Sigurnosni aspekti privatnih računalnih oblaka

Tocko, Filip

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Filip Tocko

SIGURNOSNI ASPEKTI PRIVATNIH RAČUNALNIH OBLAKA

ZAVRŠNI RAD

Varaždin, 2021.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Filip Tocko

Matični broj: 0016137478

Studij: Informacijski sustavi

SIGURNOSNI ASPEKTI PRIVATNIH RAČUNALNIH OBLAKA

ZAVRŠNI RAD

Mentor:

Doc. dr. sc. Igor Tomičić

Varaždin, srpanj 2021.

Filip Tocko

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Tema i fokus rada su sigurnosni aspekti privatnih računalnih oblaka. U početku će se prvo detaljno opisati, općenita teorija vezana uz domenu, računarstva u oblaku. Ovo je potrebno za razumijevanje glavne teme rada. Nakon toga će se obraditi privatni oblaci i njihova sigurnost. Sigurnost privatnih oblaka će biti opisana u kontekstu: sigurnost podataka i informacija (InfoSec), API sigurnost i time će se također obuhvatiti upravljanje identitetom i pristupom. Penetracijsko testiranje oblaka, kao tema koja se nastavlja na sigurnost, će isto tako biti obrađena. U teorijskom dijelu će se zatim, prikazati tehnologije koje omogućuju implementaciju privatnih oblaka. Iste će biti sigurnosno uspoređene, pomoću komparativnih tabličnih analiza sa aspekta sigurnosti. U praktičnom dijelu će biti implementirano, nekoliko najčešće korištenih, ranije opisanih tehnologija (rješenja) za privatne oblake. Iste će biti prikazane i sigurnosno razrađene. Vidjet će se korisnost takvih rješenja, u smislu jednostavnosti, efikasnosti i pogodnosti jer omogućuju implementaciju „self-hosted“ privatnih oblaka, uz većinu sigurnosnih aspekata integriranih s istima. Na kraju će se izvesti zaključak, iz svega ranije navedenog i obrađenog.

Ključne riječi: računalni oblak, sigurnost, InfoSec, privatni oblak, sigurnost privatnih oblaka, računarstvo u oblaku, self-hosting.

