjera u dva koraka povećava nivo sigurnosti. Ako se desi povreda u prvom sigurnosnom koraku, drugi i dalje štiti podatke.
- Dodatne sigurnosne mjere – Oblak treba posjedovati antivirusne programe, administratorske kontrole i sl. Za jačanje njegove sigurnosti.
- Testiranje sigurnosti – Testiranje uključuje ispitivanje u oblaku da bi se konstatovalo kako se ponaša sa aspekta sigurnosnih postavki (Kalluri, Rao, 2014).

Postoje i etičke hakeri koje je moguće unajmiti kako bi se testirao nivo sigurnosti sistema. Primjer svako rješenje za e-poštu u oblaku treba imati sljedeće:

- antivirus
- mogućnost stvaranja posebnih pravila za blokiranje sadržaja
- kontrolu protiv neželjenog sadržaja
- kontrolu curenja informacija

Sa druge strane, bilo koje Cloud aplikacijsko rješenje trebalo bi imati sljedeće mogućnosti:

- vatrozide aplikacije i vatrozide novih generacija
- alati za otkrivanje upada
- alati za ublažavanje DdoS napada
- evidenciju prijave

3.4.2. Dizajn sigurnosne arhitekture

Rittinghouse i Ransome (2010) navode da se okvir sigurnosne arhitekture treba kreirati vodeći računa o procesima (autentifikacija i autorizacija organizacije, kontrolisanje pristupa, povjerljivost, integritet, upravljanje sigurnošću), operativnim procedurama, tehničkim specifikacijama, upravljanjem ljudima i organizacijom, usklađenosti i izvještavanju o sigurnosnim programima. Potrebno je kreirati dokument o sigurnosnoj arhitekturi, koji precizira načela sigurnosti i privatnosti, da bi se lakše ostvarili poslovni ciljevi. Dokumentacija je neophodna za upravljačke kontrole, kontrole pristupanja sistemu, upravljanje mrežom i računarom, razvoj i održavanje aplikacija, metrike vezane za klasifikaciju i kontrolu imovine, kontinuirano poslovanja i usklađenost. Za program projektovanja i provedbe je poželjno da bude sadržan u životnom ciklusu razvoja sistema, da bi se uključio poslovni slučaj, definicija zahtjeva, dizajn i provedbeni planovi. Nužno je integrisati tehnologiju i metode projektovanja, te sigurnosne procese koji su potrebni za pružanje navedenih usluga u svim tehnološkim slojevima:

- autentifikacija
- autorizacija
- dostupnost
- povjerljivost
- integritet
- odgovornost
- privatnost (Rittinghouse, Ransome, 2010).

4. ISTRAŽIVANJE

4.1. Cloud computing u Bosni i Hercegovini

Sa Cloud computingom se postiže racionalno i ekonomično korištenje resursa. Suština Cloud computinga je da se vrši slanje i obrada podataka izvan kompanije koja je vlasnik tih podataka. Mjesto za obradu podataka može čak biti i u drugoj zemlji, čime se stvara sigurnosni izazov za ove podatke, ali i pitanje odgovornosti. Da bi se izbjegli sigurnosni i ostali problemi, preporučuje se da se koriste usluge certificiranih pružatelja Cloud computinga, koji mogu zadovoljiti međunarodne standard sigurnosti, a posebno sa aspekta cloud sigurnosti. U tom kontekstu je važna grupa ISO27000 standarda, a među njima posebno se ističe ISO27017, koji se fokusira na cloud. Izuzetno je važno sagledati podatke za koje nije poželjno da se pohranjuju u Cloud ili pak u Cloud van Bosne i Hercegovine. U tom smislu, takve podatke treba odrediti i za njih ne koristiti Cloud, odnosno Cloud izvan Bosne i Hercegovine.

U posljednje vrijeme su i kompanije u Bosni i Hercegovini prepoznale mogućnosti Cloud servisa, te ga sve više implementiraju u svojim poslovnim aktivnostima. Pandemija COVID-19 je još više intenzivirala ove promjene, s obzirom da su kompanije morale prilagoditi svoje poslovanje novonastaloj situaciji, te prihvatiti nove načine rada, kao što je rad na daljinu.

Ipak, process transformacije se i dalje odvija veoma usporeno. IKT istraživanje Zavoda za statistiku BiH za 2021. god. saopćilo je podatke prema kojima samo 8,9% kompanija u Bosni i Hercegovini upotrebljava u svom poslovanju neku od cloud usluga. Najčešće je riječ o usluzi skladištenja podataka.

Sporo prihvatanje cloud tehnologije je posljedica neshvatanja svih koristi od korištenja cloud usluga, brige za sigurnost podataka koji se pohranjuju "negdje u nekom oblaku", kao i neupućenosti oko funkcionisanja različitih servisa. Na temelju navedenog, neophodno je na bosanskohercegovačkom tržištu provoditi kontinuiranu digitalnu edukaciju.

4.2. Kompanije koje nude Cloud Computing rješenja u Bosni i Hercegovini

4.2.1. Pantheon Cloud Computing

Pantheon Cloud computing podaci koji se unose u program PANTHEON (kao što su fakture, plate, računovodstvo) pohranjuju se u bazu podataka koja se najčešće nalazi na namjenskom računaru, odnosno serveru. Server je stalno aktivan, što znači stalnu dostupnost podataka. Server raspolaže odgovarajućim sigurnosnim uslovima, tako da se onemogućava gubitak podataka, a to se prvenstveno odnosi na izradu sigurnosnih kopija, fizičku i programsku zaštitu. Kod usluge PANTHEON Cloud korisnici se ne brinu za serversku opremu, s obzirom da se njihova baza podataka pohranjuje u data centru BH Telecoma, koji vodi računa o sigurnosti i tehničkoj bezbrižnosti. Povezivanje sa svojom bazom podataka ostvaruje se

vezom preko Interneta, a za rad je potreban samo PANTHEON i dovoljno brza internetska veza. Hosting omogućava da manja preduzeća i računovodstveni servisi mogu pristupiti modernim poslovnim programskim rješenjima.

Korisnici PANTHEON Clouda imaju značajne benefite. Dodatna prednost hostinga jeste što je omogućen istovremeni pristup istim podacima koji se nalaze na jednom server i računovodstvenom servisu i njegovom klijentu, čime se smanjuju troškovi računovodstva. Sistem mrežnog hostinga ne treba miješati sa aplikacijama koje rade u web preglednicima. Mrežni hosting radi na principu Saas (Software as a service), gdje korisnik mora imati internetsku vezu da bi pristupio progamu PANTHEON. Internet služi samo za prenos podataka, program se nalazi u data centru, korisnik samo izvrši prijavu i radi preko Interneta u PANTHEON-u. Funkcionalnosti PANTHEON-a su iste i neograničene. Kod klasičnog načina korisnik upisuje podatke u PANTHEON koji se nalazi na njegovom računaru, dok sistem hostinga karakteriše unošenje podataka preko Interneta u PANTHEON, koji se nalazi u data centru. Sistem hostinga je više pouzdan i ima više mogućnosti u odnosu na web poslovne aplikacije.

Korisnički podaci su pohranjeni u sigurnim data centrima, certifikovanim po međunarodnim standardima sigurnosti. To podrazumijeva i zaštitu od krađe, uništavanja podataka od strane hakera (firewall, primjena enkripcije protokola), te zaštitu od katastrofa (zemljotres, požar). Kako se ne bi razotkrili podaci na putu između korisničkog računara i data centra, koristi se šifrirana komunikacija između PANTHEON-a i servera (SSL veza). SSL veza upotrebljava najmoćnije algoritme, a najčešće se koristi u poslovanju sa kreditnim karticama i e-poslovanju. Vrijedni podaci kompanija često budu izgubljeni usljed djelovanja više sile (udar groma najčešće uzrokuje gubitak podataka). Upravo zbog toga se vrši redovno arhiviranje podataka i izrada sigurnosnih kopija – backup-ova. U PANTHEON Cloudu sigurnosne kopije podataka kreiraju se barem jednom dnevno. Korisnici mogu raspolagati sa svim sigurnosnim kopijama koje su napravljene u posljednjih četrnaest dana (www.datalab.ba).

Korisnik ima pravo da u svakom momentu traži izradu sigurnosne kopije na DVD-u, ako želi fizički pristupiti bazi podataka za svoju arhivu. Kompletan e-arhivski sistem je već organizovan i postavljen u skladu sa korisnikovim potrebama. Da bi se kreirao siguran i pregledan e-arhiv samo još treba skener.

4.2.2. Cloud usluge BH Telecom-a

Portofolio Cloud usluga BH Telecom-a sadrži Cloud usluge koje BH Telecom pruža samostalno, ili u sklopu parnetrskih odnosa, i sastoji se od IaaS, Saas i PaaS servisa i usluga. BH Telecom Cloud podrazumijeva Public cloud uslugu, na vlastitoj infrastrukturi BH Telecom data centara. Data centri su lokacijski smješteni u Bosni i Hercegovini i to primarni u Sarajevo, a sekundarni disaster recovery u Zenici. BH Telecom Cloud servisi i usluge koje BH Telecom nudi krajnjim korisnicima su:

- Computing korištenje Cloud infrastrukture u data centru BHT kao servisa, tj korištenje virtualnih mašina sa zakupljenim prostorima u data centrima BHT
- Networking povezivanje udaljenih lokacija kroz javne ili iznajmljenje linkove, te Secure Geatway servis za pristup različitih lokacija
- Housing iznajmljivanje kolokacijskog prostora u BHT data centru
- Hosting pohrana web stranica i aplikacija, e-mail kao i domena na servere BHT
- Storage servis nudi pohranu podataka na serverima BHT
- Business Continuity direct backup automatsko kreiranje i pohranu sigurnosnih kopija na servere BHT
- Consalting savjetovanje, projektovanje i implementacija cloud rješenja.

4.2.3. Cloud usluge Logosofta

Korisnici usluga Virtualna mašina u okviru Cloud usluga Logosoft Data Centra mogu veoma jednostavno i brzo prilagoditi infrastrukturu svojim poslovnim potrebama. Logosoft u svojoj ponudi ima i dodatne usluge, kao što je automatska nadogradnja softvera, disaster recovery site, kao i podrška dvadesetčetiri sata u sedmici, što utiče na efikasnije poslovanje korisnika. Korisnici sami kreiraju svoj paket u skladu sa svojim potrebama. Data Centar predstavlja grupu međusobno umreženih servera i mrežnih storage-a, a koriste ih kompanije za udaljeno pohranjivanje, procesiranje ili distribuciju velike mase podataka uz upotrebu cloud usluge (www.logosoft.ba).

Logosoft Cloud usluga je bilo koji resurs koji je dostupan upotrebom Logosoftove privatne optičke mreže. Najčešće cloud usluge su softver kao usluga (SaaS), platforma kao usluga (PaaS) i infrastruktura kao usluga (IaaS). Logosoft je jedini Microsoft Silver ERP partner u Bosni i Hercegovini, te posjeduje višegodišnje iskustvo u projektima implementacije Microsoft Dynamics NAV rješenja u našoj zemlji, ali i u susjednim zemljama. Implementacija se odnosi na postavljanje NAV rješenja sa svim prilagođavanjima koja prate zakonsku regulativu Bosne i Hercegovine.

