Sigurnosni aspekti optimizacije mrežnih resursa na računalnom oblaku

Žalac, Filip

Sveučilište Jurja Dobrile u Puli

FAKULTET INFORMATIKE

Filip Žalac

SIGURNOSNI ASPEKTI OPTIMIZACIJE MREŽNIH RESURSA NA RAČUNALNOM OBLAKU

ZAVRŠNI RAD

Pula, 2024.

Sveučilište Jurja Dobrile u Puli

FAKULTET INFORMATIKE

Filip Žalac

SIGURNOSTI ASPEKTI OPTIMIZACIJE MREŽNIH RESURSA NA RAČUNALNOM OBLAKU

ZAVRŠNI RAD

JMBAG: 0303094475, redoviti student

Studijski smjer: Informatika

Kolegij: Računalne mreže

Mentor: izv. prof. dr. sc. Siniša Sovilj

Pula, listopad 2024.

IZJAVA O AKADEMSKOJ ČESTITOSTI

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

Student:

_____

U Puli, 9. listopada 2024.

IZJAVA O KORIŠTENJU AUTORSKOG DJELA

Ja, Filip Žalac, dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod naslovom „Sigurnosni aspekti optimizacije mrežnih resursa na računalnom oblaku“ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu sa Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, 9. listopada 2024.

Student:

_____

SADRŽAJ

SAŽETAK

Sigurnosti aspekti optimizacije mrežnih resursa na računalnom oblaku

Računalni oblak predstavlja suvremenu tehnologiju koja omogućuje fleksibilno i skalabilno korištenje računalnih resursa putem interneta, ali istovremeno donosi niz sigurnosnih prijetnji kao što su neovlašteni pristup, korupcija podataka te usklađivanje sa zakonskim i regulatornim okvirima. Glavni cilj rada je istražiti metode i prakse zaštite podataka, kontrolu pristupa, te tehničke i pravne izazove s kojima se organizacije suočavaju prilikom optimizacije mrežnih resursa u oblačnim okruženjima. Rad analizira kako optimizacija mrežnih resursa poput balansiranja opterećenja i dinamičkog dodjeljivanja resursa može povećati sigurnosne rizike, osobito u kontekstu zaštite osjetljivih podataka. U radu su također predložene mjere za poboljšanje sigurnosti, uključujući enkripciju podataka, višefaktorsku autentifikaciju (MFA), upravljanje enkripcijskim ključevima i kontrolu pristupa temeljenog na ulogama. Doprinos rada leži u njegovom holističkom pristupu sigurnosti u računalnim oblacima, koji integrira tehničke, pravne i organizacijske mjere zaštite. Predložene sigurnosne strategije temeljene su na aktualnim istraživanjima i primjerima dobre prakse, što ih čini primjenjivima u različitim industrijama. Rad također istražuje usklađenost sa sigurnosnim standardima i zakonima poput GDPR-a, te pruža smjernice za organizacije kako bi se osigurala usklađenost i maksimalna zaštita podataka. Ovaj rad doprinosi boljem razumijevanju sigurnosnih izazova u optimizaciji mrežnih resursa te nudi konkretne prijedloge za unapređenje sigurnosnih praksi u oblačnim okruženjima.

Ključne riječi: *računalni oblak, sigurnost, optimizacija*

ABSTRACT

Security aspects of network resource optimization in cloud computing

The computer cloud represents a modern technology that enables flexible and scalable use of computer resources via the Internet, but at the same time brings a number of security threats such as unauthorized access, data corruption, and compliance with legal and regulatory frameworks. The main goal of the paper is to investigate the methods and practices of data protection, access control, and technical and legal challenges that organizations face when optimizing network resources in cloud environments. The paper analyzes how optimization of network resources such as load balancing and dynamic resource allocation can increase security risks, especially in the context of protecting sensitive data. The paper also proposed measures to improve security, including data encryption, multi-factor authentication (MFA), encryption key management, and role-based access control. The paper's contribution lies in its holistic approach to cloud security, which integrates technical, legal and organizational safeguards. The proposed security strategies are based on current research and examples of good practice, which makes them applicable in different industries. The paper also explores compliance with security standards and laws such as GDPR, and provides guidance for organizations to ensure compliance and maximum data protection. This work contributes to a better understanding of security challenges in the optimization of network resources and offers concrete proposals for improving security practices in cloud environments.

Keywords: *computer cloud, security, optimization*

1. UVOD

Računalni oblak predstavlja jednu od najvažnijih inovacija u području informacijske tehnologije, omogućujući pristup velikim količinama podataka i računalnim resursima putem interneta. Međutim, optimizacija mrežnih resursa u ovom kontekstu donosi niz sigurnosnih prijetnji, uključujući rizik od neovlaštenog pristupa podacima, korupcije podataka te poteškoća u usklađivanju sa sigurnosnim standardima. Ovaj rad istražuje ove sigurnosne aspekte, s posebnim naglaskom na metode zaštite podataka, kontrolu pristupa i usklađenost s regulatornim zahtjevima, te nudi prijedloge za optimizaciju sigurnosnih postupaka u oblačnim okruženjima.

1.1. Predmet i cilj rada

Predmet ovog završnog rada je istraživanje sigurnosnih aspekata optimizacije mrežnih resursa na računalnom oblaku. U kontekstu sve većeg korištenja oblačnih tehnologija u poslovnim i privatnim sektorima, tema sigurnosti postaje iznimno važna. Računalni oblaci omogućuju organizacijama fleksibilan i skalabilan pristup računalnim resursima putem interneta, no s tim dolazi i niz sigurnosnih rizika koji mogu ugroziti povjerljivost, integritet i dostupnost podataka. Ključni predmet istraživanja uključuje analizu načina na koje se mrežni resursi optimiziraju unutar oblaka te kako ta optimizacija može utjecati na sigurnost podataka i sustava. Optimizacija mrežnih resursa, kao što su balansiranje opterećenja i dinamičko dodjeljivanje resursa, može otvoriti nove sigurnosne ranjivosti, osobito kada se radi o osjetljivim podacima i kritičnim sustavima. Kroz ovu analizu, rad istražuje tehničke, pravne i organizacijske izazove koje donosi uporaba računalnih oblaka.

Cilj ovog rada je detaljno analizirati i identificirati ključne sigurnosne prijetnje koje se pojavljuju u procesu optimizacije mrežnih resursa u oblačnom okruženju. Cilj je također istražiti najbolje prakse i metode za zaštitu podataka u oblaku, kao i predložiti mjere koje organizacije mogu primijeniti kako bi unaprijedile sigurnost svojih sustava. Posebna pažnja posvećena je temama kao što su povjerljivost podataka, integritet, kontrola

pristupa te usklađenost s regulatornim okvirima kao što su propisi o zaštiti osobnih podataka. Kroz teoretsku analizu i primjere iz prakse, rad nastoji pružiti holistički pristup sigurnosti u oblaku, integrirajući tehničke mjere s organizacijskim politikama. Na taj način, ovaj rad doprinosi boljem razumijevanju sigurnosnih izazova i rješenja u dinamičnom i složenom oblačnom okruženju, s ciljem osiguranja povjerljivosti i dostupnosti podataka uz istovremeno optimiziranje korištenja resursa.

1.2. Problem rada

Računalni oblak predstavlja revolucionarni korak u razvoju informacijske tehnologije, omogućujući organizacijama i pojedincima pristup velikim količinama podataka i računalnim resursima putem interneta. Međutim, optimizacija mrežnih resursa u ovom okruženju donosi niz sigurnosnih izazova koji mogu imati dalekosežne posljedice za privatnost, integritet podataka i cjelokupno poslovanje.

Jedan od ključnih problema istraživanja je osiguravanje povjerljivosti podataka u računalnom oblaku. Organizacije koje koriste oblak često pohranjuju osjetljive informacije, uključujući poslovne tajne, osobne podatke klijenata i druge kritične informacije. Optimizacija mrežnih resursa, poput balansiranja opterećenja i dinamičkog dodjeljivanja resursa, može izložiti te podatke riziku od neovlaštenog pristupa. Na primjer, kada se resursi automatski preusmjeravaju ili repliciraju između različitih podatkovnih centara, postoji mogućnost da podaci budu presretnuti ili pristupni od strane zlonamjernih korisnika.

Drugi važan aspekt je integritet podataka. U okruženju gdje se resursi dinamički alociraju i redistribuiraju, postoji rizik od korupcije podataka ili gubitka podataka zbog tehničkih grešaka, neodgovarajućih sigurnosnih politika ili zlonamjernih napada. Istraživanje sigurnosnih aspekata optimizacije mrežnih resursa mora uključivati razvoj robusnih metoda za zaštitu podataka od takvih prijetnji, kao i implementaciju sustava za brzo otkrivanje i oporavak od potencijalnih incidenata.

Još jedan ključni izazov je usklađenost sa sigurnosnim standardima i propisima. Mnoge industrije, poput financijske i zdravstvene, podliježu strogim propisima o zaštiti podataka.

Optimizacija mrežnih resursa u računalnom oblaku mora se provoditi u skladu s tim propisima kako bi se izbjegle pravne sankcije i gubitak povjerenja klijenata. Ovo zahtijeva detaljnu analizu pravnog okvira i integraciju sigurnosnih mjera koje su u skladu s relevantnim zakonodavstvom.

Osim toga, istraživanje sigurnosnih aspekata obuhvaća i upravljanje identitetima i pristupom u oblaku. U okruženju koje je toliko dinamično kao oblak, kontrola pristupa i autentifikacija korisnika postaju sve složeniji. Optimizacija mrežnih resursa može otežati praćenje i upravljanje korisničkim pristupom, što može dovesti do sigurnosnih propusta. Potrebno je razviti napredne metode autentifikacije i autorizacije koje mogu pratiti promjene u mrežnim resursima i osigurati da samo ovlašteni korisnici imaju pristup potrebnim informacijama.

Istraživanje sigurnosnih aspekata optimizacije mrežnih resursa na računalnom oblaku mora uzeti u obzir i prijetnje od vanjskih napada, poput DDoS (Distributed Denial of Service) napada. Ovi napadi mogu ciljati optimizacijske mehanizme, preopterećujući resurse i uzrokujući smanjenje performansi ili potpunu nedostupnost usluga. Razvoj učinkovitih strategija za detekciju i prevenciju takvih napada ključan je za održavanje sigurnosti i pouzdanosti računalnog oblaka. Sve navedene sigurnosne prijetnje zahtijevaju holistički pristup istraživanju, koji će kombinirati tehničke, pravne i organizacijske aspekte kako bi se osigurala cjelovita zaštita mrežnih resursa u računalnom oblaku.

1.3. Doprinos rada

Doprinos ovog rada leži u njegovom cjelovitom pristupu analizi sigurnosnih aspekata optimizacije mrežnih resursa na računalnom oblaku, s naglaskom na praktične implikacije i konkretne preporuke za poboljšanje sigurnosnih praksi. Kroz detaljnu analizu postojećih izazova, rad obuhvaća različite sigurnosne dimenzije koje su ključne za organizacije koje koriste računalne oblake. Prvo, rad pruža temeljit pregled tehničkih mehanizama optimizacije, kao što su balansiranje opterećenja i dinamička dodjela resursa, i povezuje ih s potencijalnim sigurnosnim rizicima koji proizlaze iz tih

mehanizama. Na taj način, rad omogućuje dublje razumijevanje kako tehničke odluke o optimizaciji mogu utjecati na sigurnost, što je od ključne važnosti za organizacije koje se oslanjaju na oblak u svakodnevnom poslovanju.

Jedan od značajnih doprinosa ovog rada je usmjeravanje pažnje na integraciju sigurnosnih mjera u procese optimizacije, čime se predlaže da se sigurnost ne promatra kao zasebni aspekt, već kao integralni dio svakog koraka u upravljanju mrežnim resursima. Rad predlaže konkretne mjere za unapređenje sigurnosnih praksi, kao što su implementacija naprednih metoda autentifikacije i autorizacije, enkripcija podataka te kontrola pristupa temeljenog na ulogama (Role-Based Access Control). Posebno su značajni prijedlozi za primjenu višefaktorske autentifikacije (MFA) i upravljanje enkripcijskim ključevima, koji su ključni za zaštitu povjerljivih podataka u dinamičnom okruženju računalnog oblaka. Ove preporuke temeljene su na aktualnim istraživanjima i primjerima dobre prakse, što ih čini primjenjivima u različitim poslovnim i tehnološkim kontekstima.

1.4. Struktura rada

Ovaj rad sastavljen je od pet dijelova. Prvi dio rada čini uvod u kojem se definira predmet istraživanja te postavljaju ciljevi rada. U ovom dijelu naglašava se važnost optimizacije mrežnih resursa u računalnim oblacima, uz navođenje sigurnosnih izazova koji prate ove procese. Također, uvod postavlja temelje za daljnje istraživanje, objašnjavajući ključne pojmove i metode koje će se koristiti kroz rad.

Drugi dio rada bavi se teoretskim okvirom i pregledom literature. Ovdje su prikazani temeljni pojmovi vezani za računalne oblake, mrežne resurse te optimizaciju. Poseban naglasak stavljen je na sigurnosne rizike koji se javljaju prilikom optimizacije, kao što su neovlašteni pristup, kompromitacija podataka te usklađenost sa sigurnosnim standardima. Pregled literature uključuje najnovija istraživanja i pristupe u ovom području, što čitatelju omogućuje dublje razumijevanje problematike i postojećih rješenja.