Sadržaj

1. Uvod

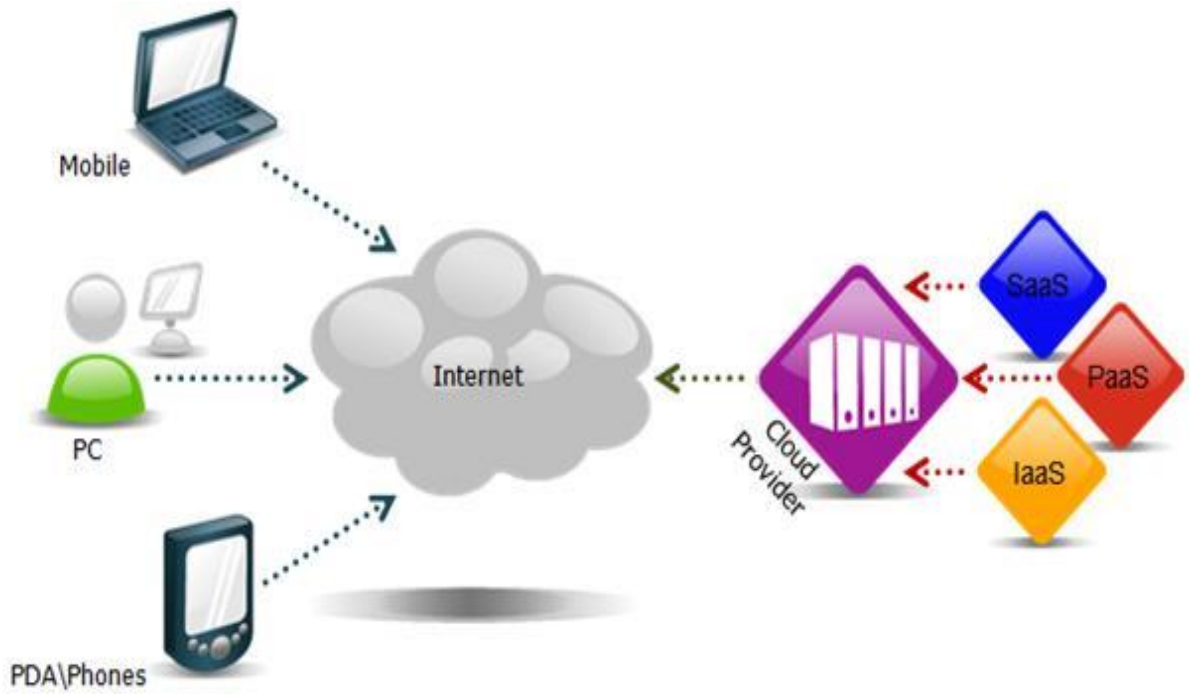
U ovom završnom radu će biti obrađena domena računarstva u oblaku s naglaskom na privatne računalne oblake i njihove sigurnosne aspekte. To je područje, koje se sve više razvija u svijetu računalstva i Interneta. Internet je svakako, najvažniji dio računarstva u oblaku. Ono se odnosi na pružanje različitih usluga putem Interneta, za šta se koriste sljedeći resursi poput: aplikacije i alati za pohranu podataka, poslužitelji, baze podataka, umrežavanje i softver [1]. Danas je vrlo korisno za učinkovitost poslovanja, osobnu pohranu podataka, sve s ciljem povećanja: produktivnosti, brzine, efikasnosti, perfomansi i sigurnosti [1]. Jednom riječju, računarstvo u oblaku bi se moglo opisati kao „korisničko, daljinsko upravljanje uslugom“, bez potrebe za vlastitim resursima osim Interneta. Ponekad, takvi vlastito pohranjeni, korisnički podaci, nisu u potpunosti sigurni od zlonamjernog korištenja. Zbog toga postoje privatni računalni oblaci, koji na neki način implementiraju sigurnost, u smislu sprječavanja zloupotrebe podataka. U ovom radu će biti obrađeni, tj. rad je fokusiran na sigurnosne aspekte privatnih računalnih oblaka: zaštita podataka u mirovanju i prijenosu (enkriptiranje i integritet podataka), autentifikacija i API sigurnost. Osim samog definiranja i opisivanja aspekata, isti će biti prikazani na primjeru tehnologija, koje omogućuje privatne računalne oblake. Sve više organizacija se orijentira prema implementiranju privatnih oblaka, s jasnom svrhom očuvanja sigurnosti, svih informacija vezanih uz poslovanje. Također i sve više korisnika traži određenu sigurnost, svojih podataka, pohranjenih u oblaku. Ovdje se jasno vidi razlog potrebe za implementacijom, privatnih računalnih oblaka.

Kada se određena IT infrastruktura usmjeri prema jednom korisniku ili organizaciji, uz izolirajući pristup, tada se radi o privatnim računalnim oblacima [2]. Dakle, organizacije žele izolirani pristup i pristup na zahtjev uslugama u oblaku, u kontekstu pružanja upravljanih usluga privatnih oblaka ili vlastito održavanje privatnih oblaka [2]. Sve se češće koristi kontekst, pružanja upravljanih usluga privatnih oblaka (upravljanje privatnim oblacima). Razlog tome je da se organizacije ne moraju brinuti oko održavanja virtualne infrastrukture za sigurnost, nego istima upravljaju drugi pružatelji takvih usluga pa tako organizacije mogu svu pažnju posvetiti svojem poslovanju uz uštedu novca i vremena [3]. Drugi kontekst, vlastitog održavanja privatnih oblaka se odnosi na vlastito implementiranje i održavanje privatnih oblaka. Krajnji korisnik može i sam implementirati privatni računalni oblak na svojem računalu, koristeći tehnologije poput: Seafile, ownCloud, Nextcloud, Pydio itd. Neka od navedenih rješenja će biti implementirana u radu i pritom će se prikazati njihove

sigurnosne komponente. Takva rješenja su vrlo korisna za korisnike i organizacije, ali zahtijevaju vrijeme, novac i potrebne kompetencije ljudi.