4.3. Koncept povjerenja u Cloud computingu

Mayer, Davis i Schoorman (1995) opisuju povjerenje kao mentalno stanje koje se sastoji od:

- očekivanja – korisnik očekuje određeno ponašanje od povjerenika (kao što je pružanje valjanih informacija ili učinkovito izvođenje radnji)
- uvjerenja – korisnik vjeruje da će se očekivano ponašanje dogoditi, na temelju dokaza povjerenikove kompetentnosti, integriteta i dobre volje
- spremnosti na preuzimanje rizika – korisnik je spreman preuzeti rizik za to uvjerenje (Mayer, Davis, Schoorman, 1995).

U Cloud computingu Huang i Nicol (2013) objašnjavaju da se izraz "povjerenje" često slobodno koristi u literaturi o Cloudu kao opći izraz za "sigurnost" i "privatnost". Ritua, Randhawab i Jainc (2017) navode povjerenje u Cloud computingu kao mjeru ugleda određenog CSP-a (Cloud Service Provider) koji ima određeni skup resursa za korisnike. Također, naveli su da postoje različite kategorije povjerenja u Cloud computing, uključujući povjerenje temeljeno na reputaciji, SLA (Service Level Agreements), povjerenje temeljeno na provjeri, povjerenje temeljeno na politici, povjerenje temeljeno na dokazima i društveno povjerenje.

Uusitalo, Karppinen, Juhola i Savola, (2010) su raspravljali o dvije vrste povjerenja koje su opisali kao čvrsto i meko. Čvrsto povjerenje ima takve atribute kao "autentičnost, enkripcija i sigurnost" dok se meko povjerenje odnosi na ljudsku psihologiju, lojalnost brendu i jednostavnost korisnika.

4.3.1. Faktori koji utiču na povjerenje u pohranu u Cloudu

Sun, Chang, Sun i Wang (2011) posmatraju povjerenje kao mjerljivo uvjerenje koje koristi iskustvo za donošenje pouzdanih odluka, gdje je povjerenje društveni, a ne tehnički problem. Komponenta povjerenja bitan je element u širokoj upotrebi i implementaciji usluga u Cloudu. Gefen, Karahanna i Straub (2003) objašnjavaju da je jedan učinkovit način podsticanja korištenja tehnologije Clouda smanjenje nepoželjnih, ali mogućih ponašanja putem percipiranog povjerenja u tehnologiju Clouda.

Rathi i Kumari (2015) ističu da u scenarijima Cloud computinga korisnici usluga u Cloudu (CSU) stavljaju svoje digitalne resurse u ruke pružatelja usluga u Cloudu (CSP), dajući CSP-u kontrolu nad gotovo svim sigurnosnim faktorima; to implicira da CSP mora naznačiti odgovarajući nivo povjerenja ako će percipirano povjerenje CSU-a rezultirati njihovim prihvatanjem usluga u Cloudu.

Mnogi su istraživači istraživali faktore koji utiču na povjerenje u pohranu u Cloudu. Na primjer, Kalloniatis (2016) je istaknuo da povjerenje u online kontekstu nije bilo prioritet za mnoge online korisnike tokom protekle decenije. Naglasio je da za razliku od offline povjerenja, online povjerenje ovisi od Interneta i povezanih tehnologija. Tehnološke determinante online povjerenja mogu uključivati sigurnosne značajke, mehanizme zaštite privatnosti, jednostavnost korištenja i pouzdanost sistema.

S druge strane, Rashidi i Movahhedinia (2012) navode da je Cloud computing uveden kao jedno od pitanja koje najviše obećava u informaciono-komunikacijskoj tehnologiji (IKT). Naglasili su da kada su podaci ili resursi kritični za korisnika u Cloudu, CSP bi trebao imati mehanizam koji bi se brinuo o odgovornosti, privatnosti, reviziji, pouzdanosti, sigurnosti, lokaciji podataka, istrazi, odvajanju podataka, integritetu, sigurnosnom kopiranju, oporavku i povlaštenom korisničkom pristupu, budući da ti elementi mogu imati veliki uticaj na nivo povjerenja korisnika u Cloud.

Ahmad, et al. (2012) je istaknuo da Cloud computing organizacijama isporučuje uslugu na zahtjev gdje god je potrebna, što se može procijeniti prema mnogim faktorima, uključujući omjer troškova i koristi, brzinu, potreban kapacitet i regulisanost podataka. Naglasili su da pružatelji usluga Clouda trebaju obratiti veliku pažnju na pouzdanost, sigurnost i zahtjeve korisnika kako bi stekli povjerenje kupaca. Uveli su model povjerenja između korisnika i pružatelja usluga Clouda koji mjeri tri aspekta povjerenja: ugovor o nivou usluge (SLA), znanje o cloud computingu te pozadinu Clouda i sigurnost.

Darsi, Babu i Darsi (2014) su skrenuli pažnju na drugu stranu povjerenja u Cloud computing, ističući da revizori moraju biti uključeni u planove svoje organizacije za Cloud computing od faze koncepcije pa nadalje, kako bi se osigurala identifikacija i ublažavanje rizika. Dodali su da faktori poput sigurnosti, standarda u okruženju Cloud computinga, problema s performansama, migracije podataka, upravljanja podacima, dostupnosti i transparentnosti Clouda mogu uticati na zadovoljstvo korisnika.

Uikey i Bhilare (2013) sugerišu da se uspostavljanje povjerenja temelji na iskustvu prikupljenom iz prethodnih interakcija entiteta. Istaknuli su da je povjerenje povezano sa sigurnošću, te da će atributi kao što su poštenje, pouzdanost, pravovremenost, sigurnost, kompetentnost, pouzdanost i istinitost funkcionisati prema očekivanjima.

Također, bitno je istaći da je visok nivo dostupnosti vjerovatno jedna od najvažnijih pokretačkih snaga za prelazak na Cloud. Stoga scenariji korištenja krajnjeg korisnika i funkcionalnost usluge imaju direktan uticaj na zahtjeve i očekivanja dostupnosti krajnjeg korisnika; dostupnost u široj slici može uticati na nivo sigurnosti cjelokupnog Clouda.

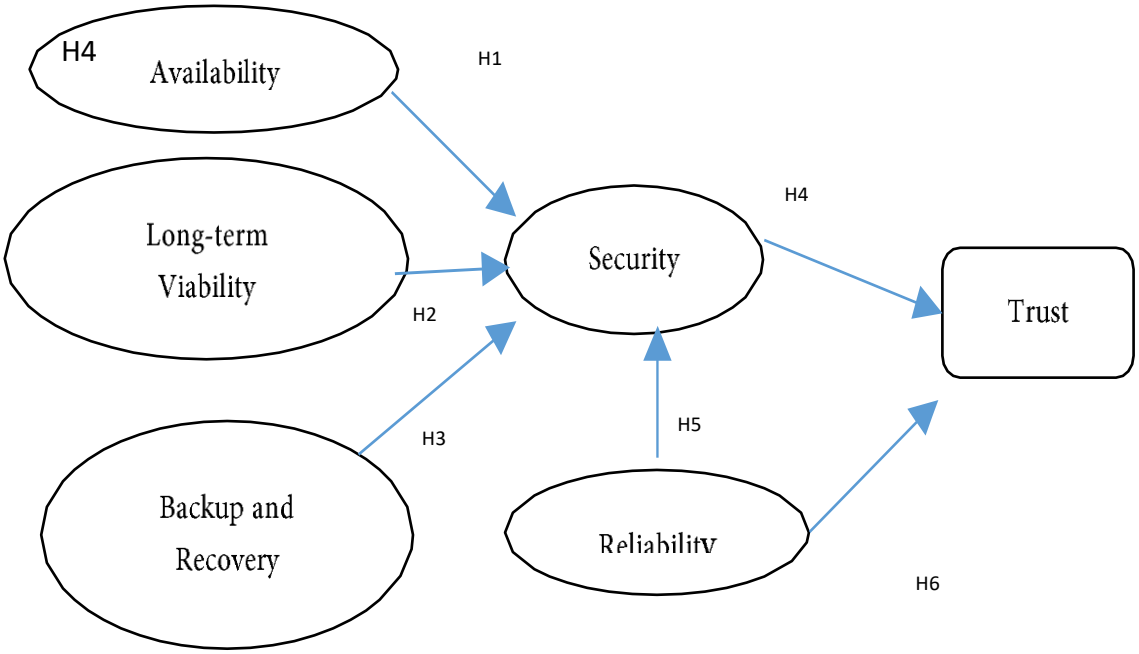
Vaish, Kushwaha, Das i Sharma (2013) predlažu mnoge faktore koje treba uzeti u obzir pri pružanju pouzdane platforme u Cloudu, uključujući povjerljivost, povjerljivost podataka, povjerljivost softvera, privatnost ili sigurnost, integritet podataka, dostupnost i lokaciju podataka.

4.4. Metodologija istraživanja

4.4.1. Razvoj instrumenata

Kako bismo istražili faktore koji utiču na percepciju korisnika u povjerenje aplikacija temeljenih na pohrani u Cloudu, kvantitativno istraživanje je provedeno sa podacima prikupljenim putem upitnika. Upitnik se sastojao od tri dijela: personalne informacije o korisnicima, korištenje pohrane u Cloudu i faktori koji utiču na povjerenje korisnika aplikacije za pohranu u Cloudu. Likertova skala od 5 bodova koristila se na način da se označi od potpuno se slažem = 1 do potpuno se ne slažem = 5. Stavke za svaku od varijabli prikazanih na slici 8 izvedene su iz literature.

Slika 8. Model istraživanja



Izvor: Autor rada

4.4.2. Analiza hipoteza

Dostupnost

Rathi i Kumari (2015) su istaknuli da korisnici trebaju stalnu dostupnost svojih podataka u Cloudu. Dostupnost Clouda je važno pitanje i pristup treba biti moguć kad god se to zatraži. Rashidi i Movahhedinia (2012) tvrde da su dostupnost i sigurnost međusobno povezane jer je sigurnost usko povezana s dostupnošću i njenim komponentama, kao što su upravljanje incidentima, nadzor i pristup podacima. Također naglašava se da ovlašteni korisnici moraju imati mogućnost pristupa svojim podacima putem svih resursa, softvera i hardvera, nakon što se uspješno prijave. Ramgovind, Eloff i Smith (2010) ističu da je dostupnost jedan od najkritičnijih zahtjeva za informacionu sigurnost u Cloudu. U skladu sa navedenim, postavlja se sljedeća hipoteza:

H1: Dostupnost je pozitivno povezana sa sigurnošću u Cloud computingu.

Dugoročna održivost

Rathi i Kumari (2015) tvrdili su da korisnici zahtijevaju da njihovi podaci budu održivi dugo vremena, tako da sebi ne mogu priuštiti prekid usluge ili da se nešto dogodi njihovim podacima. Dugoročna održivost važno je pitanje koje utiče na sigurnost. Sailaja i Usharani

(2017) su se složili da je sigurnost povezana s dugoročnom održivošću Cloud computinga, naglašavajući da treba postojati garancija dostupnosti podataka u slučaju bankrota ili akvizicije pružatelja usluga. Na temelju toga predlaže se sljedeća hipoteza:

H2: Dugoročna održivost je pozitivno povezana sa sigurnošću u Cloud computingu.