Treći dio rada posvećen je detaljnoj analizi problema i prijedlogu rješenja. U ovom dijelu razmatraju se različite tehnike optimizacije mrežnih resursa, poput balansiranja opterećenja, dinamičkog dodjeljivanja resursa i virtualizacije. Svaka od tih tehnika detaljno je analizirana u kontekstu sigurnosnih izazova koje donosi. Osim tehničkih analiza, ovaj dio uključuje i raspravu o zakonskim i regulatornim okvirima, kao što su GDPR i drugi relevantni propisi, čija usklađenost je ključna za sigurnost podataka u oblaku.

Četvrti dio rada odnosi se na prijedlog konkretnih sigurnosnih mjera i najboljih praksi. Ovdje se razmatraju metode kao što su enkripcija podataka, višefaktorska autentifikacija (MFA), te upravljanje identitetima i pristupom u oblačnim sustavima. Naglasak je na primjeni tih mjera u realnim situacijama, s ciljem zaštite podataka od potencijalnih prijetnji i sigurnosnih ranjivosti. Rad predlaže integraciju sigurnosnih procedura unutar procesa optimizacije kako bi se osiguralo da sigurnost bude sastavni dio svake faze optimizacije mrežnih resursa.

Posljednji, peti dio rada je zaključak, u kojem se sumiraju ključni nalazi i doprinosi rada. Zaključak naglašava važnost kontinuirane analize i unaprjeđenja sigurnosnih mjera u oblačnim okruženjima te pruža smjernice za buduća istraživanja. Rad završava prijedlozima za daljnje unapređenje sigurnosnih praksi, kako bi organizacije mogle još efikasnije koristiti računalne oblake, uz istovremeno održavanje visoke razine sigurnosti i usklađenosti s regulatornim okvirima.

2. RAČUNALNI OBLACI

Računalni oblaci (eng. cloud computing) postali su jedan od ključnih elemenata modernih informatičkih sustava. Koncept računalnih oblaka omogućava korisnicima pristup računalnim resursima putem interneta bez potrebe za fizičkim posjedovanjem ili održavanjem vlastitih servera ili infrastrukture. Ova tehnologija omogućava organizacijama i pojedincima fleksibilnost u korištenju resursa, jer se pristup može prilagoditi specifičnim potrebama korisnika. Računalni oblaci omogućuju korištenje različitih vrsta usluga kao što su pohrana podataka, obrada podataka i izvođenje softverskih aplikacija. Te usluge obično dolaze u tri osnovna oblika: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) i Software as a Service (SaaS). IaaS omogućava korisnicima da iznajmljuju osnovnu infrastrukturu, poput virtualnih servera i mrežne pohrane, dok PaaS nudi platformu na kojoj korisnici mogu razvijati, testirati i implementirati aplikacije bez brige o osnovnoj infrastrukturi. SaaS omogućava korisnicima pristup softverskim aplikacijama putem weba, što je često vrlo korisno za tvrtke koje trebaju rješenja poput alata za suradnju, računovodstvo ili upravljanje projektima.

Jedna od glavnih prednosti računalnih oblaka je njihova skalabilnost. Organizacije mogu lako povećati ili smanjiti korištenje resursa prema potrebi, što omogućuje fleksibilnije poslovanje i optimalno korištenje financijskih sredstava. Uz to, računalni oblaci omogućuju brzu implementaciju novih usluga i aplikacija, što je posebno važno u dinamičnom poslovnom okruženju gdje su promjene česte i brze. Računalni oblaci također igraju ključnu ulogu u razvoju novih tehnologija kao što su Internet of Things (IoT), umjetna inteligencija i analiza podataka. Ove tehnologije često zahtijevaju ogromne količine podataka i računalne snage, što računalni oblaci mogu osigurati bez velikih početnih ulaganja u infrastrukturu. Na primjer, kompanije mogu analizirati velike količine podataka koristeći oblak, što omogućuje bolje donošenje poslovnih odluka temeljenih na detaljnim analizama.

U obrazovnom sektoru, računalni oblaci omogućuju nastavnicima i učenicima pristup različitim edukativnim alatima i resursima bez obzira na njihovu lokaciju. Ovaj pristup ne samo da povećava dostupnost obrazovanja, već također olakšava kolaboraciju između učenika i nastavnika. Također, mnoge obrazovne ustanove koriste oblak za pohranu podataka, olakšavajući tako pristup informacijama na jednostavan i učinkovit način.

S obzirom na sve veću digitalizaciju poslovnih procesa, računalni oblaci postaju nezamjenjivi alat u svakodnevnom poslovanju. Različiti industrijski sektori, od financija do zdravstva, oslanjaju se na računalne oblake kako bi optimizirali svoje operacije, smanjili troškove i povećali produktivnost. Cloud tehnologija također omogućuje rad na daljinu, što je posebno postalo važno u vrijeme pandemije kada su mnoge tvrtke prešle na rad od kuće. Računalni oblaci predstavljaju temelj za daljnji tehnološki napredak. Korištenje oblaka omogućuje tvrtkama da budu agilnije i prilagodljivije promjenama na tržištu. Ova tehnologija omogućuje jednostavno prilagođavanje novim poslovnim potrebama, smanjenje složenosti IT infrastrukture i pruža tvrtkama mogućnost fokusiranja na svoj osnovni posao umjesto na tehničke aspekte IT sustava.

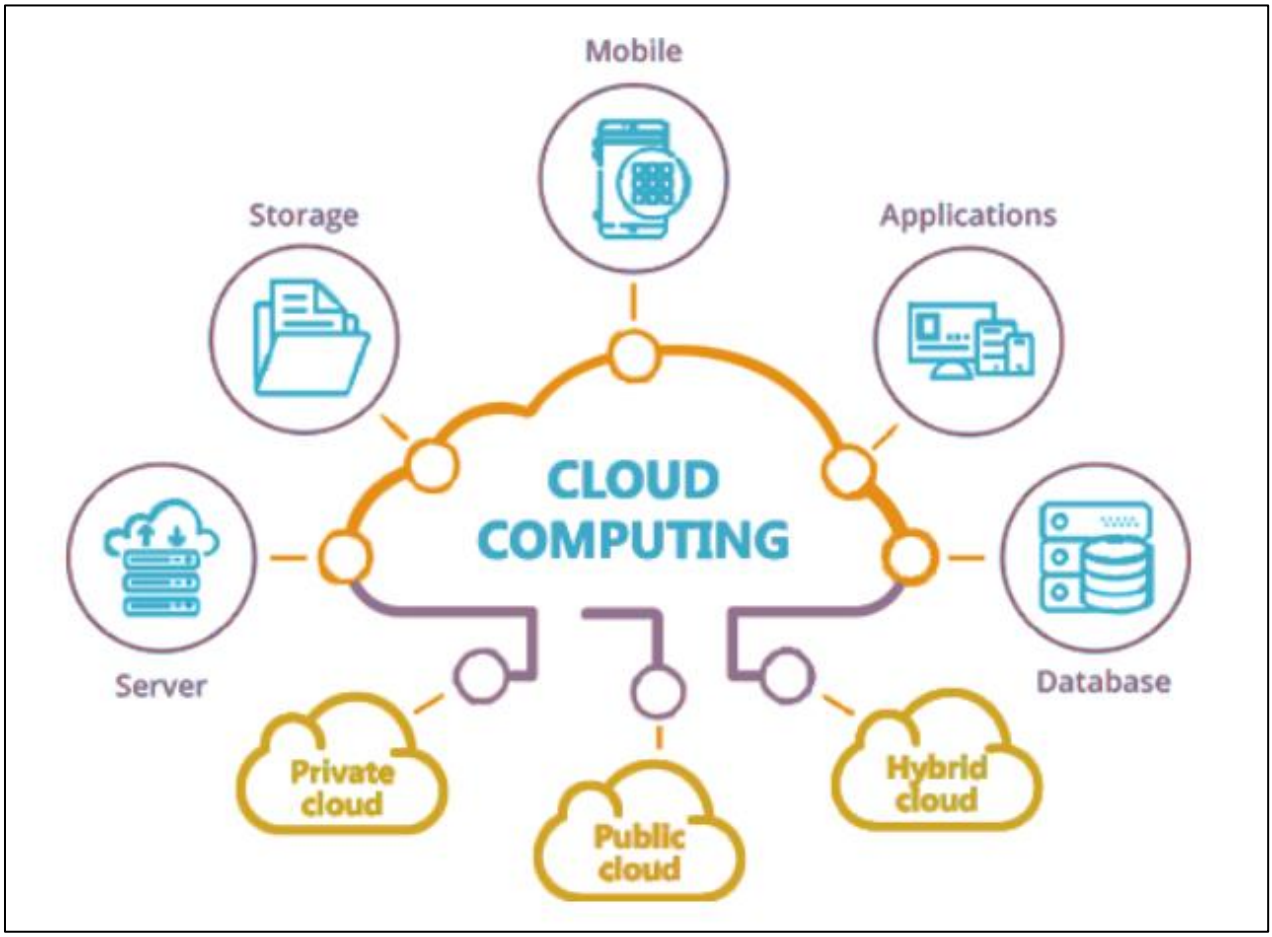
2.1. Arhitektura računalnih oblaka

Arhitektura računalnih oblaka predstavlja složen, višeslojni sustav koji omogućuje isporuku računalnih resursa putem interneta. Ključna značajka ove arhitekture je njena modularnost i fleksibilnost, što omogućava jednostavno prilagođavanje i skaliranje ovisno o potrebama korisnika. Arhitektura oblaka može se promatrati kroz nekoliko različitih slojeva, od kojih svaki ima specifičnu funkciju unutar cjelokupnog sustava (Thakkare i Singh, 2021).

Prvi sloj u arhitekturi oblaka je fizička infrastruktura, koja obuhvaća hardver poput servera, mrežnih uređaja i sustava za pohranu podataka. Ova infrastruktura obično se nalazi u velikim podatkovnim centrima koje pružatelji usluga u oblaku održavaju i upravljaju njima. Unutar ovih podatkovnih centara, resursi su organizirani tako da omogućuju virtualizaciju, ključnu komponentu arhitekture oblaka. Virtualizacija omogućuje kreiranje virtualnih strojeva (VM) i drugih virtualnih resursa, što korisnicima omogućava da pristupe

računalnim resursima bez izravne interakcije s fizičkim hardverom. Ova razina apstrakcije omogućava učinkovito upravljanje resursima i njihovu optimalnu iskorištenost (Thakkare i Singh, 2021).

Na sljedećem sloju arhitekture računalnih oblaka nalazi se virtualizacija, koja omogućuje izolaciju aplikacija i operativnih sustava unutar virtualnih okruženja. Pomoću virtualizacije, pružatelji usluga mogu optimizirati iskorištenost fizičkih resursa, raspodjeljujući ih između različitih korisnika i aplikacija. Ovaj sloj omogućuje dinamičko dodjeljivanje resursa ovisno o potrebama korisnika, čineći sustav oblaka izuzetno fleksibilnim i skalabilnim. Virtualizacija također igra ključnu ulogu u omogućavanju kontinuiranog rada aplikacija i smanjenju vremena zastoja, jer se virtualni strojevi mogu brzo premjestiti s jednog fizičkog servera na drugi bez prekida u radu.



Slika 1. Arhitektura računalnih oblaka

Izvor: Knoldus, 2024

Iznad sloja virtualizacije nalaze se platforme za upravljanje oblakom i usluge oblaka. Ovaj sloj omogućuje korisnicima pristup različitim uslugama poput Infrastructure as a Service (IaaS), Platform as a Service (PaaS) i Software as a Service (SaaS). IaaS korisnicima omogućava pristup osnovnoj infrastrukturi poput virtualnih strojeva, mrežnih resursa i pohrane, bez potrebe za upravljanjem fizičkim hardverom. PaaS nudi platformu za razvoj i implementaciju aplikacija, omogućujući programerima da se fokusiraju na kodiranje i razvoj bez brige o upravljanju infrastrukturom. SaaS omogućuje korisnicima pristup softverskim aplikacijama putem interneta, što je korisno za tvrtke koje žele koristiti softver bez potrebe za njegovom instalacijom i održavanjem (Zhang i sur., 2021).

Jedna od najvažnijih komponenti arhitekture računalnih oblaka je usmjerivački sloj ili sloj mrežne infrastrukture. Ovaj sloj osigurava povezanost između različitih dijelova oblaka, omogućavajući komunikaciju između aplikacija, podataka i korisnika. Mrežna infrastruktura omogućuje brzu i sigurnu distribuciju podataka između podatkovnih centara i korisnika, čime se osigurava visoka dostupnost i performanse usluga. U arhitekturi oblaka koriste se napredne mrežne tehnologije poput Software-Defined Networking (SDN) i Network Function Virtualization (NFV), koje omogućuju dinamičko upravljanje mrežnim resursima i povećavaju efikasnost cjelokupnog sustava (Zhang i sur., 2021).