2. Računarstvo u oblaku

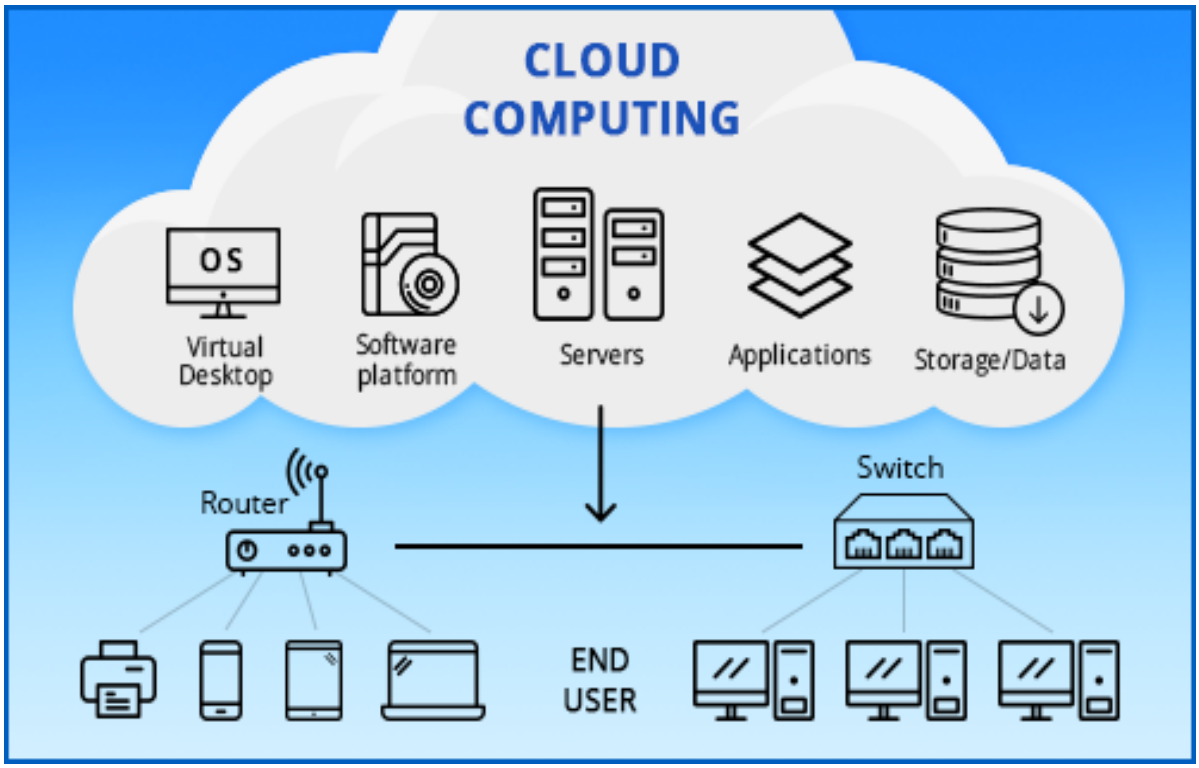
„Računarstvo u oblaku (eng. „*Cloud Computing*“) je pohrana i pristup podacima te programima putem Interneta bez korištenja HDD ili SSD računala“ [4]. Ovo područje se sve više razvija i koristi u području računalstva i Interneta. Pojam „oblak“ je metafora za Internet, jer se u domeni mreža računala, Internet prikazuje kao oblak [4]. Ovdje postoje dvije strane: pružatelj i korisnik računalnih oblaka. Pružatelj upravlja računalnim oblacima, tj. upravlja svim potrebnim resursima za isporuku usluge računarstva u oblaku. S druge strane, korisnik koristi te usluge u oblaku, kojima upravlja sam pružatelj. Dakle, korisnik pristupa uslugama u oblaku, koristeći stolno ili prijenosno računalo, pametni telefon, a pružatelj usluga u oblaku se brine oko održavanja i osiguravanja usluge na vrijeme i bez zastoja. Model usluga koji pritom pruža može biti: IaaS, PaaS i SaaS.