Sigurnosno kopiranje i oporavak

Rathi i Kumari (2015) ističu da se podaci korisnika mogu izgubiti u slučaju katastrofe. Stoga su predložili da pružatelj usluga Clouda mora imati tehnike za oporavak podataka nakon katastrofe ili bilo kakvih okolnosti koje dovode do gubitka podataka. Ako se dogodi kvar s Cloudom, ključno je potpuno vratiti podatke klijenata. Budući da klijenti nisu voljni dopustiti trećoj strani da kontroliše njihove podatke, to će uzrokovati „slijepu ulicu" u sigurnosnoj politici u ovim izazovnim situacijama. U skladu sa navedenim, postavlja se sljedeća hipoteza:

H3: Backup i Recovery su pozitivno povezani sa sigurnošću u Cloud computingu.

Sigurnost

Robinson, Valeri, Cave, et al. (2010) ukazuju da se sigurnost odnosi na povjerljivost, cjelovitost i dostupnost podataka ili informacija, dok sa druge strane ističu da se sigurnost u Cloudu odnosi na politike, tehnologije i kontrole postavljene za zaštitu aplikacija, podataka i povezane infrastrukture Cloud computinga. Sigurnost igra centralnu ulogu u sprečavanju kvarova usluga i „njegovanju" povjerenja u Cloud computing. Stoga se postavlja sljedeća hipoteza:

H4: Sigurnost je pozitivno povezana s povjerenjem korisnika Cloud computinga.

Pouzdanost

Pouzdanost se odnosi na uvjerenje da će pružatelj usluga pohrane u Cloudu učiniti ono što kaže da će učiniti, da djeluje dosljedno i pouzdano. Paine (2013) tvrdi da je pouzdanost važna komponenta povjerenja i odnosi se na pouzdanost, na sposobnost sistema ili komponente da obavlja svoje potrebne funkcije ili operacije pod navedenim uslovima u određenom vremenskom razdoblju. Bitno je istaći da pouzdanost doprinosi uspostavljanju povjerenja u usluge u Cloudu. Mora se uspostaviti visok nivo povjerenja i pouzdanosti jer ako treća strana ne pruži ispravna sredstva, to može dovesti do toga da informacije i podaci budu nesigurni. U skladu sa navedenim, postavljaju se sljedeće hipoteze:

H5: Pouzdanost je pozitivno povezana sa sigurnošću Cloud computinga.

H6: Pouzdanost je pozitivno povezana sa povjerenjem korisnika Cloud computinga.

4.4.3. Analiza podataka

Podaci su analizirani pomoću statističkog paketa (SPSS). Višestruka regresijska analiza je provedena, uz testove pouzdanosti i valjanosti. Rezultati daju temelj za prihvatanje ili odbacivanje hipoteza.

4.4.4. Uzorak istraživanja

Populacija ovog istraživanja su korisnici Cloud computinga za pohranu, te je odabran uzorak slučajnim odabirom. Ukupno je anketirano 178 ispitanika, menadžera kompanija u Bosni i Hercegovini. Tabela 4 prikazuje broj odgovora prema spolu i obrazovnom nivou menadžera. 38,8% ispitanika bili su muškarci, a nivo obrazovanja, za koji se naknadno utvrdilo da je u značajnoj korelaciji s povjerenjem korisnika u pohranu u Cloudu pretežno je bio dodiplomski (72,5%). Dodatno, u tabeli su prikazani i podaci o broju zaposlenih u kompanijama.

Tabela 3. Demografski podaci ispitanika

Demografski podaci		Procenat (%)
Spol	Muški	38.8
	Ženski	61.2
	Total	100.0
Nivo obrazovanja	Viša stručna sprema	19.1
	Bachelor Degree	72.5
	Master Degree	6.2
	PhD	2.2
	Total	100.0
Broj zaposlenih	1-9	12.4
	10-49	65.2
	50-249	21.3
	250 i više	1.1
	Total	100.0

Izvor: Autor rada

4.4.5. Test valjanosti i pouzdanosti

Većina ekstrahiranih eksponenata ima vrijednost od 0,5 i više što ukazuje na unutrašnju dosljednost i dokazuje da su stavke valjane. Tabela 5 prikazuje Cronbachove Alpha vrijednosti za svaki prihvaćeni faktor, u rasponu od 0,705 do 0,952. Također je prihvaćena dugoročna održivost od 0,677.

Tabela 4. Cronbach's Alpha za svaki faktor

Dostupnost	.709
Dugoročna održivost	.677
Backup and Recovery	.759
Sigurnost	.806
Transparentnost Clouda	.808
Pouzdanost	.758
Povjerenje	.728

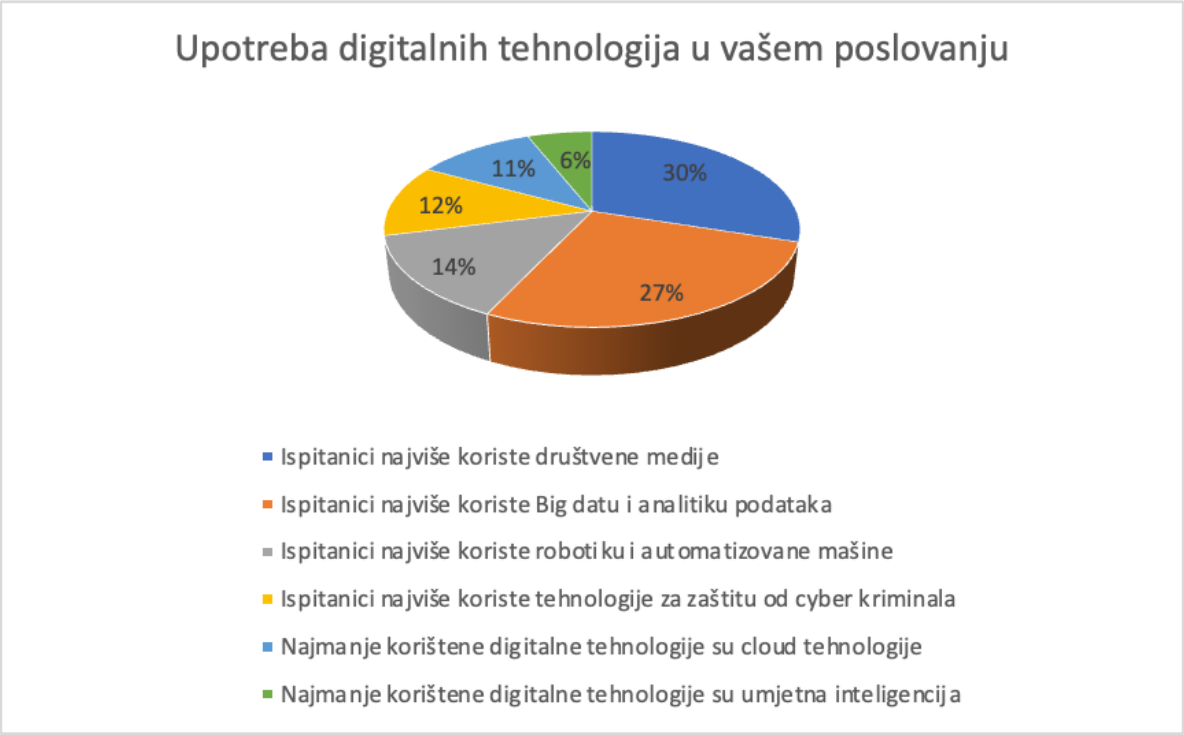
Izvor: Autor rada

4.5. Prezentacija rezultata istraživanja

4.5.1. Nivo digitalizacije poslovanja

Kada je riječ o upotrebi digitalnih tehnologija u poslovanju, ispitanici najviše koriste društvene medije, te Big datu i analitiku podataka (30%, odnosno 27% ispitanika). Zatim slijedi robotika i automatizovane mašine, te tehnologije za zaštitu od cyber kriminala (14%, odnosno 12% ispitanika). Najmanje korištene digitalne tehnologije su cloud tehnologije i umjetna inteligencija (11%, odnosno 6% ispitanika).

Grafikon 1. Upotreba digitalnih tehnologija u vašem poslovanju



Izvor: Autor rada

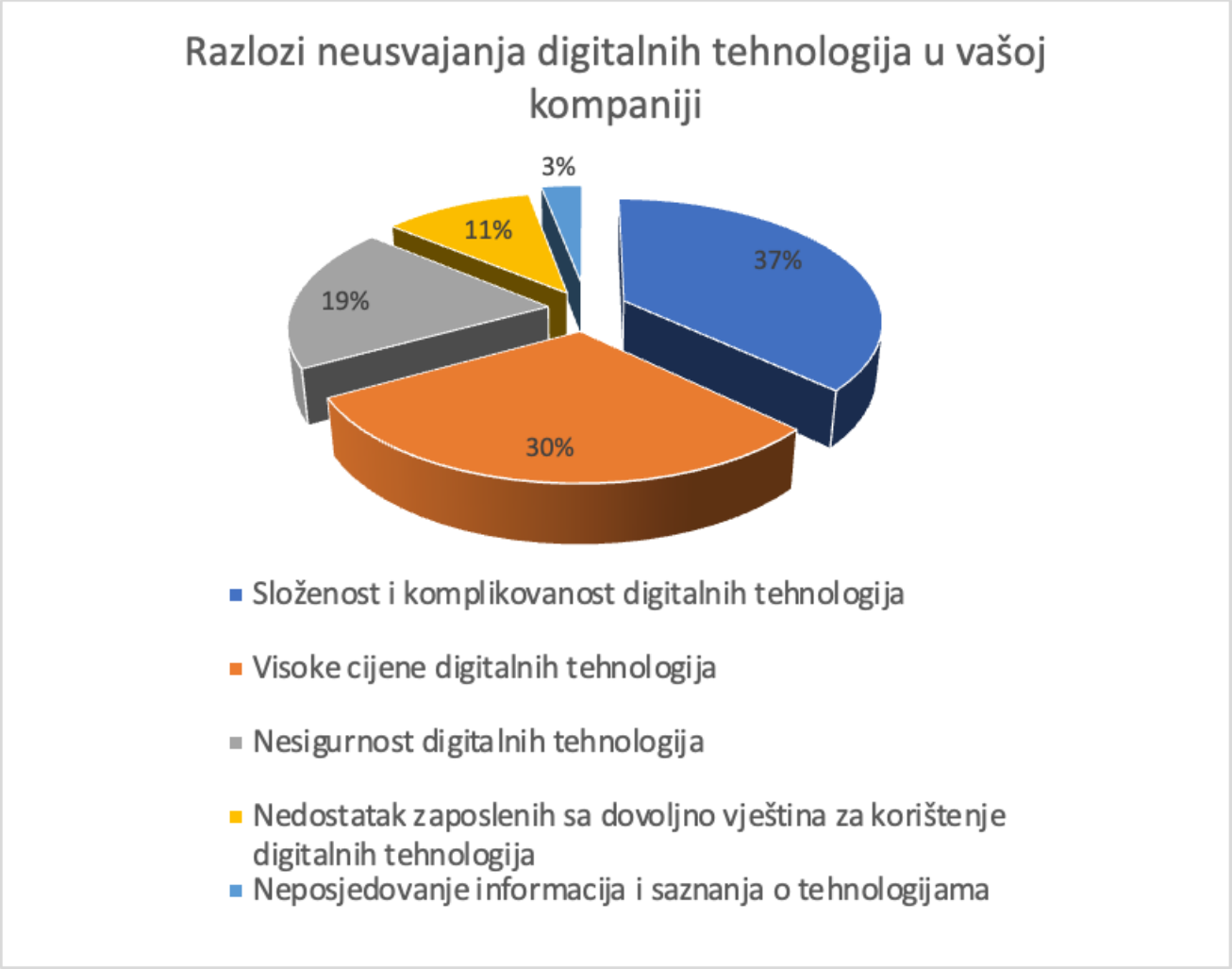
Menadžeri su istakli koji su to osnovni ciljevi njihovih kompanija kod usvajanja digitalnih tehnologija. Kao jedan od osnovnih ciljeva istaknuto je unapređenje konkurentnosti kompanije i poboljšanje usluga. Ove odgovore je dalo 40% ispitanika, odnosno 30% njih. Zatim slijede sljedeći ciljevi: unapređenje marketing strategije i oglašavanja (13%), unapređenje prodaje i bolje povezivanje s kupcima (9%) i unapređenje privatnosti zaštite podataka klijenata (8%).