Arhitektura računalnih oblaka također uključuje sloj za pohranu podataka. U ovom sloju podaci se pohranjuju na distribuirane sustave pohrane, koji omogućuju skalabilnost i visoku dostupnost. Podaci u oblaku mogu biti pohranjeni na različitim geografskim lokacijama, čime se osigurava njihova sigurnost i dostupnost čak i u slučaju lokalnih kvarova. Složeni sustavi za pohranu podataka u oblaku često koriste tehnologije poput Object Storage, koje omogućuju jednostavno i efikasno pohranjivanje velikih količina nestrukturiranih podataka. Pored toga, sustavi za pohranu u oblaku mogu koristiti razne metode replikacije i distribucije podataka kako bi se osigurala otpornost i integritet podataka

Na najvišoj razini arhitekture računalnih oblaka nalaze se aplikacijski slojevi i korisničko sučelje. Ovi slojevi omogućuju krajnjim korisnicima pristup aplikacijama i uslugama koje se nalaze u oblaku. Kroz web-bazirana sučelja ili API-je (Application Programming Interface), korisnici mogu komunicirati s aplikacijama u oblaku, koristeći resurse u

stvarnom vremenu. Ovaj sloj često uključuje i alate za upravljanje oblakom, koje korisnicima omogućuju kontrolu i praćenje korištenja resursa, konfiguriranje aplikacija i upravljanje poslovnim procesima koji se izvode u oblaku (Zhang i sur., 2021).

Arhitektura računalnih oblaka temelji se na principima skalabilnosti, fleksibilnosti i automatizacije. Ovi principi omogućuju jednostavno prilagođavanje resursa ovisno o trenutnim potrebama korisnika, bez potrebe za dugotrajnim i skupim procesima nabavke i implementacije fizičke infrastrukture. S obzirom na ove karakteristike, računalni oblaci postaju sve važniji alat za modernizaciju poslovanja i ubrzanje razvoja novih tehnologija.

2.2. Migracija u računalni oblak

Migracija u računalni oblak predstavlja ključan proces za organizacije koje žele iskoristiti prednosti oblaka i unaprijediti svoje poslovanje. Ovaj proces uključuje prijenos aplikacija, podataka i drugih IT resursa iz lokalne infrastrukture na oblačne platforme. Migracija je često motivirana željom za postizanjem veće fleksibilnosti, smanjenjem troškova IT infrastrukture te bržim skaliranjem poslovnih operacija. Iako je migracija u oblak složen proces, ona otvara vrata mnogim organizacijama za optimizaciju svojih resursa i ubrzavanje inovacija. Jedan od prvih koraka u migraciji u računalni oblak je temeljita analiza trenutne IT infrastrukture. Organizacije moraju detaljno proučiti koje aplikacije i sustave žele migrirati, kako bi identificirale koje su komponente najprikladnije za oblak. Postoji više modela migracije, uključujući tzv. "lift and shift" pristup, gdje se postojeće aplikacije prenose u oblak bez promjena u njihovoj arhitekturi. Ovaj pristup je brz i omogućava organizacijama da brzo iskoriste prednosti oblaka, no ne donosi uvijek optimalne rezultate u smislu performansi i skalabilnosti (Khan i AlAjmi, 2021).

Tablica 1. Vrijednosni prijedlozi migracije podataka u računalne oblake

vrijednost	opis
Smanjenje troškova	Model isporuke u javnom oblaku pretvara kapitalne izdatke (npr. kupnju poslužitelja) u operativne izdatke.[19] To navodno smanjuje prepreke ulasku, budući da infrastrukturu obično osigurava treća strana i nije je potrebno kupiti za jednokratne ili rijetke intenzivne računalne zadatke. Određivanje cijena na bazi komunalnog računalstva je "precizno", s opcijama naplate na temelju upotrebe. Također, manje internih IT vještina je potrebno za implementaciju projekata koji koriste računalstvo u oblaku. Najsuvremeniji repozitorij projekta e-FISCAL sadrži nekoliko članaka koji detaljnije razmatraju aspekte troškova, a većina njih zaključuje da uštede troškova ovise o vrsti aktivnosti koje se podržavaju i vrsti infrastrukture dostupne unutar tvrtke.
Nezavisnost uređaja	Neovisnost o uređaju i lokaciji omogućuje korisnicima pristup sustavima pomoću web preglednika bez obzira na njihovu lokaciju ili koji uređaj koriste (npr. računalo, mobilni telefon). Budući da se infrastruktura nalazi izvan mjesta (obično pruža treća strana) i pristupa joj se putem interneta, korisnici se na nju mogu povezati s bilo kojeg mjesta.
Održavanje	Održavanje okruženja u oblaku lakše je jer se podaci nalaze na vanjskom poslužitelju kojeg održava davatelj bez potrebe za ulaganjem u hardver podatkovnog centra. IT održavanjem upravlja i ažurira IT tim za održavanje pružatelja usluga oblaka, što smanjuje troškove računarstva u oblaku u usporedbi s lokalnim podatkovnim centrima.
Produktivnost	Produktivnost se može povećati kada više korisnika može raditi na istim podacima istovremeno, umjesto da čekaju da se oni spreme i pošalju e-poštom. Vrijeme se može uštedjeti jer

	informacije nije potrebno ponovno unositi kada se polja podudaraju, niti korisnici moraju instalirati nadogradnje aplikacijskog softvera na svoje računalo.
Sigurnost	Sigurnost se može poboljšati zbog centralizacije podataka, povećanih resursa usmjerenih na sigurnost, itd., ali zabrinutost može i dalje postojati zbog gubitka kontrole nad određenim osjetljivim podacima i nedostatka sigurnosti za pohranjene podatke. Sigurnost je često jednako dobra ili bolja od drugih tradicionalnih sustava, djelomično zato što pružatelji usluga mogu posvetiti resurse rješavanju sigurnosnih problema s kojima si mnogi korisnici ne mogu priuštiti ili za čije rješavanje nemaju dovoljno tehničkih vještina. Međutim, složenost sigurnosti znatno se povećava kada se podaci distribuiraju na širem području ili na većem broju uređaja, kao i u sustavima s više korisnika koje dijele nepovezani korisnici. Osim toga, korisnički pristup zapisnicima sigurnosne revizije može biti težak ili nemoguć. Instalacije privatnog oblaka djelomično su motivirane željom korisnika da zadrže kontrolu nad infrastrukturom i izbjegnu gubitak kontrole nad informacijskom sigurnošću.

Izvor: izrada autora prema Tabrizchi i Kuchaki Rafsanjani, 2020

Alternativni pristupi uključuju replatformiranje ili refaktoring aplikacija, gdje se postojeće aplikacije prilagođavaju kako bi bolje iskoristile mogućnosti oblaka. Replatformiranje obuhvaća manje promjene u arhitekturi aplikacija, dok refaktoring može uključivati veće preinake, poput prijelaza s monolitnih aplikacija na mikroservise. Ovi pristupi zahtijevaju više vremena i resursa, ali mogu donijeti značajne dugoročne koristi, kao što su povećana fleksibilnost, bolje performanse i smanjeni troškovi rada aplikacija u oblaku. Jedan od ključnih razloga zašto organizacije odlučuju migrirati u računalni oblak je skalabilnost. Oblak omogućuje tvrtkama da brzo povećaju ili smanje količinu resursa koje koriste, ovisno o trenutnim potrebama. To je posebno korisno za tvrtke s promjenjivim

opterećenjem IT resursa, poput e-trgovina koje tijekom sezonskih prodaja trebaju više resursa. Umjesto da unaprijed ulažu u fizičku infrastrukturu, organizacije mogu koristiti resurse oblaka na zahtjev, plaćajući samo za ono što im je u datom trenutku potrebno.

Migracija u oblak također donosi prednosti u smislu optimizacije poslovnih procesa i povećanja učinkovitosti. Korištenjem oblačnih platformi, organizacije mogu brže implementirati nove tehnologije i aplikacije, što im omogućuje brže prilagođavanje tržišnim promjenama i potrebama korisnika. Na primjer, tvrtke mogu koristiti oblak za brže razvojne cikluse softvera, testiranje novih proizvoda ili usluga te ubrzanje inovacija. Oblak također omogućuje lakši pristup naprednim alatima i analitici, što organizacijama omogućuje bolje donošenje odluka temeljenih na podacima (Kulkarni i sur., 2021).

Jedan od važnih aspekata migracije u računalni oblak je i integracija postojećih sustava s oblakom. Mnoge organizacije imaju naslijeđene sustave (legacy systems) koji nisu dizajnirani za rad u oblačnom okruženju, što može predstavljati izazov prilikom migracije. U tim slučajevima, organizacije mogu koristiti hibridni oblak, koji omogućuje kombinaciju lokalne infrastrukture s oblačnim resursima. Ovaj pristup omogućuje postupnu migraciju, gdje se kritični sustavi zadržavaju lokalno, dok se novi ili manje kritični sustavi migriraju u oblak.

Važno je napomenuti da migracija u oblak ne znači nužno potpuni prijelaz na oblačne usluge. Mnoge organizacije odlučuju se za hibridna rješenja ili multi-cloud strategije, koje omogućuju korištenje više oblačnih platformi od različitih pružatelja usluga. Hibridni oblak kombinira lokalnu infrastrukturu s oblačnim resursima, omogućujući organizacijama veću fleksibilnost i kontrolu nad svojim podacima i aplikacijama. Multi-cloud strategija omogućuje organizacijama da koriste usluge više pružatelja oblaka, čime smanjuju ovisnost o jednom pružatelju i povećavaju otpornost sustava (Kulkarni i sur., 2021).

Također, važno je razmotriti i troškovne aspekte migracije u oblak. Iako migracija može značiti smanjenje početnih ulaganja u IT infrastrukturu, važno je pažljivo planirati troškove korištenja oblaka. Troškovi mogu varirati ovisno o vrsti usluga koje se koriste, količini resursa i načinu upravljanja aplikacijama u oblaku. Organizacije moraju detaljno

analizirati modele naplate usluga oblaka kako bi osigurale optimalno korištenje resursa i izbjegle nepredviđene troškove.

Migracija u računalni oblak također može značajno poboljšati kolaboraciju i komunikaciju unutar organizacija. Zahvaljujući oblaku, timovi mogu jednostavno dijeliti datoteke, raditi na projektima u stvarnom vremenu i komunicirati bez obzira na njihovu fizičku lokaciju. Ovaj aspekt posebno je važan u modernom poslovnom okruženju, gdje je rad na daljinu postao uobičajen. Oblak omogućuje zaposlenicima pristup svim potrebnim alatima i resursima s bilo kojeg uređaja, čime se povećava produktivnost i fleksibilnost rada. Migracija u oblak predstavlja transformacijski proces za organizacije svih veličina. Ovaj proces ne samo da omogućuje optimizaciju postojećih IT resursa, već otvara i mogućnosti za inovacije i poboljšanje poslovnih procesa. Korištenje oblaka omogućuje organizacijama brže prilagodbe tržišnim promjenama, bolje upravljanje resursima te povećanje učinkovitosti i produktivnosti, čineći ih konkurentnijima na globalnom tržištu.

2.3. Učinkovitost i performanse

Učinkovitost i performanse računalnih oblaka predstavljaju ključne aspekte koji su pridonijeli njihovoj popularnosti i širokoj primjeni u raznim industrijama. Računalni oblak omogućuje optimizirano korištenje resursa, fleksibilnost u poslovanju i značajno smanjenje operativnih troškova, što rezultira visokom razinom učinkovitosti. Performanse oblaka također omogućuju bržu obradu podataka, povećanje skalabilnosti te pristup naprednim tehnologijama koje bi inače bile teško dostupne manjim organizacijama (Coppolino i sur., 2019).

Jedan od ključnih faktora koji pridonosi učinkovitosti računalnih oblaka je virtualizacija resursa. Kroz virtualizaciju, pružatelji usluga oblaka mogu dinamički dodjeljivati računalne resurse kao što su procesorska snaga, memorija i pohrana prema potrebama korisnika. Time se postiže maksimalna iskorištenost dostupnih resursa jer se kapacitet koji bi mogao ostati neiskorišten u tradicionalnim sustavima sada može podijeliti među više korisnika. Ovaj način rada omogućuje tvrtkama da optimiziraju troškove i izbjegnu

ulaganje u skupu fizičku infrastrukturu, dok istovremeno osiguravaju visoke performanse aplikacija i sustava.

Osim toga, računalni oblaci omogućuju korisnicima fleksibilnost u korištenju resursa putem modela plaćanja prema korištenju (pay-as-you-go). Ovaj model omogućuje tvrtkama da koriste samo onoliko resursa koliko im je potrebno u datom trenutku, čime se izbjegavaju fiksni troškovi koji su često povezani s tradicionalnim IT sustavima. Fleksibilnost u dodjeljivanju resursa omogućuje brzo prilagođavanje promjenama u potražnji, što znači da tvrtke mogu bez problema povećati ili smanjiti korištenje resursa na temelju trenutnih potreba. Na primjer, tijekom sezonskih vrhova u poslovanju, tvrtke mogu jednostavno povećati količinu računalne snage bez potrebe za dodatnim ulaganjima u hardver (Zou i sur., 2017).