Slika 1. Prikaz računarstva u oblaku [5].

Arhitekturu računarstva o oblaku možemo podijeliti na: Front End i Back End [6]. Front End se odnosi na korisnika usluge i uključuje web-preglednike (Google Chrome, Mozila Firefox itd.) i korisničke uređaje (PC, smartphone itd.) preko kojih se može pristupiti platformi računarstva u oblaku [6]. Back End je dio pružatelja usluge, koji upravlja resursima poput: pohrana podataka, sigurnosni mehanizmi, virtualne mašine, mehanizmi za kontrolu prometa, poslužitelji itd., potrebnih za pružanje usluga u oblaku [6].

U Front End arhitekturu ubrajamo sljedeće komponente: infrastruktura klijenta, aplikacija kojoj se želi pristupiti i tip usluge (servisa) kojemu se želi pristupiti [6]. U Back End arhitekturu pripadaju: procesorsko vrijeme računalnih oblaka, pohrana podataka, infrastruktura (poslužitelji, pohrana podataka, mrežni uređaji, softver za virtualizaciju itd.), upravljanje (za koordinaciju i upravljanje svim ostalim komponentama), sigurnost (sigurnosni mehanizmi) i Internet (ubrajamo u Front End i Back End) [6]. Ovo je bazna arhitektura svakog tipa računalnog oblaka. Iz ovog se jasno vidi da je za pružanje usluga u oblaku, potrebno mnogo resursa, vremena i novca. Stoga je za korisnike i organizacije najpovoljnije i najefikasnije, koristiti usluge na zahtjev preko ugovora odnosno korištenje pružanja upravljanih usluga u oblaku.



Slika 2. Prikaz arhitekture računarstva u oblaku [7].

Iz gornje slike, sve što se nalazi unutar oblaka je dio Back End arhitekture, a ispod oblaka Front End arhitekture. Kao što je ranije navedeno, pružatelji usluga računarstva u oblaku su dio Back End arhitekture, a najpoznatiji u svijetu su: Microsoft Azure, Amazon Web Services, Google Cloud, Alibaba Cloud, IBM Cloud, Oracle, Salesforce [8]. Oni nude modele usluga: IaaS, PaaS i SaaS i usluge pohrane podataka te brojne druge usluge, ali su modeli usluga svakako dominantni predmet pružanja usluge računarstva u oblaku [8].

Slika 3. Najpoznatiji pružatelji usluge računarstva u oblaku [8].

Računarstvo u oblaku se osim ranije navedenih modela usluga koristi i za osobnu pohranu podataka. Naime, vrlo je pogodno i korisno pohranjivanje podataka u oblaku, gdje oni ostaju trajno, za razliku od pohrane na diskovima računala ili u memoriji ostalih uređaja. Međutim, ovdje se postavlja pitanje o sigurnosti tako spremljenih podataka u oblaku, što je ujedno i tema ovog završnog rada. Najpoznatiji pružatelji usluge pohrane podataka u oblaku su: pCloud, Zoolz Cloud Backup, Dropbox, Google Drive, iDrive, OneDrive [9]. Takva tehnologija pohrane podataka se drastično razvija i vrlo je popularna te sve više zamijenjuje USB stickove i tvrde diskove računala [9]. Ona je sada već uveliko razvijena i korištena.