Grafikon 2. Osnovni ciljevi vaših kompanija kod usvajanja digitalnih tehnologija

Izvor: Autor rada

Kompanije koje nisu usvojile digitalne tehnologije, navele su i razloge za to. Kao najčešće razloge za neusvajanje digitalnih tehnologija, menadžeri su naveli sljedeće: složenost i komplikovanost digitalnih tehnologija (37%), visoke cijene digitalnih tehnologija (30%), nesigurnost digitalnih tehnologija (19%). Nedostatak zaposlenih sa dovoljno vještina za korištenje digitalnih tehnologija je razlog koji je navelo 11% ispitanika. Najmanje važan razlog jeste neposjedovanje informacija i saznanja o tehnologijama koje bi se mogle koristiti (3% ispitanika).

Grafikon 3. Razlozi neusvajanja digitalnih tehnologija u vašoj kompaniji



Izvor: Autor rada

4.5.2. Korištenje aplikacija za pohranu u Cloudu

Grafikon 4 prikazuje vrste pohrane u Cloudu koje se koriste, na temelju prikupljenih podataka. Drop Box je najpopularniji, koristi ga 40,9% ispitanika, a slijedi ga Google Drive sa 30,8%. iCloud koristi 17,5% ispitanika, a My Drive njih 10,8%.

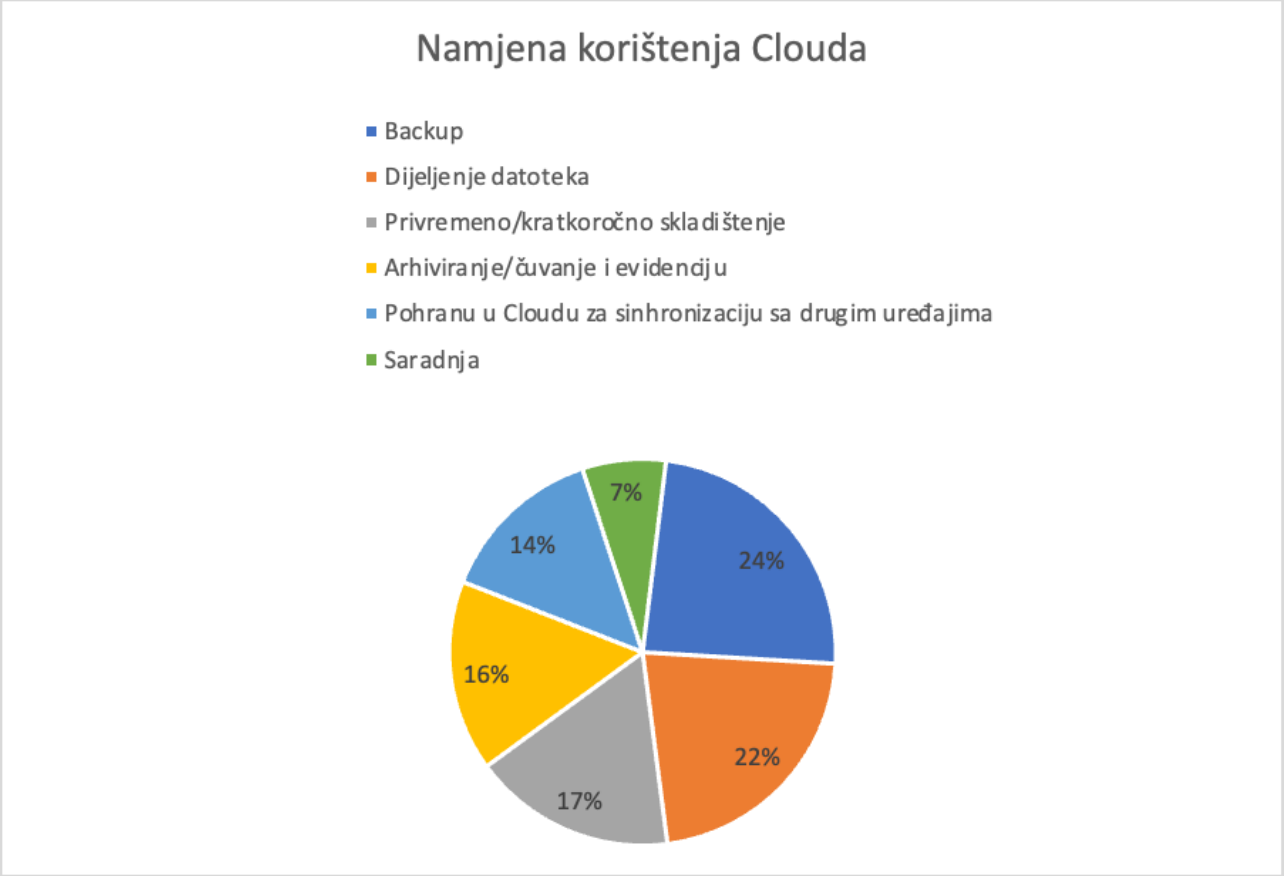
Grafikon 4. Vrste korištenih pohrana u Cloudu

Izvor: Autor rada

Budući da je kontrola ovih aplikacija na strani trećih strana gdje je kontrola korisnika svedena na minimum, nivo povjerenja korisnika je smanjen. Stoga je povjerenje važan aspekt koji treba uzeti u obzir u okruženju za pohranu u Cloudu, posebno zato što sigurnosne prijetnje rastu i čine pitanja sigurnosti i povjerenja najvažnijim pitanjima na koja se treba fokusirati, a koja su dosad samo djelimično riješena.

Za korištenje pohrane u Cloudu, Grafikon 5 pokazuje da 24% korisnika koristi za backup, a zatim 22% za dijeljenje datoteka. Za privremeno/kratkoročno skladištenje i arhiviranje/čuvanje i evidenciju se opredijelio približno isti broj ispitanika (17%, odnosno 16% njih). Nešto manje ispitanika (14%) koristi pohranu u Cloudu za sinhronizaciju sa drugim uređajima. Saradnja, s 7%, bila je najmanje popularna upotreba. Rezultati pokazuju da su dijeljenje datoteka i sinhronizacija s drugim uređajima značajno povezani s povjerenjem; utvrđeno je da druge svrhe nisu značajno povezane s povjerenjem.

Grafikon 5. Namjena korištenja Clouda

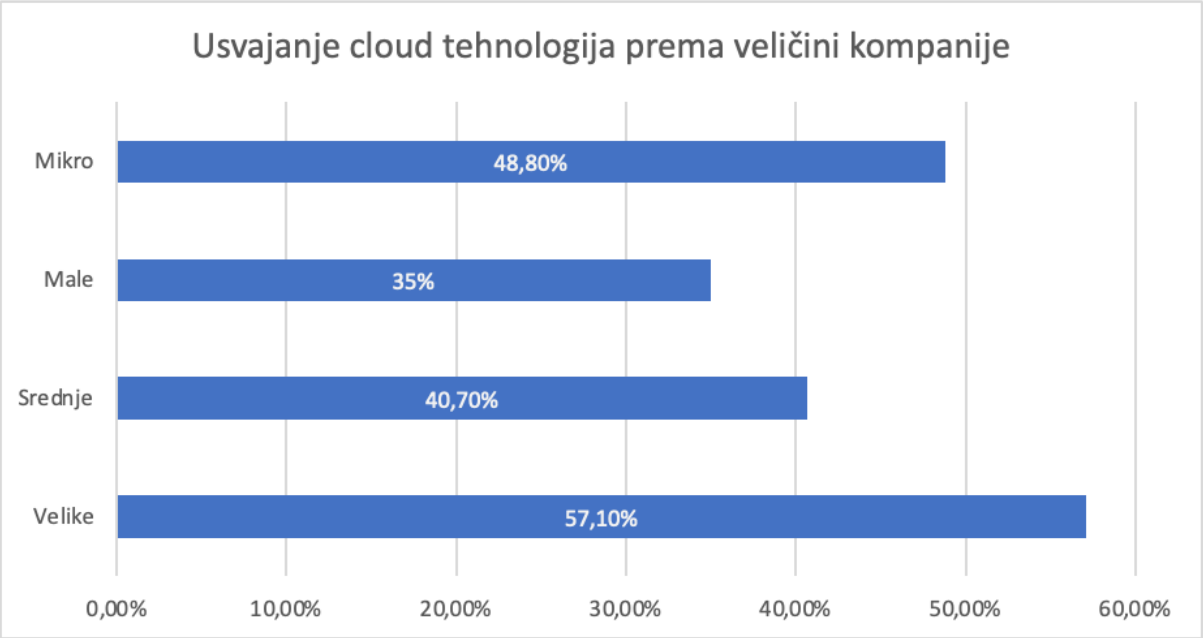


Izvor: Autor rada

U svjetlu rezultata prikazanih na Grafikonu 5, povjerenje u aplikacije za pohranu u Cloudu mora biti visoko, jer se uglavnom koristi u svrhe sigurnosnog kopiranja. Stoga je potrebno razmotriti neke mehanizme i faktore koji bi igrali ključnu ulogu u minimiziranju negativnih uočenih faktora, kao i za povećanje pozitivnog očekivanja prema većem povjerenju i usvajanju ovih aplikacija.

Velike kompanije su u najvećem procentu usvojile cloud tehnologije (57,1% njih), slijede ih mikro kompanije (48,8%), zatim srednje i male kompanije (40,7%, odnosno 35%). Navedeni rezultati pokazuju korištenje neke od cloud-baziranih tehnologija, ali ne i kupovinu barem jedne od usluga.