Perforanse računalnih oblaka također su poboljšane zahvaljujući mogućnosti skalabilnosti. Oblaci omogućuju horizontalnu i vertikalnu skalabilnost, što znači da se resursi mogu povećati dodavanjem dodatnih virtualnih strojeva (horizontalno skaliranje) ili poboljšanjem performansi postojećih resursa (vertikalno skaliranje). Ova sposobnost omogućuje organizacijama da zadovolje promjenjive poslovne zahtjeve, kao i da osiguraju dosljedne performanse čak i tijekom naglih povećanja potražnje. Na primjer, aplikacije koje obrađuju velike količine podataka mogu koristiti skalabilnost oblaka kako bi se prilagodile promjenjivom opterećenju, osiguravajući tako brzinu obrade i pouzdanost. Brzina pristupa podacima i aplikacijama jedan je od ključnih elemenata performansi računalnih oblaka. Globalno distribuirane mreže podatkovnih centara omogućuju korisnicima brži pristup resursima bez obzira na njihovu fizičku lokaciju. Ova geografska distribucija omogućuje smanjenje kašnjenja i povećanje brzine obrade podataka. Kada su podaci pohranjeni u podatkovnim centrima koji su bliži krajnjim korisnicima, vrijeme odziva aplikacija se značajno smanjuje, što povećava opću korisničku učinkovitost. Primjerice, tvrtke koje pružaju usluge korisnicima na globalnoj razini mogu imati koristi od ove geografske distribucije jer omogućuju korisnicima diljem svijeta brz i nesmetan pristup njihovim aplikacijama (Zou i sur., 2017).

Jedan od dodatnih aspekata učinkovitosti računalnih oblaka jest i automatizacija. Moderni oblačni sustavi nude visok stupanj automatizacije u procesima poput dodjeljivanja resursa, skaliranja i održavanja aplikacija. Automatizirani procesi smanjuju

potrebu za ručnim upravljanjem i intervencijama, čime se povećava učinkovitost poslovanja i smanjuje vjerojatnost pogrešaka. Organizacije mogu koristiti alate za automatizaciju kako bi postigle konzistentnost u poslovnim operacijama, smanjile vrijeme zastoja i optimizirale radne procese. Primjerice, automatizacija omogućuje da se resursi automatski skaliraju u trenucima povećanog opterećenja, bez potrebe za ručnim prilagodbama od strane IT timova.

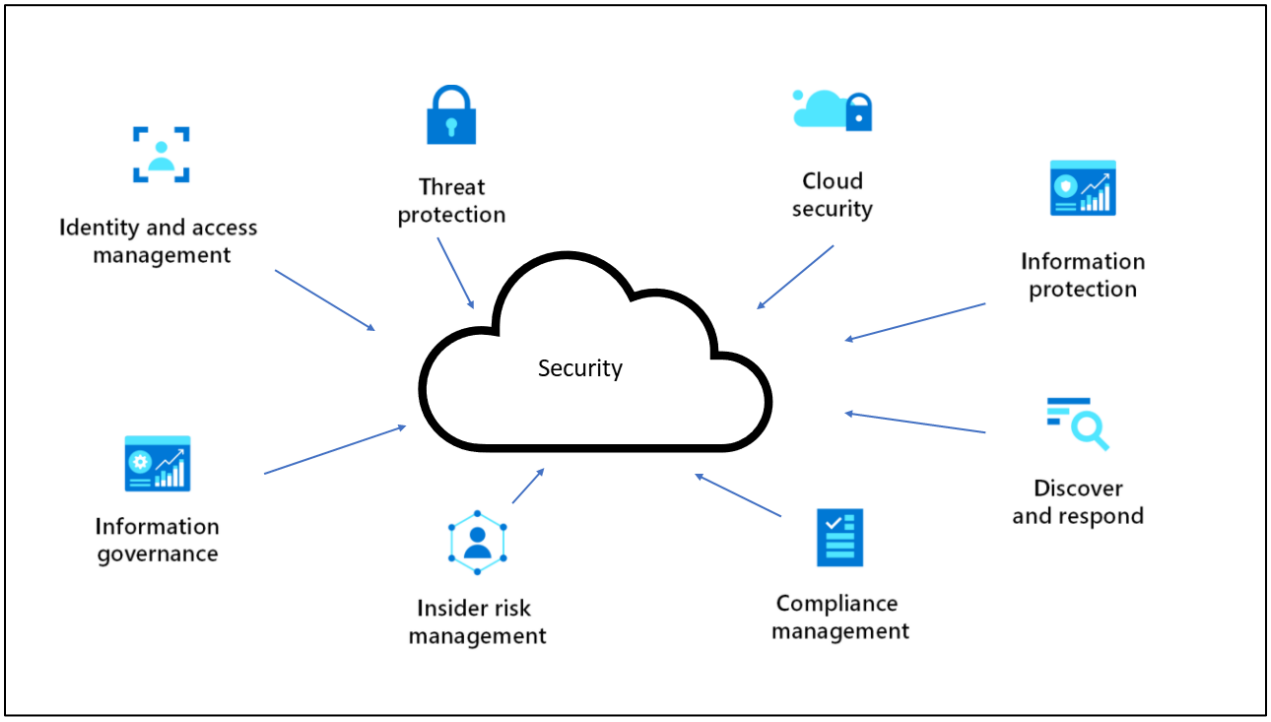
Performanse računalnih oblaka također su unaprijeđene korištenjem naprednih tehnologija kao što su kontejneri i mikroservisi. Ove tehnologije omogućuju modularni pristup razvoju aplikacija, što povećava agilnost i poboljšava performanse. Kontejneri omogućuju izolaciju aplikacija unutar virtualnih okruženja, osiguravajući da svaka aplikacija radi neovisno o drugim komponentama sustava. Ovaj pristup povećava učinkovitost jer omogućuje bržu implementaciju novih značajki, smanjujući vrijeme potrebno za razvoj i održavanje aplikacija. Mikroservisi, s druge strane, omogućuju raspodjelu aplikacija na manje, neovisne module, čime se poboljšava skalabilnost i povećava otpornost sustava na promjene u opterećenju. Učinkovitost računalnih oblaka također se ogleda u njihovoj sposobnosti da podrže napredne analitičke procese i velike podatke (big data). Obrada velikih količina podataka zahtijeva značajne resurse, a oblak omogućuje da se ti resursi koriste na fleksibilan i troškovno učinkovit način. Tvrtke mogu analizirati podatke u stvarnom vremenu koristeći oblačne resurse, što im omogućuje brže donošenje odluka i prilagođavanje tržišnim trendovima. Veliki podaci također mogu biti pohranjeni u oblaku, čime se smanjuju troškovi pohrane i povećava dostupnost podataka za analitičke timove (Zou i sur., 2017).

Na kraju, performanse računalnih oblaka omogućuju tvrtkama pristup naprednim tehnologijama kao što su umjetna inteligencija (AI) i strojno učenje (ML). Ove tehnologije često zahtijevaju ogromnu računalnu snagu i velike količine podataka, što oblak može osigurati. Korištenje AI i ML tehnologija omogućuje tvrtkama automatizaciju poslovnih procesa, prediktivnu analitiku i prilagodbu korisničkog iskustva. Računalni oblak olakšava integraciju ovih tehnologija u poslovne procese, čime se značajno povećava operativna učinkovitost i konkurentska prednost na tržištu. Učinkovitost i performanse računalnih oblaka ne samo da omogućuju optimizaciju postojećih IT resursa, već pružaju

organizacijama mogućnost da ubrzaju inovacije, poboljšaju operativnu učinkovitost i brže odgovore na promjenjive poslovne potrebe.

3. SIGURNOSTI ASPEKTI PODATAKA

Sigurnosni aspekti podataka ključni su za svaku organizaciju i pojedinca koji koristi digitalne tehnologije. S obzirom na sve veći rast količine podataka koji se generiraju i pohranjuju, kao i sveprisutnost digitalnih sustava u svakodnevnom životu, osiguravanje integriteta, povjerljivosti i dostupnosti podataka postalo je presudno za uspješno funkcioniranje modernih informacijskih sustava. Podaci su temelj mnogih poslovnih procesa i odluka, te je njihova zaštita jedan od najvažnijih zadataka u digitalnom dobu (Zovko, 2017).



Slika 2. Sigurnosni aspekti računalnih oblaka

Izvor: Microsoft, 2024

Jedan od ključnih aspekata zaštite podataka je povjerljivost podataka, koja podrazumijeva zaštitu podataka od neovlaštenog pristupa. Organizacije moraju osigurati da samo ovlašteni korisnici imaju pristup osjetljivim informacijama. Povjerljivost se često postiže korištenjem metoda enkripcije, kontrolom pristupa i strogo definiranim pravilima

o tome tko i pod kojim uvjetima može pristupiti određenim informacijama. Na primjer, osobni podaci klijenata moraju biti zaštićeni kako bi se izbjegla neovlaštena upotreba ili krađa identiteta (Zovko, 2017).

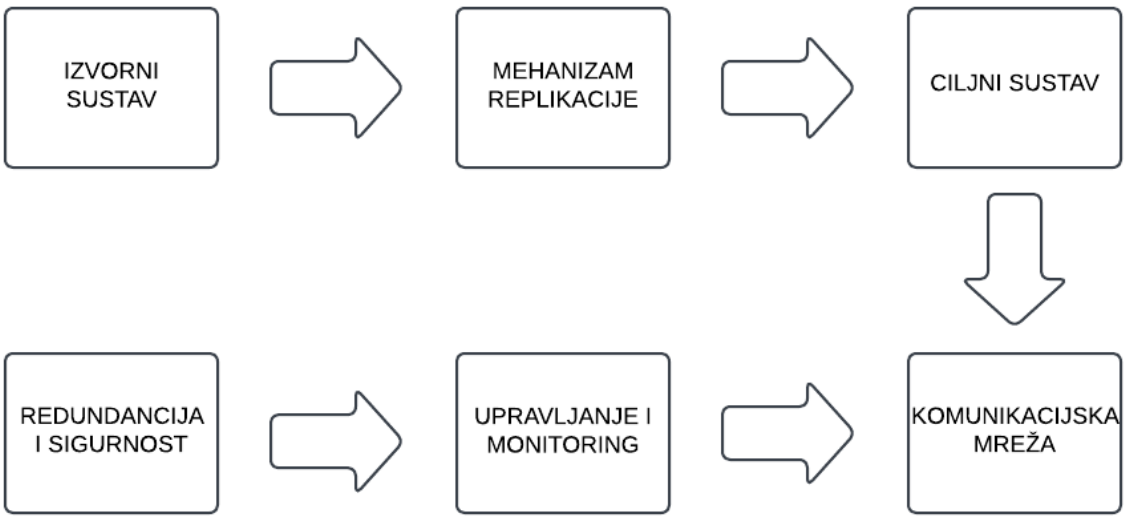
Drugi važan aspekt sigurnosti podataka je integritet podataka, što znači da podaci moraju ostati točni i nepromijenjeni tijekom svog životnog ciklusa. Bilo kakva izmjena ili oštećenje podataka može imati ozbiljne posljedice, osobito u sektorima poput financija, zdravstva i upravljanja kritičnim infrastrukturama. Organizacije moraju implementirati mehanizme za provjeru integriteta podataka kako bi osigurale da podaci nisu neovlašteno promijenjeni ili oštećeni prilikom prijenosa ili pohrane. Kontinuirano praćenje i revizija sustava ključni su za osiguranje točnosti podataka.

Dostupnost podataka treći je ključni aspekt sigurnosnih standarda. Podaci moraju biti dostupni korisnicima kad god su im potrebni, bez obzira na eventualne tehničke poteškoće ili prekide u sustavu. To je posebno važno za poslovne procese koji se oslanjaju na stalni pristup informacijama, kao što su bankarstvo, e-trgovina ili zdravstveni sustavi. Kako bi se osigurala dostupnost, organizacije koriste metode poput replikacije podataka, distribuiranih sustava pohrane i automatiziranih sigurnosnih kopija. Ovi sustavi omogućuju kontinuirani rad čak i u slučaju kvarova ili drugih tehničkih problema (slika 3.).

Jedan od glavnih izazova u zaštiti podataka je upravljanje osjetljivim podacima. Pojedinci i organizacije svakodnevno obrađuju velike količine osjetljivih podataka, kao što su osobni identifikacijski podaci, financijski podaci i povjerljive poslovne informacije. Upravljanje ovim podacima zahtijeva stroge politike i procedure kako bi se osiguralo njihovo pravilno rukovanje i pohrana. Mnoge organizacije koriste politike upravljanja podacima kako bi osigurale da su osjetljivi podaci obrađeni na siguran način i da su zaštićeni tijekom cijelog njihovog životnog ciklusa (Zovko, 2017).

Pravni i regulatorni aspekti također igraju ključnu ulogu u sigurnosti podataka. Sve veći broj zakonodavnih okvira diljem svijeta regulira način na koji organizacije moraju upravljati podacima, osobito kada su u pitanju osobni podaci. Zakonodavstva poput Opće uredbe o zaštiti podataka (GDPR) u Europskoj uniji zahtijevaju od organizacija da implementiraju stroge mjere zaštite podataka i da osiguraju da se podaci obrađuju u skladu s pravnim zahtjevima. Organizacije moraju pratiti i poštivati ove propise kako bi izbjegle značajne

kazne i zaštitile povjerenje svojih korisnika. Upravljanje podacima i zaštita podataka postaju sve složeniji procesi s obzirom na napredak digitalnih tehnologija i globalizaciju poslovanja. Korištenje naprednih tehnologija i metoda upravljanja podacima ključno je za osiguranje da podaci ostanu povjerljivi, točni i dostupni, bez obzira na izazove koji se pojavljuju u sve složenijem digitalnom okruženju.