2.1. Karakteristike

Računarstvo u oblaku ima mnoštvo zanimljivih karakteristika, koje su obećavajuće za budućnost IT aplikacija i usluga [4]. One su: usluga na zahtjev, isplativost, široki mrežni pristup (mobilnost), udruživanje resursa, brza elastičnost, odmjerena usluga, multitenacija, skalabilnost, pouzdanost, ekonomija razmjera, prilagođavanje, učinkovito korištenje resursa i virtualizacija [4]. Između svih prethodno navedenih karakteristika, postoji pet spomenutih, koje su najvažnije za računarstvo u oblaku [10].

Najvažnijih pet karakteristika računarstva u oblaku su:

- Usluga na zahtjev – korisnici sami pristupaju i upravljaju uslugom oblaka te im se ona dodijeljuje, bez potrebe za administratorima [4].

- Široki mrežni pristup (mobilnost) – korisnici mogu pristupiti uslugama oblaka s bilo koje lokacije i preko bilo kojeg tipa uređaja [4].

- Brza elastičnost – IT resursi se automatski brzo povećavaju (proširuju) kod potrebe i potražnje korisnika, a nakon toga se ponovo smanjuju [10].

- Udruživanje resursa – IT resursi (mreže, poslužitelji, pohrana podataka, aplikacije, usluge itd.) su podijeljeni između više korisnika i aplikacija na neograničeni način. Mnoštvo korisnika se poslužuje iz istog fizičkog resursa [10].

- Odmjerena usluga – resursi oblaka i usluge se nadziru, kontroliraju i optimiziraju, zbog tzv. „pay-per-use“ poslovnog modela. Korisnici plaćaju usluge u oblaku u skladu s ugovorom, na sličan način kao i npr. korištenje električne energije [4].

Ove opisane karakteristike na neki način definiraju i pobliže određuju računarstvo u oblaku.