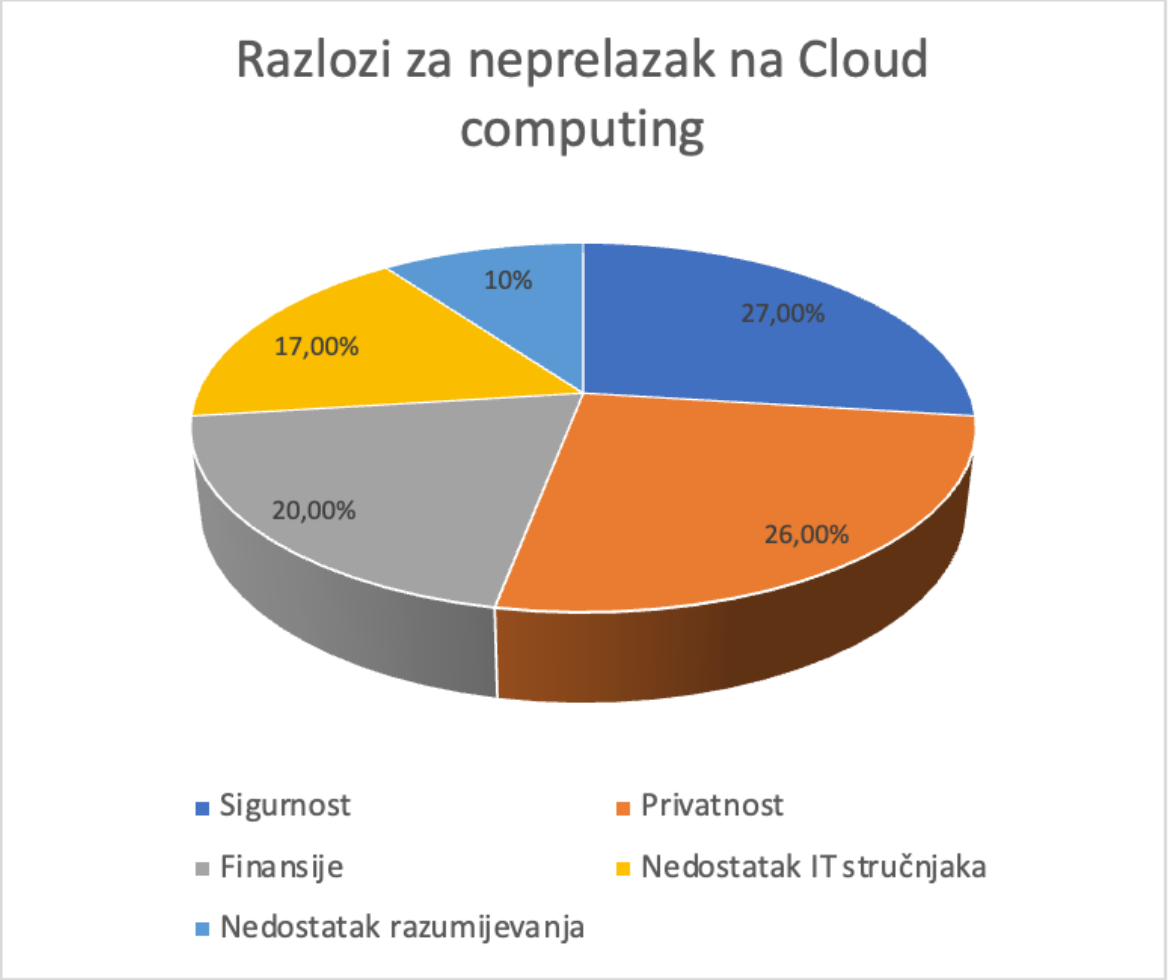
Grafikon 6. Usvajanje cloud tehnologija prema veličini kompanije



Izvor: Autor rada

S obzirom na razloge za neprelazak na Cloud computing, ispitanici su naveli da im je pitanje sigurnosti i privatnosti najvažnije (27% ispitanika ističe problem sigurnosti, a njih 26% problem privatnosti). Dodatno, finansije su razlog za neprelazak na Cloud kod 20% ispitanika, a nedostatk IT stručnjaka ističe 17% ispitanika. Najmanje važan razlog (10% ispitanika) neprelaska na Cloud je nedostatak razumijevanja.

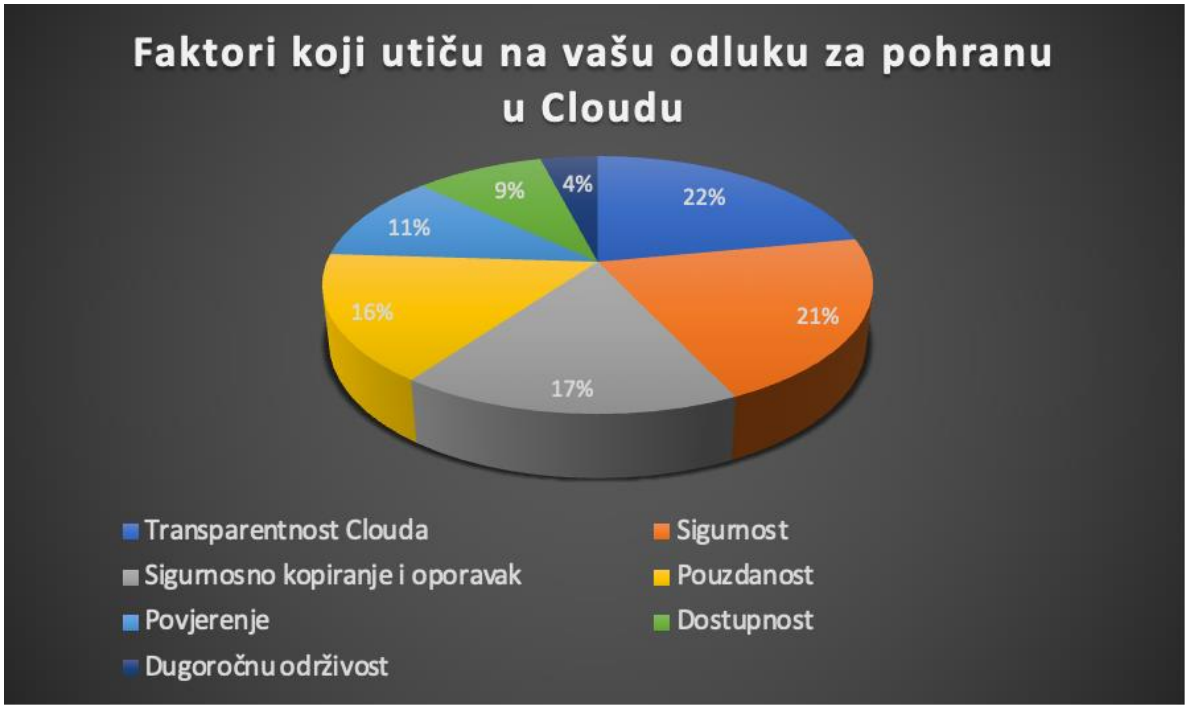
Grafikon 7. Razlozi za neprelazak na Cloud computing



Izvor: Autor rada

Kada je riječ o faktorima koji utiču na odluku za pohranu u Cloudu, ispitanici su se izjasnili na sljedeći način. Za transparentnost Clouda i sigurnost opredijelilo se najviše ispitanika (22%, odnosno 21%). Sigurnosno kopiranje i oporavak, te pouzdanost su faktori koje ističe 17%, odnosno 16% ispitanika. Zatim slijede povjerenje i dostupnost, za koje se odlučilo 11% ispitanika, odnosno 9% ispitanika. Kao najmanje važan faktor su istakli dugoročnu održivost (4% ispitanika).

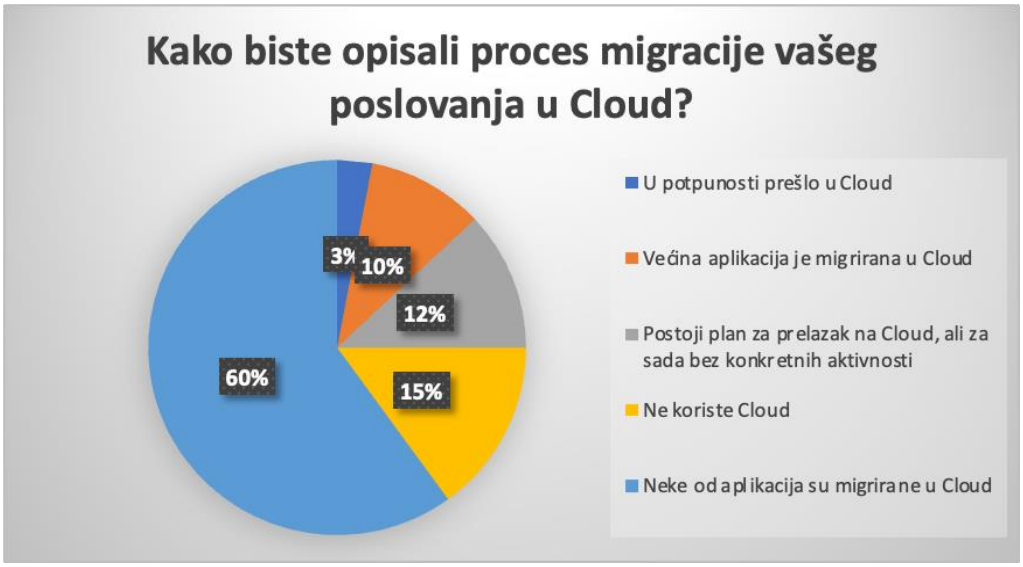
Grafikon 8. Faktori koji utiču na vašu odluku za pohranu u Cloudu



Izvor: Autor rada

Rezultati ankete pokazuju da je vrlo mali broj ispitanika u potpunosti prešao na Cloud – njih samo 3%, kao što je navedeno u Grafikonu 9. Dodatno, 10% ispitanika odgovorilo je da je većinu svojih aplikacija migriralo u Cloud. 15% ispitanika se izjasnilo da ne koristi usluge Clouda, a 12% je odgovorilo da postoji plan za prelazak na Cloud, ali za sada bez konkretnih aktivnosti. Dakle, 27% ispitanika je van Clouda, dok 60% njih ima samo neke od aplikacija migrirane u Cloud. Znatan broj ispitanika koristi Cloud kao „storage“ koji je besplatan prilikom korištenja određenih usluga e-pošte, kao što su usluge e-pošte od Microsoft i Google. Štaviše, povećan je broj korisnika Office 365, koji dobijaju značajnu količinu prostora za pohranu na OneDriveu kao dio paketa. Uglavnom, rezultati istraživanja govore o tome da velika većina ispitanika svoje poslovanje ne temelji na Cloudu, već u isto vrijeme postoje usluge migrirane u Cloud, prvenstveno referirajuće na e-mail.

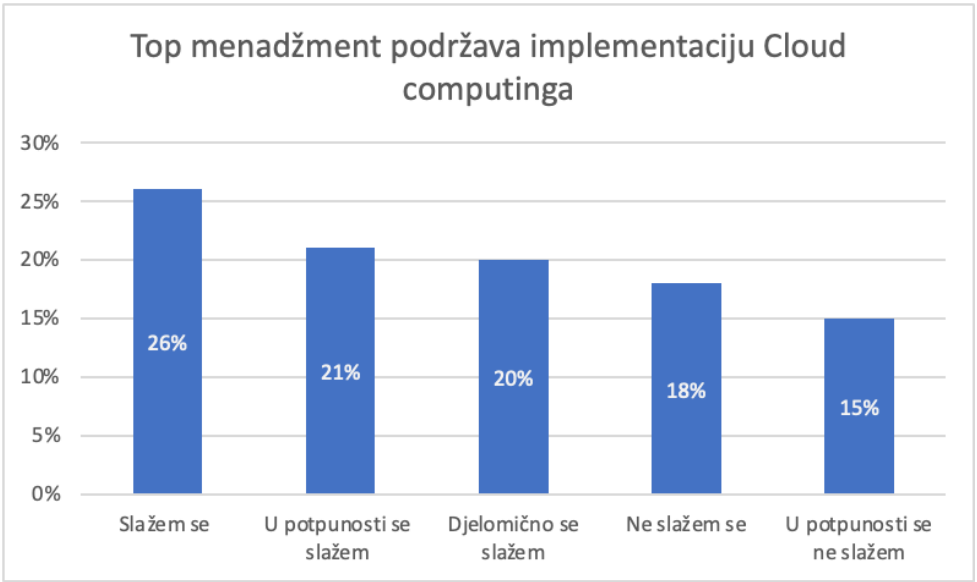
Grafikon 9. Kako biste opisali proces migracije vašeg poslovanja u Cloud?