Slika 3. Logički dijagram replikacije podataka

Izvor: vlastita izrada autora

3.1. Metode i prakse zaštite podataka

Zaštita podataka u računalnim oblacima od iznimne je važnosti s obzirom na sve veću primjenu oblaka u poslovanju, javnim službama i privatnim sektorima. U okruženju računalnih oblaka podaci su često pohranjeni i obrađeni na udaljenim poslužiteljima, što donosi brojne prednosti, ali također otvara nova pitanja vezana uz zaštitu i sigurnost podataka. Postoje mnoge metode i prakse zaštite podataka u oblaku koje omogućuju organizacijama da smanje rizike i osiguraju visoku razinu sigurnosti prilikom korištenja oblačnih tehnologija (Pokić, 2013).

Jedna od temeljnih metoda zaštite podataka u računalnim oblacima je enkripcija podataka. Enkripcija se koristi kako bi se podaci pretvorili u kodirani oblik, koji može biti dekodiran samo pomoću odgovarajućeg ključa. Ova metoda osigurava da, čak i ako dođe do neovlaštenog pristupa podacima, oni ne mogu biti pročitani ili zloupotrijebljeni. Enkripcija se može primijeniti na podatke u mirovanju (kad su pohranjeni) i podatke u prijenosu (kad se prenose između korisnika i oblačne platforme). Praksa korištenja end-to-end enkripcije posebno je važna jer osigurava da su podaci zaštićeni cijelim putem, od krajnjeg korisnika do pohrane na oblačnim poslužiteljima.

Osim enkripcije, učinkovite politike upravljanja pristupom također igraju ključnu ulogu u zaštiti podataka u oblaku. Upravljanje pristupom podrazumijeva uspostavu sustava koji kontrolira tko ima pristup podacima, koje akcije može poduzimati i pod kojim uvjetima. Koristeći model najmanjih privilegija, organizacije mogu osigurati da korisnici i sustavi imaju pristup samo onim resursima koji su im nužno potrebni za obavljanje njihovih zadataka. Autentifikacija i autorizacija ključni su elementi u ovom procesu. Višefaktorska autentifikacija (MFA) predstavlja naprednu mjeru koja zahtijeva dodatne slojeve provjere identiteta, što značajno smanjuje rizik od neovlaštenog pristupa (Dražić, 2022).

Segmentacija podataka ili tokenizacija predstavlja još jednu važnu metodu zaštite podataka u oblaku. Ova praksa uključuje razdvajanje osjetljivih podataka od ostatka sustava, čime se smanjuje rizik u slučaju da određeni dijelovi sustava budu kompromitirani. Tokenizacija zamjenjuje osjetljive podatke slučajnim generiranim vrijednostima, tzv. tokenima, koji nemaju nikakvu inherentnu vrijednost izvan sigurnog sustava za dekodiranje. Ova metoda je korisna u zaštiti podataka o plaćanju, osobnih podataka i drugih osjetljivih informacija (Dražić, 2022).

Kontrola verzija podataka i sigurnosne kopije također su važne prakse u zaštiti podataka u oblaku. Redovito stvaranje sigurnosnih kopija podataka omogućava da se izgubljeni ili oštećeni podaci brzo obnove, minimizirajući vrijeme zastoja i gubitak važnih informacija. Automatizirane sigurnosne kopije osiguravaju da su podaci kontinuirano zaštićeni i ažurirani bez potrebe za ručnim intervencijama. Ovaj pristup je posebno važan za organizacije koje upravljaju velikim količinama podataka i ne mogu si priuštiti gubitak ili dugotrajnu nedostupnost podataka.

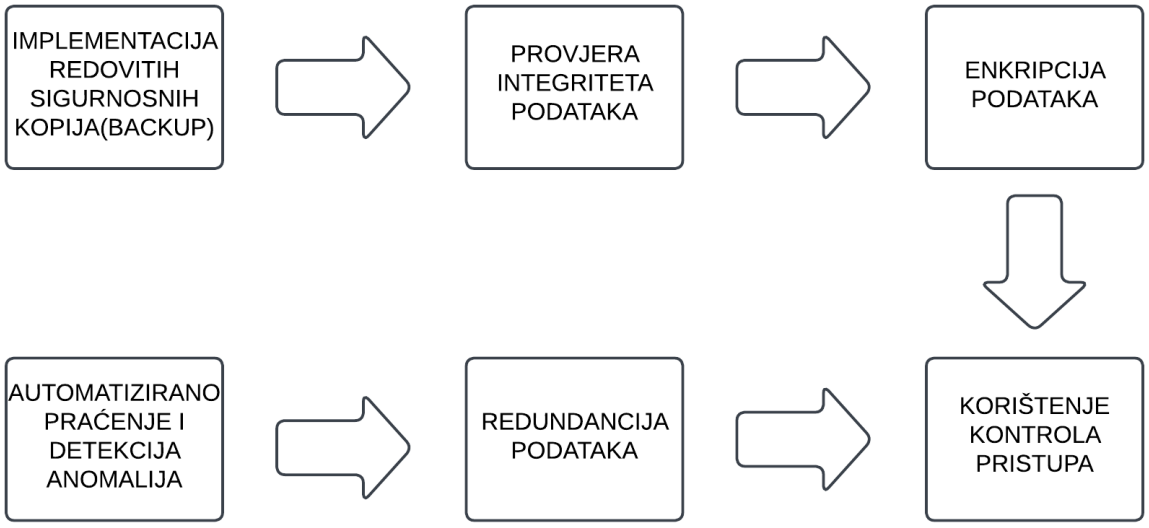
Auditi i praćenje aktivnosti također su ključni aspekti sigurnosti podataka u oblaku. Sustavi za nadzor omogućuju organizacijama da prate aktivnosti unutar oblačne infrastrukture, otkrivajući potencijalno sumnjive ili neovlaštene aktivnosti. Redoviti auditi sigurnosti pomažu identificirati slabosti ili potencijalne prijetnje u sustavima, omogućujući organizacijama da pravovremeno poduzmu mjere za smanjenje rizika. Praćenje u stvarnom vremenu omogućuje brzo otkrivanje i reakciju na sigurnosne incidente, smanjujući štetu koja bi mogla nastati u slučaju napada ili tehničkog kvara.

Korištenje sigurnosnih alata temeljenih na umjetnoj inteligenciji (AI) i strojnom učenju također je sve popularnija praksa u zaštiti podataka u oblaku. Ovi alati koriste napredne algoritme za otkrivanje nepravilnosti u obrascima korištenja podataka i sustava. AI tehnologije mogu analizirati velike količine podataka u stvarnom vremenu i identificirati potencijalne sigurnosne prijetnje, poput neobičnih uzoraka pristupa ili neovlaštenih pokušaja prijave. Strojno učenje omogućuje sustavima da se neprestano prilagođavaju i poboljšavaju svoje sposobnosti prepoznavanja prijetnji, čime se povećava razina zaštite podataka.

Sukladnost s regulativama i zakonskim zahtjevima još je jedan važan aspekt zaštite podataka u oblaku. Organizacije moraju osigurati da njihovi procesi obrade i pohrane podataka zadovoljavaju sve relevantne propise, kao što su Opća uredba o zaštiti podataka (GDPR) u Europskoj uniji ili slični zakoni u drugim jurisdikcijama. Sukladnost s ovim regulativama ne samo da pomaže zaštiti podataka, već i izbjegavanju potencijalnih pravnih posljedica i kazni (Dražić, 2022).

Razgraničenje odgovornosti između pružatelja usluga oblaka i korisnika važan je faktor u osiguravanju cjelovite zaštite podataka. Iako pružatelji oblaka nude osnovne sigurnosne mjere, korisnici su odgovorni za implementaciju dodatnih sigurnosnih praksi, poput enkripcije ili upravljanja pristupom. Organizacije moraju jasno razumjeti koja je razina odgovornosti na strani pružatelja usluga, a koja na njihovoj, kako bi osigurale potpunu zaštitu podataka unutar oblačne infrastrukture. Najbolja praksa u zaštiti podataka u računalnim oblacima leži u kombiniranju više slojeva zaštite. Ovaj pristup, poznat kao obrana u dubini, uključuje primjenu različitih sigurnosnih mjera koje zajedno pružaju sveobuhvatnu zaštitu. Korištenjem enkripcije, upravljanjem pristupom, redovitim sigurnosnim kopijama, nadzorom aktivnosti i usklađenošću s regulativama, organizacije

mogu značajno smanjiti rizik od gubitka podataka ili neovlaštenog pristupa. Ova slojevita strategija osigurava da, čak i ako jedna razina sigurnosti bude kompromitirana, druge mjere ostaju na snazi kako bi zaštitile osjetljive podatke.



Slika 4. Dijagram signurnosnih praksi i zaštite podataka

Izvor: vlastita izrada autora

3.2. Kontrola pristupa i upravljanje identitetima

Kontrola pristupa i upravljanje identitetima (Identity and Access Management, IAM) na računalnim oblacima ključni su elementi za osiguranje sigurnosti i zaštitu podataka u oblačnim sustavima. Ove tehnologije omogućuju organizacijama da učinkovito upravljaju korisničkim identitetima, definiraju tko ima pristup određenim resursima i osiguraju da pristup bude kontroliran prema strogo definiranim pravilima i politikama. Korištenje ovih metoda omogućuje organizacijama da smanje rizike vezane uz neovlašteni pristup te da zaštite osjetljive podatke i poslovne aplikacije koje se nalaze u oblaku (Dražić, 2022).

Kontrola pristupa na računalnim oblacima osigurava da samo ovlašteni korisnici mogu pristupiti određenim resursima i aplikacijama unutar oblačne infrastrukture. To je važno

jer oblak omogućuje dijeljenje resursa na globalnoj razini, a bez pravilno implementirane kontrole pristupa podaci i aplikacije mogu biti izloženi neovlaštenom pristupu. Osnovni princip kontrole pristupa je autentifikacija, proces kojim korisnik dokazuje svoj identitet prilikom prijave u sustav. Standardne metode autentifikacije uključuju korištenje korisničkih imena i lozinki, ali s porastom sofisticiranosti prijetnji, sve veći naglasak stavlja se na korištenje višefaktorske autentifikacije (MFA), koja zahtijeva dodatne slojeve provjere, poput upotrebe jedinstvenih kodova, biometrijskih podataka ili fizičkih tokena.

Jedna od ključnih metoda kontrole pristupa je upravljanje korisničkim pravima. Ova praksa obuhvaća definiranje tko ima pristup određenim resursima na temelju njihove uloge unutar organizacije. Ovdje se primjenjuje model najmanjih privilegija (Least Privilege Principle), koji osigurava da korisnici imaju samo one privilegije koje su im nužne za obavljanje njihovih zadataka, čime se smanjuje rizik od zloupotrebe podataka ili neovlaštenog pristupa. Na primjer, zaposlenik koji radi u odjelu financija trebao bi imati pristup samo financijskim aplikacijama, dok IT stručnjaci trebaju imati pristup alatima za održavanje infrastrukture. Ovaj model pomaže minimizirati potencijalne prijetnje koje mogu nastati zbog ljudskih pogrešaka ili zloupotrebe privilegija. Upravljanje identitetima je također ključna komponenta u oblačnim sustavima, jer se njime osigurava dosljedna i centralizirana kontrola nad svim korisničkim identitetima koji pristupaju resursima unutar oblaka. Identity and Access Management (IAM) sustavi omogućuju automatizaciju procesa upravljanja korisničkim pravima, provodeći politike sigurnosti u stvarnom vremenu i osiguravajući da su identiteti pravilno autorizirani za pristup potrebnim resursima. Ovi sustavi omogućuju organizacijama da brzo dodaju nove korisnike, uklone one koji više ne trebaju pristup te ažuriraju korisnička prava kako bi odgovarala trenutnim poslovnim potrebama. IAM sustavi također omogućuju organizacijama da vode evidenciju o tome tko je i kada pristupao određenim resursima, što je važno za reviziju i praćenje aktivnosti unutar oblaka (Nassif i sur., 2021).

Korištenje jedinstvene prijave (Single Sign-On, SSO) jedan je od popularnih alata unutar oblačnih sustava za upravljanje identitetima i kontrolu pristupa. SSO omogućuje korisnicima da se prijave jednom kako bi dobili pristup više aplikacija i sustava bez potrebe za ponovnim unosom svojih vjerodajnica. Ovo značajno pojednostavljuje

korisničko iskustvo i smanjuje potrebu za pamćenjem više lozinki. SSO ne samo da povećava produktivnost, već i poboljšava sigurnost jer smanjuje rizik od krađe identiteta ili lozinki prilikom ponovljenih prijava na različite sustave. U kombinaciji s višefaktorskom autentifikacijom, SSO pruža robustan i siguran način upravljanja identitetima u oblačnim sustavima (Nasiff i sur., 2021).

Za organizacije koje koriste više pružatelja usluga oblaka, federacija identiteta postaje ključni koncept. Federacija identiteta omogućuje korisnicima da koriste jedinstveni identitet za pristup resursima kod različitih pružatelja usluga oblaka, čime se pojednostavljuje upravljanje identitetima i omogućuje dosljedna primjena sigurnosnih politika u cijelom oblačnom ekosustavu. Ovaj pristup omogućuje organizacijama da izbjegnu stvaranje zasebnih računa i identiteta za svaki oblak koji koriste, čime se smanjuje kompleksnost i povećava sigurnost. Upravljanje identitetima i kontrola pristupa također uključuju automatsko upravljanje životnim ciklusom identiteta, što podrazumijeva kontinuirano praćenje i prilagođavanje korisničkih privilegija tijekom vremena. Na primjer, kada korisnik napusti organizaciju, IAM sustavi automatski uklanjaju njegove pristupne vjerodajnice, čime se sprječava daljnji pristup osjetljivim podacima. Slično tome, ako se zaposlenik premjesti u drugi odjel ili promijeni svoju ulogu unutar organizacije, IAM sustavi mogu automatski ažurirati njegove pristupne privilegije kako bi odgovarale novim poslovnim zahtjevima. Ova automatizacija smanjuje rizik od pogrešaka i osigurava da su korisnička prava uvijek usklađena s trenutnim potrebama (Dražić, 2022).