2.2. Modeli usluga

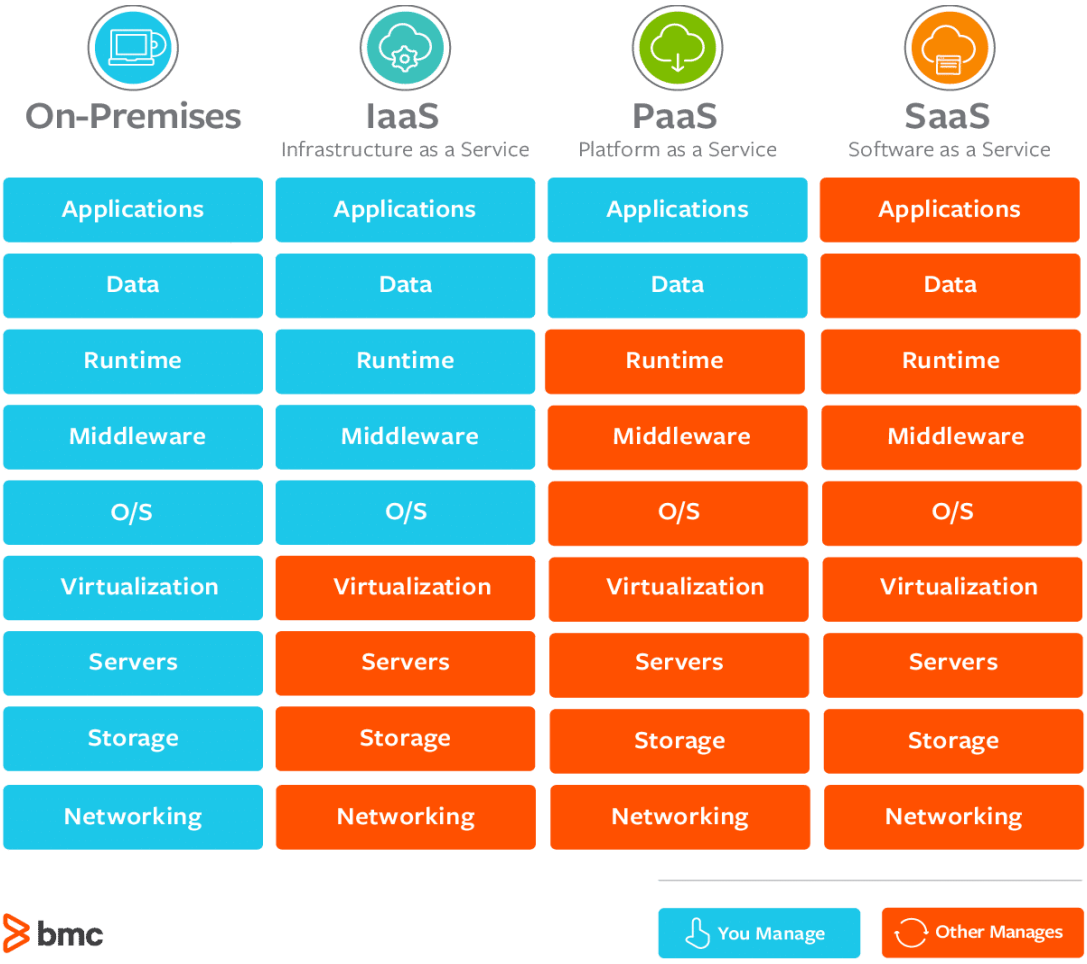
Pružatelj usluga računarstva u oblaku pruža korisniku, tri glavna modela usluge: Iaas, Paas i SaaS. Svaki od tih triju modela, pruža korisniku određeni opseg informacija i prava pristupa [11]. Modeli usluga uvelike olakšavaju poslovanje organizacijama, u smislu uštede novca i vremena te doprinose njihovoj poslovnoj učinkovitosti i uspješnosti. Korisnik (organizacija) sam odlučuje, koji model usluge želi, ovisno o poslovnoj potrebi. Iz modela usluga se jasno očituje, da je računarstvo mnogo složenija konfiguracija, za razliku od mikročipa ili smartphona [4]. Kod svih ovih modela usluga je upitna sigurnost za korisnika. Osim glavnih modela usluge, postoje i drugi modeli usluga, a oni su: pohrana podataka kao usluga (STaaS), sigurnost kao usluga (SECaaS), podaci kao usluga (DaaS), testno okruženje kao usluga (TeaaS) i Backend kao usluga (BaaS) [15]. Od ovih sporednih modela usluga, svakako je SECaaS vrlo važna. SECaaS je model usluge, gdje pružatelj usluge

integrira svoje sigurnosne usluge u infrastrukturu organizacija, što je za organizacije isplativije, nego izgradnja i održavanje vlastitih [15]. Najčešće uključene sigurnosne usluge su: autentifikacija, antivirusna i antišpijunska zaštita, prevencija nedopuštenog upada i upravljanje sigurnosnim događajem [15]. Danas, organizacije osim što žele efikasnije i ekonomičnije poslovati, žele također i sigurnosnu garanciju pružanih usluga, zbog privatnosti i zaštite informacija u vezi poslovanja. Tako da SECaaS, pogotovo u današnjem svijetu razvijenog računalstva, postaje sve važniji model usluge. Poslovni zahtjevi korisnika su sve više orijentirani, prema modelima usluga računarstva u oblaku. Pa tako računarstvo u oblaku, postaje dominantno korištena tehnologija, u svijetu poslovanja.

Slika 4. Prikaz modela usluge SECaaS [16].

Na donjoj slici se nalaze modeli usluga. Modeli usluga su definirani i određeni, pomoću količine resursa koju treba osigurati sam korisnik (plava boja) i količine resursa koju osigurava pružatelj usluge (narančasta boja). Sa slike se jasno vidi, da ako se ne koristi usluga računarstva u oblaku (On-Premises), tada korisnik sam treba osigurati sve potrebne resurse. Kod Iaas, PaaS i SaaS, pružatelj usluge osigurava različitu razinu (opseg) resursa korisniku. IaaS osigurava korisniku resurse: mrežna infrastruktura, pohrana podataka, poslužitelji i virtualizacija. PaaS osigurava korisniku sve resurse kao i Iaas, ali još dodatno resurse: procesorsko vrijeme, međuoprema i operacijski sustav. PaaS pruža više resursa