Izvor: Autor rada

Na temelju rezultata istraživanja prikazanih na Grafikonu 10 može se zaključiti da značajan broj ispitanika podržava implementaciju Clouda. Uz adekvatnu obuku i analizu poslovanja preduzeća od strane konsultanata ili cloud pružatelja usluga, ispitanici bi bili voljni razmotriti opciju da pređu na Cloud (vjerovatno javni ili hibridni cloud).

Grafikon 10. Top menadžment podržava implementaciju Cloud computinga

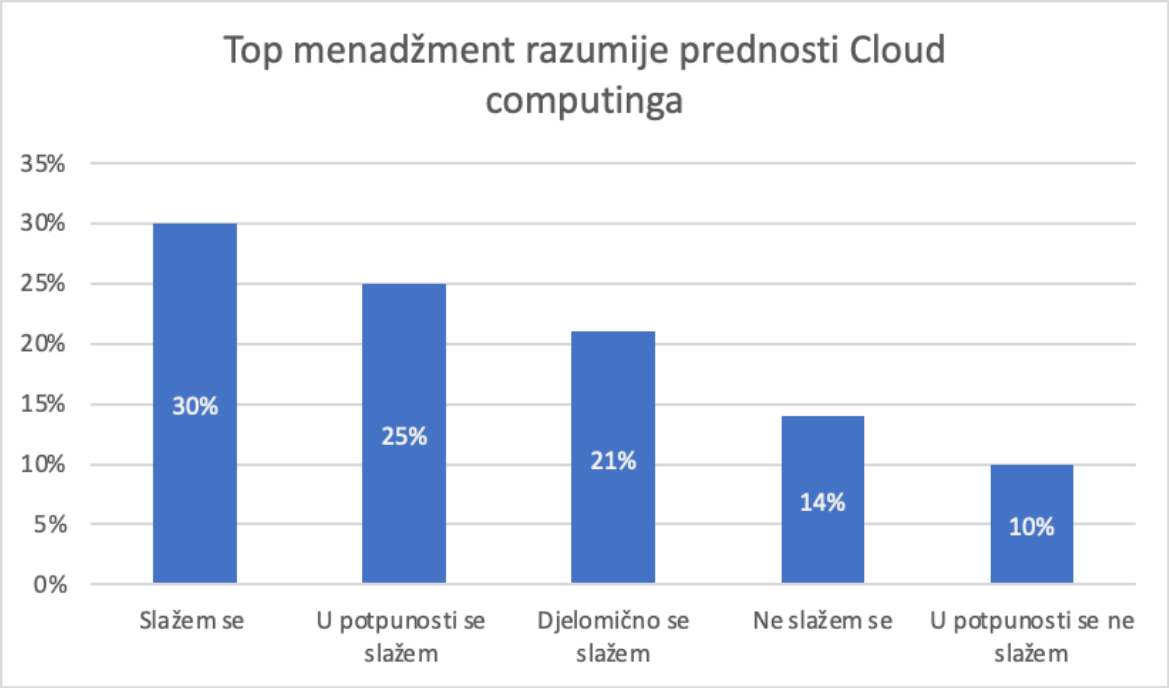


Izvor: Autor rada

Rezultati istraživanja prikazani na Grafikonu 11 pokazuju da značajan broj ispitanika još uvijek nema stav o prednostima i snagama Clouda, što znači da oni ne posjeduju potrebna

znanja u ovom segmentu. Analiza aktuelnih trendova u implementaciji tehnologije u BiH pokazuje da će u bliskoj budućnosti sve veći broj preduzeća migrirati u Cloud, pogotovo u slučajevima kada su potrebna značajna ulaganja za nabavu opreme. Istovremeno, moguće je uočiti povećanje troškova zapošljavanja odgovarajućih IT stručnjaka koji imaju znanje i iskustvo potrebno za implementaciju adekvatnih rješenja koja uključuju zadovoljavanje kratkoročnih i dugoročnih potreba preduzeća, koja u većini slučajeva implementiraju veći broj informacionih sistema s tendencijom za stalno poboljšanje.

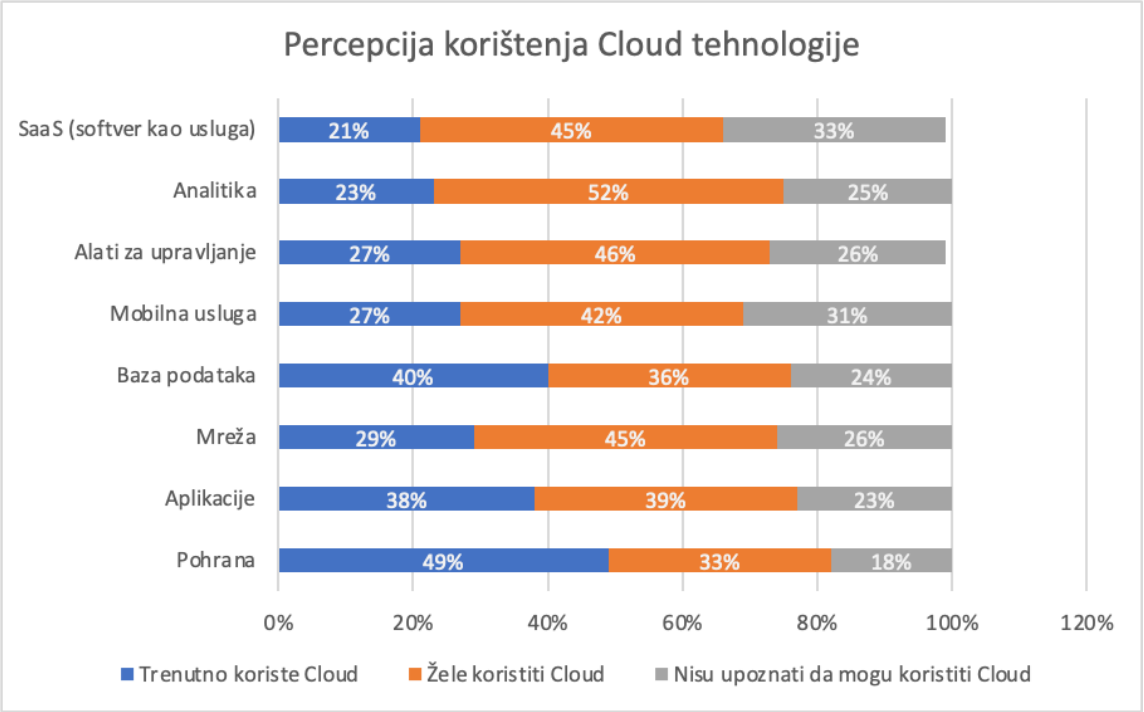
Grafikon 11. Top menadžment razumije prednosti Cloud computinga



Izvor: Autor rada

Sljedeći grafikon će prikazati nalaze istraživanja koja se odnose na percepciju korištenja Cloud tehnologije za osam različitih potencijalnih usluga, a rezultati istraživanja otkrivaju da visok procenat ispitanika ne koristi navedene usluge.

Grafikon 12. Percepcija korištenja Cloud tehnologije



Izvor: Autor rada

4.5.3. Testiranje hipoteza

Model regresijske analize u Tabeli 5 prikazuje dostupnost, dugoročnu održivost, sigurnosno kopiranje i oporavak i pouzdanost kao neovisne varijable, a sigurnost kao ovisnu varijablu, u skladu s hipotezama H1, H2, H3 i H5.

Tabela 5. Vrijednosti koeficijenta za regresijski model 1

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	.208	.315		.661	.510
	Dostupnost	.163	.074	.156	2.203	.029
	Dugoročna održivost	.090	.075	.095	1.200	.232
	Backup and Recovery	.147	.065	.170	2.245	.026
	Pouzdanost	.305	.075	.303	4.063	.000
a. Ovisna varijabla: Sigurnost						

Izvor: Autor rada

Tabela 5 pokazuje da sve neovisne varijable osim dugoročne održivosti imaju učinak na sigurnost, značajan na nivou P < 0,05. Model regresijske analize 2 u Tabeli 6 pokazuje da sigurnost i pouzdanost (neovisne varijable) imaju značajan učinak na povjerenje (ovisna varijabla) (P vrijednost < 0,05), odražavajući hipoteze H4 i H6.

Tabela 6. Vrijednosti koeficijenata za regresijski model 2

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
2	(Constant)	.566	.225		2.518	.013
	Sigurnost	.433	.061	.428	7.102	.000
	Pouzdanost	.440	.061	.432	7.165	.000

Izvor: Autor rada

Tabela 7 sažima ove rezultate iz SPSS-a, prema kojima se hipoteze prihvataju ili odbacuju.

Tabela 7. Sažetak rezultata hipoteze

Hipoteze	**Prihvata se/Odbacuje se**
H1: Dostupnost je pozitivno povezana sa sigurnošću u Cloud computingu.	**Prihvata se**
H2: Dugoročna održivost je pozitivno povezana sa sigurnošću u Cloud computingu.	**Odbacuje se**
H3: Backup i Recovery su pozitivno povezani sa sigurnošću u Cloud computingu.	**Prihvata se**
H4: Sigurnost je pozitivno povezana s povjerenjem korisnika Cloud computinga.	**Prihvata se**
H5: Pouzdanost je pozitivno povezana sa sigurnošću Cloud computinga.	**Prihvata se**
H6: Pouzdanost je pozitivno povezana sa povjerenjem korisnika Cloud computinga.	**Prihvata se**

Izvor: Autor rada

5. ZAKLJUČAK

Jedna od najvećih sigurnosnih briga s modelom Cloud computinga je dijeljenje resursa. Pružatelji usluga u Cloudu moraju obavijestiti svoje postojeće kupce o nivou sigurnosti koji pružaju na svom Cloudu. Pružatelji usluga u Cloudu trebaju edukovati potencijalne klijente o modelima implementacije Clouda kao što su javni, privatni i hibridni, zajedno s prednostima i nedostacima svakog od njih. Moraju pokazati svojim klijentima da osiguravaju odgovarajuće sigurnosne mjere koje će zaštititi podatke njihovih klijenata i izgraditi povjerenje za njihovu uslugu. Jedan od načina na koji to mogu postići je korištenje revizora treće strane. Potrebno je razviti nove sigurnosne tehnike i radikalno prilagoditi starije sigurnosne tehnike kako bi mogle raditi s arhitekturom Clouda. Uključivanje postojeće sigurnosne tehnologije neće funkcionisati jer ovaj novi model isporuke uvodi nove promjene u načinu pristupanja i korištenja računarskih resursa.

Cloud computing je nevjerovatna prilika za većinu preduzeća da fleksibilno reorganizuju svoju infrastrukturu, ali to ima i svoju cijenu. Iako, prema zadanim postavkama, sigurnost u Cloudu pruža mnogo veću sigurnost od lokalno hostiranih podataka, postoji mnogo toga što bi organizacija trebala uzeti u obzir prilikom postavljanja. Kao i većina sistema, Cloud computing nije bez svojih slabih tačaka. Većina povreda podataka rezultat je pogrešnih konfiguracija i loših kontrola autentifikacije. Važno je naglasiti da sigurnost u Cloudu nije zadana stvar. Mora se održavati visok status sigurnosti.