Za upravljanje identitetima na računalnim oblacima, od ključne važnosti je i praćenje i revizija aktivnosti korisnika. Organizacije moraju biti u stanju pratiti tko, kada i kako pristupa njihovim resursima u oblaku. Sustavi za praćenje aktivnosti omogućuju stvaranje detaljnih zapisa o svim korisničkim aktivnostima, što je neophodno za sigurnosne audite i analize u slučaju potencijalnih incidenata. Ovi zapisi omogućuju brzo otkrivanje neovlaštenih pokušaja pristupa ili zloupotrebe resursa te omogućuju organizacijama da brzo reagiraju na potencijalne prijetnje. Kontrola pristupa i upravljanje identitetima temeljni su elementi sigurnosti u računalnim oblacima. Ove tehnologije omogućuju organizacijama da zaštite svoje resurse i podatke, osiguravajući da su samo ovlašteni korisnici s odgovarajućim privilegijama u mogućnosti pristupiti osjetljivim informacijama. Kombinacija višefaktorske autentifikacije, jedinstvene prijave, federacije identiteta i

automatiziranog upravljanja životnim ciklusom identiteta stvara sveobuhvatnu i sigurnu infrastrukturu koja omogućuje sigurno korištenje oblačnih tehnologija.

3.3. Uloga automatizacije

Automatizacija na računalnim oblacima ima ključnu ulogu u optimizaciji i efikasnom upravljanju resursima, procesima i uslugama unutar oblaka. Ona omogućuje organizacijama da smanje potrebu za ručnim upravljanjem i intervencijama, povećavajući time produktivnost, pouzdanost i skalabilnost poslovanja. Računalni oblaci pružaju dinamično okruženje u kojem se resursi, poput procesorske snage, pohrane podataka i mrežnih kapaciteta, mogu brzo prilagoditi trenutnim potrebama korisnika, a automatizacija omogućuje da se ti resursi koriste na najučinkovitiji način. Uloga automatizacije postaje sve važnija kako se oblak sve više koristi u različitim industrijama i za sve složenije poslovne operacije.

Jedna od najvažnijih funkcija automatizacije u oblaku je automatizirano upravljanje resursima. Umjesto da IT timovi ručno konfiguriraju i prilagođavaju oblačne resurse, automatizacijski alati omogućuju automatsko skaliranje resursa ovisno o opterećenju aplikacija ili sustava. Na primjer, ako web aplikacija doživi nagli porast broja korisnika, automatizacijski sustavi mogu automatski povećati broj virtualnih strojeva ili dodijeliti dodatne resurse za pohranu kako bi se osigurao nesmetan rad aplikacije. Ovaj proces poznat je kao automatsko skaliranje (auto-scaling) i ključan je za postizanje optimalne učinkovitosti oblaka, jer omogućuje korištenje resursa samo kad su potrebni, čime se smanjuju troškovi i povećava operativna učinkovitost (Muttik i sur., 2019).

Automatizacija također značajno ubrzava proces implementacije aplikacija u oblak. U tradicionalnim IT okruženjima, postavljanje nove aplikacije ili usluge često je dugotrajan proces koji zahtijeva ručne konfiguracije servera, baza podataka i mrežnih postavki. U oblačnim okruženjima, automatizacija omogućuje korištenje infrastrukture kao koda (Infrastructure as Code, IaC), što omogućuje programerima i IT timovima da definiraju cijelu infrastrukturu putem kodnih skripti. Ova praksa ne samo da smanjuje mogućnost ljudskih pogrešaka, već omogućuje brzo i dosljedno postavljanje infrastrukture na

različitim oblačnim platformama. Korištenje IaC alata poput Terraform-a ili AWS CloudFormation-a omogućuje organizacijama da automatiziraju cijeli proces od razvoja do implementacije, čime se značajno skraćuje vrijeme potrebno za lansiranje novih proizvoda i usluga na tržište. Još jedan važan aspekt automatizacije u računalnim oblacima je automatizirano održavanje i upravljanje radnim procesima. U oblačnim okruženjima, aplikacije i sustavi moraju biti kontinuirano nadzirani i održavani kako bi se osigurala njihova pouzdanost i performanse. Automatizacijski alati omogućuju IT timovima da definiraju pravila i zadatke koji se izvršavaju automatski, kao što su redovne sigurnosne kopije podataka, ažuriranja softvera ili upravljanje kapacitetima pohrane. Na primjer, sustavi mogu automatski pokrenuti sigurnosne kopije u određeno vrijeme ili povećati kapacitet pohrane ako se preostali prostor smanji ispod zadanog praga. Ovi procesi smanjuju potrebu za ručnim intervencijama i osiguravaju stalnu dostupnost i pouzdanost aplikacija u oblaku. Automatizacija na računalnim oblacima također igra ključnu ulogu u kontinuiranoj integraciji i isporuci (CI/CD). CI/CD je metodologija koja omogućuje da se promjene u kodu automatski integriraju, testiraju i implementiraju u produkcijsko okruženje. Korištenjem oblačnih CI/CD alata, razvojni timovi mogu automatizirati cijeli proces od pisanja koda do njegovog postavljanja u produkciju, čime se značajno skraćuje vrijeme razvoja i omogućuje brža isporuka novih funkcionalnosti korisnicima. Ova metodologija posebno je korisna za agilne timove koji često implementiraju male promjene i ažuriranja u svojim aplikacijama. Automatizacija u CI/CD procesu osigurava da se svaka promjena testira na dosljedan način, čime se smanjuje rizik od grešaka ili problema u produkcijskom okruženju (Muttik i sur., 2019).

Optimizacija troškova još je jedan važan aspekt automatizacije na računalnim oblacima. S obzirom na to da oblak omogućuje model plaćanja prema korištenju resursa (pay-as-you-go), automatizacijski alati mogu pomoći organizacijama da izbjegnu nepotrebne troškove optimiziranjem korištenja resursa. Na primjer, automatizacijski sustavi mogu prepoznati kada određeni resursi nisu u upotrebi i automatski ih isključiti kako bi se smanjili troškovi. Također, mogu se koristiti za identifikaciju manje učinkovitih resursa ili aplikacija koje troše previše kapaciteta, omogućujući organizacijama da proaktivno upravljaju svojim budžetima i osiguraju optimalno korištenje oblačnih usluga. Ova praksa

pomaže tvrtkama da zadrže fleksibilnost oblaka uz istodobno smanjenje nepotrebnih troškova i povećanje profitabilnosti (Muttik i sur., 2019).

Automatizacija na računalnim oblacima također omogućuje bolju kolaboraciju između razvojnih i operativnih timova, što je poznato kao DevOps. DevOps metodologija potiče tijesnu suradnju između timova koji razvijaju aplikacije i onih koji upravljaju infrastrukturom, a automatizacija igra ključnu ulogu u osiguravanju da procesi razvoja, testiranja i implementacije teku glatko i brzo. Automatizirani sustavi omogućuju kontinuirano praćenje i prilagodbu infrastrukture, čime se smanjuje vrijeme potrebno za otkrivanje i rješavanje potencijalnih problema. Na taj način, razvojni timovi mogu brže lansirati nove funkcionalnosti i poboljšanja, dok operativni timovi mogu osigurati da infrastruktura ostane stabilna i responzivna.

4. POVJERLJIVOST PODATAKA U RAČUNALNOM OBLAKU

Povjerljivost podataka u računalnom oblaku jedan je od najvažnijih aspekata sigurnosti u digitalnom poslovanju. Ona podrazumijeva zaštitu podataka od neovlaštenog pristupa te osiguranje da samo ovlaštene osobe i sustavi mogu pristupiti osjetljivim informacijama pohranjenim ili obrađivanim u oblaku. S obzirom na to da organizacije sve više koriste oblačne servise za pohranu i obradu kritičnih poslovnih podataka, povjerljivost postaje ključna za očuvanje integriteta podataka, zaštitu privatnosti korisnika te usklađenost s regulatornim zahtjevima. Jedan od ključnih mehanizama za očuvanje povjerljivosti podataka u oblaku je enkripcija. Enkripcija podataka omogućuje da podaci, bilo da su u prijenosu ili pohranjeni u oblaku, budu nečitljivi svima osim ovlaštenim korisnicima koji posjeduju odgovarajuće ključeve za dešifriranje. Ova metoda posebno je važna jer podaci u oblaku često prolaze kroz različite mrežne slojeve i mogu biti pohranjeni na različitim fizičkim lokacijama, ovisno o pružatelju usluga. Koristeći napredne algoritme enkripcije, kao što su AES (Advanced Encryption Standard), podaci postaju zaštićeni od neovlaštenog pristupa i presretanja tijekom prijenosa između klijenta i oblaka. Osim enkripcije podataka u prijenosu, enkripcija se primjenjuje i na podatke u pohrani, što osigurava da su čak i u slučaju fizičkog pristupa diskovima ili serverima podaci i dalje nečitljivi bez odgovarajućeg ključa (Dražić, 2022).

Upravljanje ključevima za enkripciju kritični je dio strategije povjerljivosti podataka u oblaku. Ključevi za enkripciju moraju biti pažljivo zaštićeni i upravljani kako bi se spriječio njihov gubitak ili krađa, jer bi to moglo ugroziti povjerljivost podataka. Pružatelji usluga oblaka često nude rješenja za upravljanje ključevima, no neke organizacije preferiraju samostalno upravljanje ključevima kako bi zadržale potpunu kontrolu nad njima. Postoji nekoliko modela za upravljanje ključevima, uključujući KMS (Key Management Services), koji omogućuju organizacijama automatizirano i sigurno upravljanje cijelim životnim ciklusom enkripcijskih ključeva, od njihovog generiranja do rotacije i povlačenja.

4.1. Izazovi balansiranja opterećenja i sigurnosti podataka

Balansiranje opterećenja i sigurnosti podataka u računalnim oblacima predstavlja izazov s kojim se suočavaju organizacije i pružatelji usluga oblaka. Dok balansiranje opterećenja ima za cilj optimizirati performanse i raspodjelu resursa, sigurnost podataka osigurava njihovu povjerljivost, integritet i dostupnost. Ove dvije komponente često su u napetom odnosu jer povećanje performansi kroz dinamičko raspoređivanje resursa može otvoriti nove sigurnosne ranjivosti, dok stroga sigurnosna pravila mogu usporiti sustav i otežati učinkovitu distribuciju opterećenja (Krutz i sur., 2020).

Balansiranje opterećenja odnosi se na distribuciju mrežnog ili aplikacijskog prometa na više servera kako bi se osiguralo da niti jedan pojedini server nije preopterećen, čime se poboljšavaju performanse i skalabilnost aplikacija i usluga. U oblačnim okruženjima, balansiranje opterećenja je ključno jer omogućuje skaliranje resursa ovisno o potrebama korisnika, optimizira korištenje resursa i osigurava visoku dostupnost usluga čak i pod velikim opterećenjem. Na primjer, ako web-aplikacija doživi nagli porast broja korisnika, sustav za balansiranje opterećenja automatski će raspodijeliti promet na različite servere kako bi se spriječilo usporavanje ili pad aplikacije.

S druge strane, sigurnost podataka u oblačnom okruženju zahtijeva stroge kontrole i mjere koje osiguravaju da podaci budu zaštićeni od neovlaštenog pristupa, curenja ili gubitka. To uključuje enkripciju podataka, upravljanje identitetima i pristupom, kontrolu prometa i redovite sigurnosne provjere. Međutim, stroge sigurnosne mjere mogu usporiti proces balansiranja opterećenja jer zahtijevaju dodatne provjere, autentifikaciju i inspekciju podataka prije nego što se promet može preusmjeriti ili resursi dinamički raspodijeliti. Jedan od glavnih izazova u balansiranju opterećenja i sigurnosti podataka je latencija koja može nastati zbog sigurnosnih provjera. Na primjer, ako se promet mora enkriptirati i dekriptirati pri svakom prelasku s jednog servera na drugi ili između različitih dijelova mreže, to može povećati vrijeme obrade i smanjiti ukupnu brzinu sustava. U slučajevima kada aplikacija zahtijeva nisku latenciju, kao što su aplikacije u stvarnom vremenu (npr. financijske transakcije ili video streamovi), sigurnosne mjere mogu postati prepreka postizanju željenih performansi (Krutz i sur., 2020).

Drugi izazov leži u upravljanju identitetima i kontrolama pristupa tijekom balansiranja opterećenja. U oblačnom okruženju, aplikacije i resursi često su raspodijeljeni na više servera i regija, što zahtijeva dinamično upravljanje korisničkim pristupima. Sigurnosni sustavi, poput upravljanja identitetima i pristupom (IAM), moraju se prilagoditi ovom dinamičkom okruženju i osigurati da ovlašteni korisnici imaju dosljedan pristup podacima, bez obzira na to gdje se resursi fizički nalaze. Međutim, s povećanjem broja resursa i korisnika, kontrola pristupa postaje sve složenija, što može stvoriti rizik od neusklađenosti i sigurnosnih propusta.