(usluga) u odnosu na IaaS. Saas pruža sve resurse kao i IaaS i Paas te dodatno resurse: aplikacije i podaci. Iz toga se jasno zaključuje, da najmanje usluga pruža IaaS, a najviše SaaS. Redoslijed: IaaS, PaaS i SaaS je rastući niz po broju osiguranih resursa (usluga). Kao što je ranije navedeno, korisnik sam odlučuje koju razinu usluge želi.



Slika 5. Modeli usluga [12].

2.2.1. IaaS

Model usluge IaaS (Infrastruktura kao usluga) nudi osnovne resurse: mrežna infrastruktura, pohrana podataka, poslužitelji i virtualizacija. IaaS omogućuje korisnicima kupnju resursa prema potrebi i zahtjevu, umjesto ulaganja u cjelokupnu infrastrukturu [13]. Resursi: mrežna infrastruktura, pohrana podataka i poslužitelji se isporučuju korisniku kroz tehnologiju za virtualizaciju (oblak) tj. korisnik dobiva potpunu kontrolu nad njima preko API-a [13]. Svi resursi se nalaze u oblaku i korisnik im pristupa po zahtjevu, bez potrebe za održavanjem istih. Dakle, IaaS pruža istu razinu usluge kao i tradicionalni podatkovni

centar, samo što je kod njega, on u virtualnom obliku u oblaku i njime upravlja pružatelj usluge, a ne sam korisnik [13].

Glavne prednosti IaaS-a su: smanjenje troškova ulaganja u kapital, plaćanje usluge po želji, povećanje ili smanjenje količine isporučenih resursa prema zahtjevu i potrebi korisnika u bilo kojem trenutku i pristup IT resursima na razini poduzeća te insfrastrukturi [4]. IaaS omogućuje organizacijama lakše, jefitinije i brže poslovanje. Organizacije ne trebaju brinuti oko održavanja i upravljanja infrastrukturom te ulaganja u istu, već je mogu koristiti prema potrebi, preko računalnog oblaka. To je danas standard, koji se snažno razvija i raste sve veća potražnja za njim. Primjeri IaaS-a su: DigitalOcean, Linode, Rackspace, Amazon Web Services, Cisco Metacloud, Microsoft Azure i Google Compute Engine [13].

2.2.2. PaaS

„Model usluge PaaS (Platforma kao usluga) je tipično, virtualizirano razvojno okruženje u oblaku“ [14]. PaaS nudi sve resurse iz modela usluge IaaS i još dodatno svoje resurse: međuoprema, procesorsko vrijeme, operacijski sustav, razvojni alati, usluge poslovne inteligencije, upravljanje bazama podataka i brojne druge [14]. PaaS je prvenstveno namijenjen organizacijama, koje razvijaju softverska rješenja. Hardver i softver se isporučuju virtualno preko računalnog oblaka. Time organizacije ne moraju brinuti oko nabave i angažiranja zaposlenika za održavanje istih [14]. PaaS omogućuje tvrtkama dizajniranje i izradu aplikacija, koje će biti ugrađene u sami s posebnim programskim komponentama [13]. Takve aplikacije su visoko dostupne i izrazito skalabilne [13].

Glavne prednosti PaaS-a su: povezivanje razvojnih timova kod izrade aplikacije, tj. stvaranje zajednice, gdje svi koriste istu uslugu, rasterećenje oko održavanja i ažuriranja infrastrukturnog softvera i smanjenje troškova ulaganja u hardver i softver, što rezultira manjim rizikom i potpunim fokusom na razvoj aplikacije [4]. Jednom riječju, PaaS se može opisati kao „virtualizirana platforma u oblaku za razvoj softvera“, koja olakšava tvrtkama poslovanje, kao i IaaS, samo uz veći broj usluga. Primjeri PaaS-a su: Windows Azure, Heroku, Force.com, Google App Engine, OpenShift i AWS Elastic Beanstalk [13].