Zatim, postoji dosta ranjivosti koje bi haker mogao iskoristiti kada planira napad na naš Cloud. Mrežni administratori trebali bi biti u toku s najnovijim razvojem događaja u vezi s iskorištavanjem spremnika i biti vrlo oprezni u pogledu brisanja sigurnosnih kopija i drugih podataka. Samo pravovremenim rješavanjem različitih rizika u Cloudu moguće je stvoriti siguran model koji pomaže kompanijama da postignu svoje ciljeve. Za kompaniju je najvažnija sigurnost njihovih podataka, a u tom pogledu Cloud computing se istakao kao alat sa značajnom sigurnošću, a s obzirom da Cloud computing pruža redovne backup-ove, skoro da je nemoguće gubljenje podataka.

Posljednjih godina sve je više aplikacija za Cloud computing. Međutim, s ovim povećanjem postoje mnoge brige koje utiču na usvajanje ovih aplikacija. Jedan od njih je percipirano povjerenje korisnika. Ovo istraživanje istražuje faktore koji utiču na percipirano povjerenje u aplikacije temeljene na pohrani u Cloudu u Bosni i Hercegovini. U tu svrhu ovo je istraživanje slijedilo kvantitativni istraživački pristup gdje se glavna strategija istraživanja temelji na rezultatima upitnika. Putem upitnika, predloženi model testiran je na 178 ispitanika kako bi se identifikovali faktori koji utiču na njihovo povjerenje u aplikacije za pohranu u Cloudu. Rezultati su otkrili da sigurnost i pouzdanost direktno utiču na povjerenje korisnika u aplikacije za pohranu u Cloudu. U isto vrijeme sigurnosno kopiranje i oporavak, dostupnost i transparentnost u oblaku utiču na povjerenje indirektno kroz sigurnost. Doprinos ovog istraživanja sastoji se u predlaganju novog modela povjerenja korisnika u aplikacije Cloud computinga koji se može dodati modelima drugih istraživača u tom

području. Osim toga, rezultati ovog istraživanja pružaju uvid programerima aplikacija za Cloud computing prema boljem percipiranom povjerenju korisnika.

Ovo istraživanje mjeri faktore koji utiču na povjerenje korisnika u aplikacije za pohranu u Cloud computing u BiH. Kako bi se postigao ovaj cilj, predložen je istraživački model kombinovanjem različitih faktora identifikovanih iz pregleda literature: dostupnost, sigurnosno kopiranje i oporavak, dugoročna održivost, sigurnost i pouzdanost. Upitnik je podijeljen korisnicima aplikacija za pohranu u Cloud computing. Utvrđeno je da svi navedeni faktori osim jednog doprinose uticaju na nivo povjerenja korisnika u aplikaciju za pohranu podataka u Cloudu, izuzetak je dugoročna održivost. Stoga pouzdanost i sigurnost imaju direktan uticaj na povjerenje u aplikacije za pohranu u Cloudu, dok dostupnost, sigurnosno kopiranje i oporavak indirektno utiču na sigurnost. Ovi faktori, u kombinaciji sa sigurnošću, značajno utiču na povjerenje u aplikacije za pohranu u Cloudu.

Ovo istraživanje ima mnoga ograničenja koja se mogu uzeti u obzir za daljnje istraživanje. Na primjer, veličina uzorka je mala i potrebna je veća veličina uzorka prije bilo kakve generalizacije rezultata. Također, veći uzorak bi dao drugačiju perspektivu povjerenja i faktora koji na njega utiču.

Što se tiče postavljenih hipoteza, može se rezimirati sljedeće. Model regresijske analize 1 prikazuje dostupnost, dugoročnu održivost, sigurnosno kopiranje i oporavak, te pouzdanost kao neovisne varijable, a sigurnost kao ovisnu varijablu, u skladu sa hipotezama H1, H2, H3 i H5. Sve neovisne varijable, osim dugoročne održivosti, imaju učinak na sigurnost. Model regresijske analize 2 pokazuje da sigurnost i pouzdanost (neovisne varijable) imaju značajan učinak na povjerenje (ovisna varijabla), odražavajući hipoteze H4 i H6.

Na osnovu svega izloženog prihvataju se sljedeće hipoteze: H1: Dostupnost je pozitivno povezana sa sigurnošću u Cloud computingu; H3: Backup i Recovery su pozitivno povezani sa sigurnošću u Cloud computinga; H4: Sigurnost je pozitivno povezana sa povjerenjem korisnika Cloud computinga; H5: Pouzdanost je pozitivno povezana sa sigurnošću Cloud computinga; H6: Pouzdanost je pozitivno povezana sa povjerenjem korisnika Cloud computinga. Odbacuje se hipoteza H2: Dugoročna održivost je pozitivno povezana sa sigurnošću u Cloud computingu.

REFERENCE

1. Ahmad, S., et al. (2012). Trust Model: Cloud's Provider and Cloud's User. *International Journal of Advanced Science and Technology*, Vol. 44, str.69-79. Dostupno na: www.ebsco.com (pristupljeno: 20.06.2023. godine)

2. Almanea, M. I. (2014). CloudAdvisor – A Framework Towards Assessing the Trustworthiness and Transparency of Cloud Providers. UCC2014. *7th IEEE/ACM International Conference on Utility and Cloud Computing*, London, UK.

3. Armbrust, M., Fox, A., Griffith, R., Anthony D. J., Katz, R. H., Konwinski, A. (2009). Above the clouds: A berkeley view of cloud computing. *Technical Report, EECS Department*, University of California, Berkeley, str. 28. Dostupno na: www.ebsco.com (pristupljeno: 10.05.2023. godine)

4. Aymerich, F.M., Fenu, G., Surcis, S. (2008). An approach to a cloud computing network. *Applications of Digital Information and Web Technologies, ICADIWT*, str. 115. Dostupno na: www.doaj.org (pristupljeno: 15.05.2023. godine)

5. Balwinder, S., S. (2017). *Virtualization and Cloud Computing.* India: Ropar PB.

6. Bhaskar, P. R., Choi, E., Lumb, I. (2009). A taxonomy and survey of cloud computing systems. *Networked Computing and Advanced Information Management, International Conference*, str. 119. Dostupno na: www.ebsco.com (pristupljeno: 10.05.2023. godine)

7. Brumec, S. (2011). *Računalni oblaci kao dio servisno orjentisane arhitekture.* Zagreb: Sveučilište u Zagrebu.

8. Clark, C. et al. (2005). Live Migration of Virtual Machines. Proc. *2nd Conf. Symp. Networked Systems Design and Implementation,* Vol. 2, USENIX Association, str. 273–86. Dostupno na: www.ebsco.com (pristupljeno: 10.05.2023. godine)

9. Chen, S-L. *et.al.* (2013). Development of cloud virtualization technology and its application in manufacturing management system-a case study. *Proceeding of 2013 International Conference on Technology Innovation and Industrial Management*, Phuket, Thailand, str. 29. Dostupno na: www.ebsco.com (pristupljeno: 10.05.2023. godine)

10. Chowdhury, R.R. (2014). Security in Cloud Computing. *International Journal of Computer Applications, Vol. 96, No. 15*, str. 24-30. Dostupno na: www.doaj.org (pristupljeno: 15.06.2023. godine)

11. Darsi, M., Babu, D, V. and Darsi, G. (2014). *Addressing Trust Issues in Cloud Computing. International Journal of P2P Network Trends and Technology (IJPTT).*

12. Davidović, V. (2011). *Cloud computing: što s bazom podataka (u oblacima)?*, str. 1. Dostupno na: www.hrcak.srce.hr (pristupljeno: 10.05.2023. godine)

13. Dhiman, A., and Joshi, M. (2014). Analysis of Performance for Data Center under for Private Cloud through Cloud Computing. *International Journal of Engineering and Computer Science* (IIECS), Vol. 3, No. 6, str. 6422-6431. Dostupno na: www.doaj.org (pristupljeno: 15.06.2023. godine)

14. Shimba, F. (2010). *Cloud Computing: Strategies for Cloud Computing Adoption.* MSc Thesis. Dublin Inst. Technol.

15. Farber, D. (2010). *Defining Cloud Services and Cloud Computing.* CNET, str. 11. Dostupno na: www.doaj.org (pristupljeno: 20.05.2023. godine)

16. Gefen, D.; Karahanna, E., Straub, D.W. (2003). *Trust and TAM in Online Shopping: An Integrated Model. MIS Quarterly* 27.

17. Huang, J. and Nicol, D. (2013). Trust mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications Advances, Systems and Applications Vol. 2, No. 9*. Dostupno na: www.doaj.org (pristupljeno: 20.05.2023. godine)

18. 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 (pristupljeno: 25.06.2023. godine).

19. Benson, K., Dowsley, R., Shacham, H. (2011). Do you know where your cloud files are? *In Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, ACM.

20. Kalloniatis, C. (2016). Increasing Internet Users Trust in the Cloud Computing Era: The Role of Privacy. *J Mass Communication Journalism, Vol. 6, No. 3*, str. 2-5. Dostupno na: www.doaj.org (pristupljeno: 05.07.2023. godine)

21. Kalluri, R., Rao, C. V. G. (2014) *Adressing the Security, Privacy and Trust Challenges of Cloud Computing*.

22. Karnwal, T., Sivakumar, T., Aghila, G. (2011). *Cloud Services in Different Cloud Deployment Models: An Overview*. New York: Foundation of Computer Science.

23. Khan, K., Malluhi, Q. (2010). *Establishing trust in cloud computing. IT Prof* 2010, Vol. 12, No. 5, str. 20–27. Dostupno na: www.doaj.org (pristupljeno: 05.07.2023. godine)

24. King, R. (2010). Cloud Computing. *Bloomberg Business Week*, str. 12. Dostupno na: www.doaj.org (pristupljeno: 01.06.2023. godine)

25. Kretschmer, T. (2012). Information and Communication Technologies and Productivity Growth: A Survey of the Literature, *OECD Digital Economy Papers, No. 195*, OECD Publishing. Dostupno na: www.doaj.org (pristupljeno: 10.05.2023. godine)

26. Kumar, V., Chaisiri, S., i Ko, R. (2017). *Data Security in Cloud Computing*. Springer.

27. Alhamad, M., Dillon, T., Chang, E. (2011). A trust-evaluation metric for cloud applications. *Learning Comput., Vol. 1, No.4*, str. 416-421. Dostupno na: www.doaj.org (pristupljeno: 05.07.2023. godine)

28. Naehrig, M., Lauter, K., Vaikuntanathan, V. (2011). Can homomorphic encryption be practical? *In Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, pages.

29. Mayer, R., Davis, J., Schoorman,F. (1995). An Integrative Model of Organizational Trust: Past, Present, and Future. *Academic of Management Rev., Vol. 20, No. 3*, str. 709–734. Dostupno na: www.doaj.org (pristupljeno: 05.07.2023. godine)

30. Mikkilineni, R., Sarathy, V. (2009). Cloud Computing and the Lessons from the Past. *In Proceedings of the 18 th IEEE International Workshops Enabling Technologies.* The Netherlands.