Pitanje geografske distribucije podataka predstavlja još jedan izazov u usklađivanju balansiranja opterećenja i sigurnosti. Pružatelji usluga oblaka često distribuiraju podatke na različitim geografskim lokacijama kako bi poboljšali performanse i osigurali otpornost sustava u slučaju lokalnih prekida. Međutim, ovo može predstavljati sigurnosni rizik, jer podaci mogu biti podložni različitim zakonskim okvirima o zaštiti privatnosti i suverenitetu podataka ovisno o zemlji u kojoj su pohranjeni. Organizacije moraju osigurati da balansiranje opterećenja ne kompromitira sigurnost podataka prenošenjem osjetljivih informacija u jurisdikcije koje ne zadovoljavaju njihove sigurnosne i regulatorne zahtjeve (Krutz i sur., 2020).

Dinamička skalabilnost koja je omogućena balansiranjem opterećenja također može predstavljati izazov u pogledu sigurnosti, posebno kada se koriste resursi u stvarnom vremenu. Kada oblačne platforme automatski povećavaju ili smanjuju resurse kako bi zadovoljile trenutne potrebe, potrebno je osigurati da svi novi ili privremeni resursi imaju odgovarajuće sigurnosne postavke. Ako se sigurnosne politike ne primijene konzistentno tijekom dinamičkog skaliranja, postoji rizik da će novi resursi biti podložni napadima ili sigurnosnim prijetnjama. Automatizacija sigurnosnih postavki i provjera integriteta postaje ključna kako bi se osiguralo da sigurnosne mjere prate dinamičke promjene u oblačnom okruženju. Usmjeravanje i analiza prometa tijekom balansiranja opterećenja može biti potencijalni izvor sigurnosnih ranjivosti. Balansiranje opterećenja često uključuje preusmjeravanje prometa između različitih dijelova mreže ili između različitih oblačnih usluga, a ako se taj promet ne prati i analizira u stvarnom vremenu, zlonamjerne aktivnosti mogu proći nezapaženo. Implementacija naprednih alata za praćenje i analizu prometa, poput sustava za otkrivanje upada (IDS) ili alata za analizu ponašanja mrežnog

prometa, može pomoći u prepoznavanju anomalija i potencijalnih prijetnji prije nego što one uzrokuju štetu (Dražić, 2022).

Održavanje ravnoteže između performansi i sigurnosti zahtijeva pristup u kojem automatizacija igra ključnu ulogu. Automatizirani sustavi mogu pomoći u osiguravanju da se sigurnosne postavke automatski primjenjuju na sve nove resurse, da se promet kontinuirano prati i analizira te da se podaci pravilno enkriptiraju i dekriptiraju bez ručnih intervencija. Automatizacija također omogućuje dosljednu primjenu sigurnosnih politika čak i u slučajevima kada se resursi brzo skaliraju ili se promet dinamično preusmjerava. Organizacije koje koriste računalne oblake moraju pažljivo planirati i implementirati strategije koje uravnotežuju visoke performanse sustava kroz balansiranje opterećenja s potrebom za strogo definiranom sigurnošću podataka. Ovaj proces uključuje kombinaciju naprednih tehnoloških rješenja, poput enkripcije, IAM sustava i alata za praćenje prometa, kao i razvoj odgovarajućih sigurnosnih politika koje prate dinamičnost oblačnog okruženja. Dugoročno, uspješno balansiranje između ovih dviju potreba omogućuje organizacijama da maksimalno iskoriste prednosti oblaka, istovremeno osiguravajući sigurnost svojih podataka.

4.2. Napredne metode autentifikacije i autorizacije

Napredne metode autentifikacije i autorizacije igraju ključnu ulogu u zaštiti digitalnih sustava, osobito u kontekstu računalnih oblaka i modernih IT okruženja. Kako se prijetnje postaju sve sofisticiranije, tradicionalni sustavi autentifikacije i autorizacije više nisu dovoljni za osiguravanje podataka i resursa. Napredne metode pružaju jaču zaštitu putem višeslojnih mehanizama, koristeći biometrijske podatke, kriptografske alate i metode stroge provjere identiteta korisnika. Ove tehnike omogućuju precizniju kontrolu nad pristupom podacima i aplikacijama, osiguravajući da samo ovlaštene osobe ili sustavi imaju pristup povjerljivim resursima (Krutz i sur., 2020).

1. Višefaktorska autentifikacija (MFA)

Višefaktorska autentifikacija (MFA) jedan je od najčešće korištenih naprednih pristupa autentifikaciji. Ova metoda zahtijeva od korisnika da potvrdi svoj identitet korištenjem barem dvaju različitih faktora iz tri osnovne kategorije:

Nešto što korisnik zna: Lozinka, PIN ili odgovori na sigurnosna pitanja.

Nešto što korisnik ima: Sigurnosni token, pametni telefon (s aplikacijama poput Google Authenticatora) ili pametna kartica.

Nešto što korisnik jest: Biometrijske značajke kao što su otisak prsta, prepoznavanje lica ili šarenice oka.

Kombiniranjem ovih faktora, MFA značajno povećava sigurnost jer čak i ako jedan faktor, poput lozinke, bude ugrožen, napadač neće moći pristupiti sustavu bez drugih potrebnih faktora. Ovaj sustav pruža snažnu zaštitu protiv krađe identiteta i neovlaštenih pristupa, te se koristi u mnogim osjetljivim aplikacijama poput bankarstva, zdravstva i korporativnih sustava.

2. Jednokratne lozinke (OTP) i aplikacije za autentifikaciju

Jednokratne lozinke (OTP) su dinamične lozinke koje vrijede samo za jednu sesiju ili transakciju. OTP sustavi generiraju nasumične kodove koje korisnici moraju unijeti prilikom prijave ili autorizacije osjetljivih radnji. Kodovi se mogu generirati putem SMS-a, emaila, ili sigurnosnih aplikacija poput Google Authenticatora ili Authy-ja.

OTP-ovi pružaju dodatnu sigurnost jer se, za razliku od statičnih lozinki, ne mogu ponovno upotrijebiti. Ako je OTP kompromitiran, napadač ne može koristiti isti kod ponovno, jer on vrijedi samo za ograničeno vrijeme (obično između 30 sekundi i jedne minute). OTP-ovi su često ključni dio višefaktorske autentifikacije.

3. Biometrijska autentifikacija

Biometrijska autentifikacija temelji se na fizičkim ili bihevioralnim karakteristikama korisnika kako bi potvrdila njegov identitet. Ova metoda postaje sve popularnija zahvaljujući napretku tehnologije prepoznavanja i širokoj dostupnosti biometrijskih

senzora na pametnim telefonima i drugim uređajima. Neke od najčešćih biometrijskih metoda uključuju:

Otisak prsta: Prepoznavanje jedinstvenog uzorka otiska prsta.

Prepoznavanje lica: Analiza i usporedba geometrijskih karakteristika lica.

Prepoznavanje šarenice ili mrežnice: Koristi jedinstveni uzorak šarenice ili krvnih žila mrežnice.

Prepoznavanje glasa: Analiza tonova i ritma govora.

Biometrijska autentifikacija nudi visoku razinu sigurnosti jer su biometrijski podaci jedinstveni za svaku osobu i teško ih je falsificirati. Ova metoda često se koristi u kombinaciji s drugim oblicima autentifikacije kako bi se osigurala dodatna zaštita (npr. MFA).

4. Jedinstvena prijava (SSO)

Jedinstvena prijava (Single Sign-On, SSO) omogućuje korisnicima da se autentificiraju jednom te da potom pristupe višestrukim aplikacijama ili sustavima bez potrebe za ponovnim unosom vjerodajnica. SSO se često koristi u korporativnim okruženjima kako bi se olakšalo upravljanje korisničkim pristupom i smanjilo administrativno opterećenje povezano s lozinkama.

SSO sustavi koriste standardizirane protokole poput OAuth, SAML (Security Assertion Markup Language) i OpenID Connect, koji omogućuju sigurno dijeljenje vjerodajnica između različitih sustava i aplikacija. SSO značajno poboljšava korisničko iskustvo, a istovremeno smanjuje rizik povezan s upravljanjem više lozinki. Međutim, kako bi bio siguran, SSO se često kombinira s MFA-om kako bi se spriječilo da kompromitacija jedne prijave otvori pristup svim povezanim sustavima.

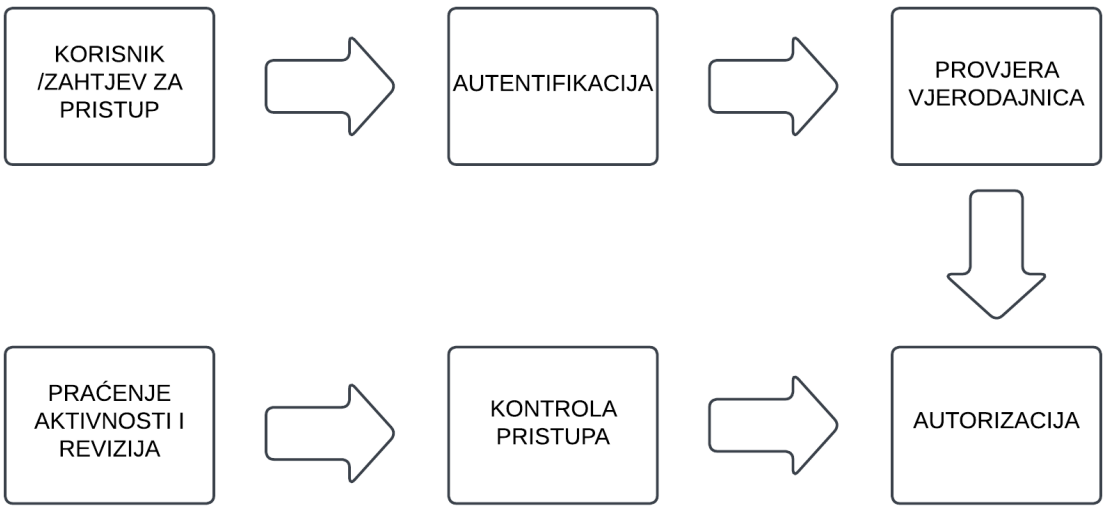
5. Autentifikacija temeljena na riziku

Autentifikacija temeljena na riziku koristi kontekstualne informacije i analizu ponašanja korisnika kako bi prilagodila razinu autentifikacije potrebnu za određene radnje. Ova metoda procjenjuje čimbenike poput lokacije prijave, korištenog uređaja, vremena prijave i uobičajenih obrazaca ponašanja korisnika. Ako sustav primijeti odstupanje od uobičajenih aktivnosti (npr. prijava iz nepoznate lokacije), može zahtijevati dodatnu autentifikaciju putem MFA-a.

Ovaj pristup pruža fleksibilnost jer omogućuje korisnicima nesmetan pristup u sigurnim okruženjima, dok se dodatne sigurnosne mjere primjenjuju samo kada postoji povećani rizik. Time se balansira između sigurnosti i korisničkog iskustva.

6. Autorizacija temeljena na atributima (ABAC)

Autorizacija temeljena na atributima (Attribute-Based Access Control, ABAC) sofisticirana je metoda kontrole pristupa koja koristi više parametara za određivanje tko može pristupiti određenim resursima. Umjesto da se pristup temelji isključivo na ulogama korisnika (kao u RBAC-u), ABAC koristi širok raspon atributa, uključujući korisničke informacije (npr. pozicija, odjel), vrstu resursa, vrijeme, lokaciju, i druge kontekstualne faktore (slika 4.).



Slika 5. Dijagram metoda autentifikacije i autorizacije

Izvor: vlastita izrada autora

ABAC omogućuje precizniju i dinamičniju kontrolu pristupa jer sustav donosi odluke na temelju specifičnih uvjeta i atributa korisnika. Ovo je posebno korisno u složenim IT okruženjima i oblačnim sustavima gdje različiti korisnici imaju različite razine pristupa ovisno o kontekstu.

7. Kriptografska autentifikacija

Kriptografska autentifikacija koristi kriptografske ključeve za provjeru identiteta korisnika. Javni ključ infrastrukture (PKI) sustav koristi se za digitalne potpise i certifikate kako bi se osigurala autentičnost komunikacije između korisnika i sustava. Korisnici posjeduju privatni ključ koji se koristi za digitalno potpisivanje podataka, dok se javni ključ koristi za verifikaciju potpisanih podataka. Ova metoda pruža visoku razinu sigurnosti i često se koristi u sigurnosno osjetljivim okruženjima poput financijskih transakcija i pravnih sustava.

Napredne metode autentifikacije i autorizacije postale su ključne za zaštitu modernih IT sustava. Višefaktorska autentifikacija, biometrijska autentifikacija, SSO, ABAC, i autentifikacija temeljena na riziku nude slojevit pristup sigurnosti koji osigurava da samo ovlašteni korisnici imaju pristup resursima. Kombiniranjem ovih tehnika organizacije mogu značajno smanjiti rizik od neovlaštenog pristupa i osigurati sigurnost podataka u dinamičnim i distribuiranim okruženjima.

4.3. Prevencija korupcije podataka

Prevencija korupcije podataka igra ključnu ulogu u osiguravanju integriteta, pouzdanosti i dugoročnog očuvanja podataka u različitim sustavima, uključujući računalne oblake, baze podataka, mrežne sustave i fizičke medije za pohranu. Korupcija podataka odnosi se na oštećenje ili neovlaštenu promjenu podataka, što može dovesti do gubitka vrijednih informacija, kompromitiranja sustava ili čak narušavanja poslovanja. Kako bi se spriječila korupcija podataka, organizacije koriste niz metoda i praksi koje osiguravaju integritet podataka tijekom njihovog stvaranja, prijenosa, pohrane i obrade (Krutz i sur., 2020).

1. Provjera integriteta podataka

Provjera integriteta podataka jedan je od osnovnih pristupa u prevenciji korupcije podataka. Koriste se tehnike kao što su kontrolne zbrojeve (checksums) i kripto-hash funkcije kako bi se osigurala dosljednost i točnost podataka. Ovi mehanizmi omogućuju stvaranje jedinstvenih oznaka (hash vrijednosti) za svaki skup podataka. Kada se podaci premještaju ili pohranjuju, sustav izračunava novu hash vrijednost i uspoređuje je s izvornom vrijednošću. Ako su vrijednosti iste, podaci nisu promijenjeni; ako su različite, to ukazuje na potencijalnu korupciju.

Najčešće korištene hash funkcije uključuju SHA-256 i MD5, koje stvaraju jedinstvene kodove temeljene na sadržaju podataka. Ove hash vrijednosti pomažu u otkrivanju bilo kakvih promjena u podacima tijekom prijenosa, kao što su neovlaštene izmjene ili oštećenje zbog tehničkih problema.

2. Redundancija i replikacija podataka

Jedan od najvažnijih mehanizama za prevenciju gubitka i korupcije podataka je redundancija. Redundancija znači pohranu više kopija podataka na različitim lokacijama ili u različitim formatima, kako bi se osiguralo da su podaci dostupni čak i u slučaju oštećenja jedne kopije. Replikacija podataka često se koristi u računalnim oblacima i distribuiranim sustavima gdje se podaci automatski repliciraju na više servera ili lokacija kako bi se spriječio gubitak podataka u slučaju kvara jednog sustava. U oblačnim sustavima, redundancija se često postiže pomoću geo-replikacije, gdje se podaci automatski pohranjuju u više podatkovnih centara diljem svijeta. Ako dođe do kvara ili korupcije podataka u jednom podatkovnom centru, sustav automatski prebacuje na drugu lokaciju, osiguravajući kontinuitet poslovanja i zaštitu podataka.

3. Sigurnosne kopije podataka

Redovito stvaranje sigurnosnih kopija (backup) ključna je metoda za osiguravanje da podaci ostanu netaknuti i dostupni u slučaju korupcije. Sigurnosne kopije omogućuju povratak na ranije, nekompromitirane verzije podataka u slučaju oštećenja, gubitka ili neovlaštenih izmjena. Preporučena praksa je primjena pravila 3-2-1, koje podrazumijeva:

Tri kopije podataka: Jedna primarna i dvije sigurnosne kopije.

Dva različita medija za pohranu: Na primjer, lokalni disk i oblak.

Jedna kopija izvan lokacije: Pohrana podataka na fizički odvojenom mjestu kako bi se osigurala zaštita od katastrofa poput požara, poplava ili kibernetičkih napada.

Kombinirajući lokalne sigurnosne kopije i oblačne sigurnosne kopije, organizacije mogu smanjiti rizik od gubitka ili korupcije podataka te osigurati njihov povratak u slučaju problema.

4. Detekcija i korekcija pogrešaka

Sustavi za otkrivanje i ispravljanje pogrešaka (Error Detection and Correction, EDC) koriste se za prepoznavanje i automatsku ispravku manjih pogrešaka u podacima. Ovi sustavi koriste različite tehnike, kao što su paritetni bitovi, kôdovi za ispravljanje pogrešaka (ECC) i složeniji algoritmi poput Hammingovih kôdova, koji omogućuju prepoznavanje i ispravljanje pogrešaka koje nastanu tijekom prijenosa ili pohrane podataka.

Kodovi za ispravljanje pogrešaka posebno su korisni u sustavima za pohranu podataka, kao što su RAID konfiguracije diskova. RAID (Redundant Array of Independent Disks) koristi redundanciju i distribuciju podataka na više diskova kako bi se smanjio rizik od gubitka podataka zbog kvara jednog diska. RAID sustavi s ECC-om mogu otkriti i ispraviti pogreške u pohranjenim podacima, čime se značajno smanjuje rizik od korupcije podataka.

5. Transakcijsko upravljanje i zaključavanje podataka

Transakcijski sustavi osmišljeni su kako bi osigurali integritet podataka tijekom njihovih ažuriranja i obrade. Korištenje transakcijskog upravljanja, posebno u bazama podataka, osigurava da se sve promjene podataka provode u cjelini, ili da se, u slučaju pogreške, sustav vrati u prethodno stanje. Ovaj princip poznat je kao ACID svojstva (Atomicity, Consistency, Isolation, Durability), koja jamče da se transakcije provode ispravno, bez nepotpunih ili korumpiranih podataka.

4.4. DDoS napadi

DDoS (Distributed Denial of Service) napadi predstavljaju ozbiljnu kibernetičku prijetnju usmjerenu na ometanje rada mreža, usluga i web stranica preplavljujući ih ogromnim količinama lažnog prometa s ciljem da ih učine nedostupnima legitimnim korisnicima. Ovi napadi koriste botnet mreže koje se sastoje od zaraženih uređaja, poznatih kao "zombiji", koji istovremeno šalju zahtjeve prema cilju. Razlikuju se po vrstama poput volumetrijskih napada, napada na mrežne protokole (npr. SYN flood) te aplikacijskih napada (npr. HTTP flood), a mogu uključivati i tehnike amplifikacije, gdje napadač koristi ranjive poslužitelje za pojačavanje prometa prema meti. Posljedice DDoS napada uključuju financijske gubitke, reputacijsku štetu i prekide poslovanja, osobito za tvrtke čije poslovanje ovisi o internetskim uslugama, kao što su banke, e-trgovine i organizacije pružatelji online usluga. Kako bi se obranile od ovih napada, organizacije koriste različite metode zaštite, uključujući mrežne vatrozide, sustave za balansiranje opterećenja, CDN mreže i cloud zaštitu, kao i IDS/IPS sustave za rano otkrivanje anomalija u prometu. Proaktivne strategije uključuju redovitu analizu mrežnog prometa, suradnju s pružateljima usluga interneta i računalnih oblaka te planiranje kapaciteta za apsorpciju velikih količina prometa. Kombinacija tehnoloških alata i pažljivog planiranja ključna je za ublažavanje utjecaja DDoS napada i osiguravanje kontinuiteta poslovanja unatoč prijetnjama.

Prevencija DDoS napada zahtijeva sustavan pristup i pripremu jer se oni mogu dogoditi iznenada i s različitim intenzitetima. Jedan od ključnih koraka je proaktivno praćenje mrežnog prometa kako bi se na vrijeme prepoznale nepravilnosti ili neuobičajeni obrasci koji ukazuju na početak DDoS napada. Ovo omogućava bržu reakciju i primjenu mjera za

ublažavanje napada. Osim toga, skalabilnost infrastrukture ključna je za minimiziranje učinka napada – tvrtke trebaju osigurati dovoljno mrežnih kapaciteta kako bi apsorbirale veće količine prometa, osobito kod volumetrijskih napada. Integracija s pružateljima usluga računalnih oblaka ili CDN mrežama, koje koriste distribuirane servere diljem svijeta, omogućuje raspršivanje napadačkog prometa na više lokacija i smanjenje opterećenja na pojedine sustave (Krutz i sur., 2020).

Pružatelji usluga interneta (ISP) i oblačnih usluga mogu pružiti napredne DDoS zaštitne usluge koje koriste tehnike filtriranja i blokiranja zlonamjernih zahtjeva prije nego što oni dosegnu ciljanu infrastrukturu. Tehnologije kao što su rate limiting i geografsko filtriranje omogućuju ograničavanje broja zahtjeva koji dolaze iz određenih geografskih područja ili IP adresa, što može biti posebno korisno u slučaju napada koji dolaze iz određenih dijelova svijeta. Automatizirani sustavi za otkrivanje i odgovor (IDS/IPS) omogućuju brzo reagiranje na sumnjive aktivnosti, blokirajući zlonamjerne IP adrese i filtrirajući lažne zahtjeve u stvarnom vremenu. Plan za upravljanje incidentima također je ključan za brzo reagiranje tijekom DDoS napada. Organizacije trebaju imati jasan plan koji uključuje korake za identificiranje napada, komunikaciju s ključnim dionicima, aktiviranje obrambenih mjera te eventualno angažiranje pružatelja usluga za DDoS zaštitu. Ovaj plan mora biti redovito ažuriran i testiran kroz simulacije kako bi se osiguralo da timovi zaduženi za sigurnost mogu brzo djelovati u slučaju napada. Uz tehničke mjere, edukacija zaposlenika o prepoznavanju i prijavljivanju sumnjivih aktivnosti također igra važnu ulogu u cjelokupnoj obrani organizacije (Krutz i sur., 2020).

DDoS napadi se neprestano razvijaju, a napadači koriste sve sofisticiranije metode za zaobilaženje obrane. Stoga, kombinacija više slojeva zaštite – uključujući mrežne alate, oblačne tehnologije, automatizirane sustave detekcije i ljudski nadzor – predstavlja najučinkovitiji pristup u suzbijanju ovih napada. Dugoročno, ulaganje u napredne zaštitne sustave i razvoj otpornosti na DDoS napade postaje sve važniji element u očuvanju poslovne kontinuiteta i zaštiti reputacije organizacija u digitalnom svijetu.

5. ZAKLJUČAK

Računalni oblak, iako donosi brojne prednosti poput fleksibilnosti, skalabilnosti i učinkovitosti, nosi sa sobom i niz sigurnosnih izazova. Kako bi se osigurala maksimalna povjerljivost, integritet i dostupnost podataka, neophodno je koristiti napredne metode zaštite, kao što su enkripcija, višefaktorska autentifikacija i stroga kontrola pristupa. Nadalje, organizacije moraju uzeti u obzir pravne i regulatorne okvire kako bi uskladile svoje operacije s propisima i standardima u industriji. Ovaj rad naglašava da uspješno upravljanje sigurnosnim aspektima u oblaku zahtijeva multidisciplinarni pristup koji obuhvaća tehničke, organizacijske i pravne mjere. Ovaj pristup omogućava organizacijama da iskoriste prednosti računalnih oblaka, smanjujući pritom rizike povezane s neovlaštenim pristupom, gubitkom podataka i potencijalnim napadima. Integracijom naprednih tehnoloških rješenja i pravovremenim odgovaranjem na sigurnosne prijetnje, moguće je osigurati stabilno i sigurno okruženje za poslovanje u oblaku.

LITERATURA

1. Bajaj, P., Arora, R., Khurana, M., & Mahajan, S. (2022). Cloud security: the future of data storage. In Cyber Security and Digital Forensics: Proceedings of ICCSDF 2021 (pp. 87-98). Springer Singapore.
2. Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2019). Cloud security: Emerging threats and current solutions. Computers & Electrical Engineering, 59, 126-140.
3. Dražić, B. (2022). Privatnost i sigurnost podataka u oblaku.
4. Khan, S., & AlAjmi, M. F. (2021). Cloud Computing Safety Concerns in Infrastructure as a Service. Research Journal of Recent Sciences ISSN, 2277, 2502.
5. Knoldus. (2024). Know about cloud computing (online). Dostupno na: https://blog.knoldus.com/know-about-cloud-computing-architecture/. Datum pristupa: 5. 10. 2024.
6. Krutz, R. L., Krutz, R. L., & Russell Dean Vines, R. D. V. (2020). Cloud security a comprehensive guide to secure cloud computing. Wiley.
7. Kulkarni, G., Chavan, N., Chandorkar, R., Waghmare, R., & Palwe, R. (2021). Cloud security challenges. In 2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA) (pp. 88-91). IEEE.
8. Microsoft. (2024). Security architecture design (online). Dostupno na: https://learn.microsoft.com/en-us/azure/architecture/guide/security/security-start-here. Datum pristupa: 6. 10. 2024.
9. Muttik, I., & Barton, C. (2019). Cloud security technologies. Information security technical report, 14(1), 1-6.
10. Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: a systematic review. IEEE Access, 9, 20717-20735.
11. Pokić, T. (2013). SIGURNOST PODATAKA U OBLAKU.
12. Tabrizchi, H., Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions". The Journal of Supercomputing. 76 (12): 9493–9532.

13. Thakare, V. R., & Singh, J. (2021). A study of computational trust models in cloud security. International Journal of Grid and High Performance Computing (IJGHPC), 13(3), 1-11.
14. Zhang, X., Du, H. T., Chen, J. Q., Lin, Y., & Zeng, L. J. (2021). Ensure data security in cloud storage. In 2011 International conference on network computing and information security (Vol. 1, pp. 284-287). IEEE.
15. Zou, P. X., Lun, P., Cipolla, D., & Mohamed, S. (2017). Cloud-based safety information and communication system in infrastructure construction. Safety science, 98, 50-69.
16. Zovko, I. (2017). Sigurnost i računarstvo u oblaku.

POPIS SLIKA

POPIS TABLICA