31. Nicoletti, B. (2013). *Cloud Computing in Financial Services.* Palgrave Macmillan.

32. Ogigau-Neamtiu, F. (2012). Cloud computing security issues. *Journal of Defense Resources Management, Vol. 3, No. 2*, str. 141. Dostupno na: www.doaj.org (pristupljeno: 05.07.2023. godine)

33. Ogrizek, Biškupić, I., Banek, Z. M. (2014). *Web tehnologije.* Zagreb: Mate d.o.o.

34. Ohlman, B., Eriksson, A., Rembarz, R. (2009). What Networking of Information can do for Cloud Computing. *IEEE International Workshops on Enabling Technologies*, The Netherlands.

35. Paine, K. (2013). *Guidelines for Measuring Trust in Organizations.* Gainesville: University of Florida.

36. Pickavance, M., Nield, D. i DeMuro, J. P. (2021). *Box cloud storage review*. Dostupno na: https://www.techradar.com/reviews/box (pristupljeno: 15.07.2023. godine)

37. Potdar, A., Patil, P., Bagla, R., Pandey, R. (2015). Security Solutions for Cloud Computing. *International Journal of Computer Applications, Vol. 128, No. 16*, str. 17-21. Dostupno na: www.doaj.org (pristupljeno: 05.07.2023. godine)

38. Moreno, R., et al. (2013). Key Challenges in Cloud Computing: Enabling the Future Internet of Services. *IEEE Internet Computing*.

39. Radić, B. (2011). *Sigurnost u računarskom oblaku.* Zagreb: Sveučilište, str. 45. Dostupno na: www.hrcak.srce.hr (pristupljeno: 01.06.2023. godine)

40. Rajaraman, V. (2014). Cloud computing. *Resonance, Vol. 19, No.* 3, str. 242-258. Dostupno na: www.doaj.org (pristupljeno: 05.07.2023. godine)

41. Ramgovind, S., Eloff, M., Smith, E. (2010). The management of security in cloud computing. *In: The Proceedings of IEEE Conference on Information Security for South Africa*, 2-4 Aug. 2010, Johannesburg, South Africa, South Africa.

42. Rashidi, A., Movahhedinia, N. (2012). A Model for User Trust in Cloud Computing. *International Journal on Cloud Computing: Services and Architecture (*IJCCSA), Vol. 2, No. 2, str.1-8. Dostupno na: www.doaj.org (pristupljeno: 05.07.2023. godine)

43. Rathi, K., Kumari, S. (2015). Analyzing and Surveying Trust In Cloud Computing Environment. *Journal of Computer Engineering (IOSR-JCE), Vol. 17, No. 3*, str. 66-70. Dostupno na: www.doaj.org (pristupljeno: 15.07.2023. godine)

44. Rittinghouse, J. W., Ransome, J. F. (2010). *Cloud Computing, Implementation, Managment and Security.* CRC Press

45. Ritua, Randhawab, S., Jainc. S. (2017). Trust Models in Cloud Computing: A Review. *International Journal of Wireless and Microwave Technologies, Vol.* 7, *No. 4*, str. 14-27. Dostupno na: www.doaj.org (pristupljeno: 15.07.2023. godine)

46. Robinson, N.; Valeri, L., Cave, J. et al. (2010). *The Cloud: Understanding the Security, Privacy and Trust Challenges.* Report prepared for Unit F.5, Directorate-General Information Society and Media, European Commission.

47. Ryan, M.D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. *The Journal of Systems and Software, Vol. 86, No. 9.*

48. Sailaja, D., Usharani, P. (2017). Cloud Computing Security Issues, Challenges and its Solutions in Financial Sectors. *International Journal of Advanced Scientific Technologies, Engineering and Management Sciences*.

49. Srića, V., Spremić, M. (2000). *Informacijskom tehnologijom do poslovnog uspjeha.* Zagreb: Sinergija.

50. Srinivasan, M. (2012). Building a secure enterprise model for cloud computing environment. *Academy of Information and Management Sciences Journal, Vol. 15, No. 1, str. 127.* Dostupno na: www.doaj.org (pristupljeno: 15.07.2023. godine)

51. Staten, J. (2009). Is Cloud Computing Ready for the Enterprise? *Forrester Report*.

52. Subashini, S., Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, Vol. 34, No. 1, str. 1-11*. Dostupno na: www.ebsco.com (pristupljeno: 20.07.2023. godine)

53. Sun,D Chang, G., Sun,L., Wang,X. (2011). *Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments.*

54. Tomac, R. (2013). *Tehno – ekonomska analiza usluga zasnovanih na računarstvu u oblaku.* Zagreb: Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva.

55. Uikey, C., Bhilare, D. (2013). A Broker Based Trust Model for Cloud Computing. *International Journal of Emerging Technology and Advanced Engineering, Vol. 3, No. 11*, str. 247-252. Dostupno na: www.ebsco.com (pristupljeno: 20.07.2023. godine)

56. Uusitalo, I., Karppinen, K., Juhola, A., Savola, R. (2010). Trust and cloud services-an interview study. In Cloud Computing Technology and Science (CloudCom), *2010 IEEE Second International Conference on IEEE*.

57. Vaish, A., Kushwaha, A., Das, R. and Sharma, C. (2013). Data Location Verification in Cloud Computing. *International Journal of Computer Applications, Vol.* 68, No. 12, str.23-26. Dostupno na: www.ebsco.com (pristupljeno: 20.07.2023. godine)

58. Wheeler, A. i Winburn, M. (2015). *Cloud Storage Security*. A Practical Guide, Elsevier.

59. Whitney, L. (2020). *How to share files using Microsoft OneDrive*. Dostupno na: https://www.techrepublic.com/article/how-to-share-files-using-microsoft-onedrive/

60. Younis, Y. A., Kifayat, K., Merabti, M. (2014). An access control model for cloud computing. *Journal of Information Security and Applications, Vol. 19, No. 1*, str. 45-60. Dostupno na: www.ebsco.com (pristupljeno: 20.07.2023. godine)

61. Zissis, D., Lekkas, D. (2010). Addressing cloud computing security issues. *Future Generation Computer Systems, Vol. 28, No. 3*, str. 583-592. Dostupno na: www.ebsco.com (pristupljeno: 20.07.2023. godine)

62. http://opensourceforgeeks.blogspot.com/2015/01/difference-between-saas-paas-and-iaas.html (pristupljeno: 10.06.2023. godine)

63. https://info.focustsi.com/it-services-boston/resources/blog/cloud-computing-101-public-vs-private-clouds (pristupljeno: 10.05.2023. godine)

64. https://info.focustsi.com/it-services-boston/resources/blog/cloud-computing-101-public-vs-private-clouds (pristupljeno: 10.05.2023. godine)

65. https://www.stablenet.net/solutions/cloud-computing/hybrid-cloud/ (pristupljeno: 10.05.2023. godine)

66. www.datalab.ba/pantheon-cloud (pristupljeno: 15.09.2023. godine)

67. www.eline.ba (pristupljeno: 15.09.2023. godine)

68. www.logosoft.ba (pristupljeno: 15.09.2023. godine)

PRILOZI

Prilog 1

Poštovane/i,

Molimo Vas da izdvojite par minuta za anketu koja je potrebna radi istraživanja za magistarski rad na temu "Sigurnosni aspekti Cloud computinga".

Anketa je u potpunosti anonimna u smislu odavanja javnosti bilo kakvih ličnih podataka i odgovora. Prilikom odgovaranja na pitanja ankete molimo vas da dajete tačne i direktne odgovore kako bi dobili što preciznije rezultate. Podaci dobijeni ovim istraživanjem će biti korišteni isključivo u svrhu izrade naprijed navedenog naučno-istraživačkog rada, te u druge svrhe neće biti korišteni. U slučaju bilo kakvih nejasnoća molimo kontaktirati anketara.

Neizmjerno sam Vam zahvalna na učešću u ovom projektu,

Nejra Dervišević

i DEMOGRAFSKA PITANJA

1. Spol:

a) Muški

b) Ženski.

2. Nivo obrazovanja:

a) VŠS

b) Bachelor

c) Master

d) PhD

3. Broj zaposlenih u kompaniji

a) 1-9

b) 10-49

c) 50-249

d) 250 i više.

II NIVO DIGITALIZACIJE POSLOVANJA

1. Koje od sljedećih digitalnih tehnologija koristite u svom poslovanju?

a) Društveni mediji

b) Cloud tehnologije

c) Tehnologije za zaštitu od cyber kriminala

d) Robotika i automatizovane mašine

e) Big data i analitika podataka

f) Umjetna inteligencija.

2. Koji su bili osnovni ciljevi vaše kompanije kod usvajanja neke od digitalnih tehnologija?

a) Unapređenje privatnosti i zaštite podataka klijenta

b) Unapređenje prodaje i bolje povezivanje s kupcima

c) Unapređenje marketing strategije i oglašavanja

d) Unapređenje konkurentnosti kompanije

e) Poboljšanje usluge.

3. Ako u svom poslovanju niste usvojili ništa od digitalnih tehnologija, navedite razloge.

a) Digitalne tehnologije su preskupe

b) Digitalne tehnologije su previše složene i komplikovane

c) Digitalne tehnologije su nesigurne

d) Nedostatak zaposlenih sa dovoljno vještina za korištenje digitalnih tehnologija

e) Nemamo informacija i saznanja o tehnologijama koje bi mogli koristiti.

III CLOUD COMPUTING

1. Vrste korištenih pohrana u Cloudu:

a) iCloud

b) My Drive

c) Google Drive

d) Drop Box.

2. Namjena korištenja:

a) Privremeno / kratkoročno skladištenje

b) Sigurnosna kopija

c) Saradnja

d) Arhiviranje / čuvanje i evidencija

e) Dijeljenje datoteka

f) Sinhronizacija s drugim uređajima

3. Usvajanje Cloud tehnologije prema veličini kompanije:

a) Velike kompanije

b) Mikro kompanije

c) Srednje kompanije

d) Male kompanije

4. Razlozi za neprelazak na Cloud Computing

a) Nedostatak IT stručnjaka

b) Nedostatak razumijevanja

c) Finansije

d) Pitanje sigurnosti

e) Pitanje privatnosti.

5. Koji faktori utiču na vašu odluku za pohranu u Cloudu?

    a) Dostupnost

    b) Sigurnosno kopiranje i oporavak

    c) Sigurnost

    d) Dugoročna održivost

    e) Transparentnost Clouda

    f) Pouzdanost

    g) Povjerenje.

6. Kako biste opisali proces migracije vašeg poslovanja u Cloud?

a) Ne koristimo Cloud

b) Postoji plan za prelazak na Cloud ali za sada bez konkretnih aktivnosti

c) Neke od aplikacija su premještene u Cloud

d) Većina aplikacija je migrirana u Cloud

e) Kompanija je u potpunosti migrirala u Cloud.

7. Top menadžment podržava implementaciju Cloud computing:

a) U potpunosti se ne slažem

b) Ne slažem se

c) Djelimično se slažem

d) Slažem se

e) U potpunosti se slažem.

8. Top menadžment razumije prednosti Cloud Computinga:

a) U potpunosti se ne slažem

b) Ne slažem se

c) Djelimično se slažem

d) Slažem se

e) U potpunosti se slažem.

9. Percepcija korištenja Cloud computinga

a) Skladištenje

b) Aplikacije

c) Mreža

d) Baza podataka

e) Mobilne usluge

f) Alati za upravljanje

g) Analitika

h) SaaS (sowter-as-a-service).