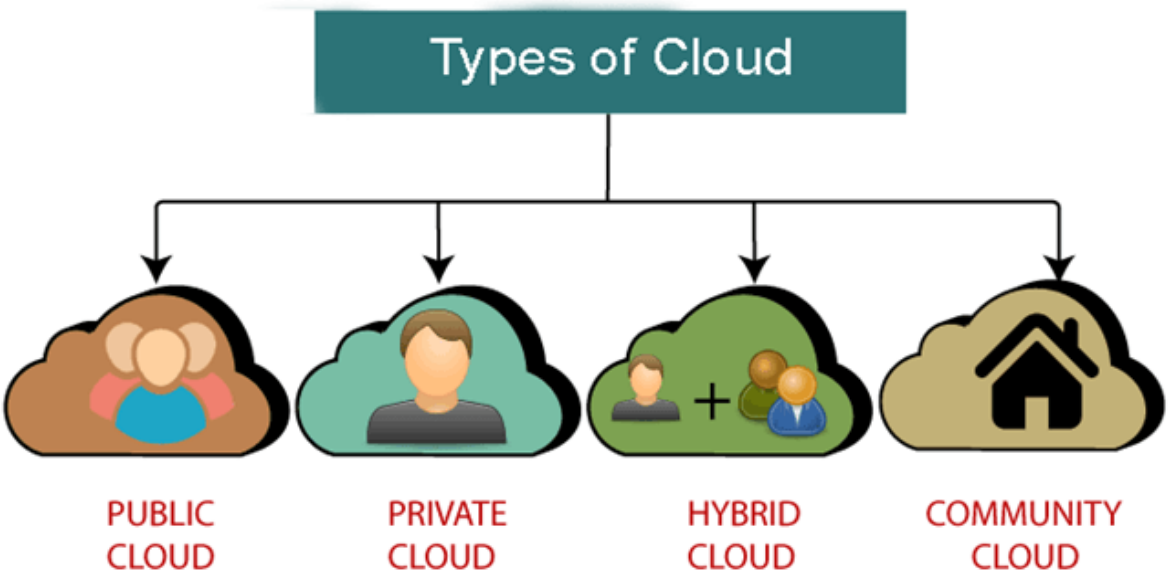
2.2.3. SaaS

„Model usluge SaaS (Softver kao usluga) je zapravo niz usluga aplikacije u oblaku i jedan je od najčešće korištenih opcija na tržištu računalnih oblaka“ [13]. Glavna svrha SaaS-a je isporuka aplikacije u oblaku korisnicima. Pružatelj usluge se brine oko održavanje i upravljanja tom uslugom, a korisnik je koristi preko Internetski orijentiranog sučelja aplikacije [4]. Osim aplikacije, SaaS osigurava sve resurse iz modela usluga: IaaS i PaaS, na kojima se nalazi aplikacija. SaaS time nudi najveću količinu usluga. Većina isporučenih aplikacija u oblaku, pripada tipu aplikacija krajnjih korisnika [12]. Tipično područje korištenja SaaS-a je upravljanje odnosima s kupcima (CRM) temeljenog na webu, bez potrebe za ažuriranjem softvera na najnoviju verziju, održavanjem poslužitelja i operacijskog sustava [12].

Glavne prednosti SaaS-a su: brza skalabilnost, pristup s bilo koje lokacije putem Interneta, otklanjanje zabrinutosti oko infrastrukture, održavanje i podrška u paketu i prilagođene razine usluga [4]. SaaS je orijentiranim prema krajnjim korisnicima i fazi održavanja i korištenja tvrtka (uslužna potpora i isporuka usluga krajnjim korisnicima od strane uslužnih tvrtka). Primjeri SaaS-a su: Google Workspace, Dropbox, Salesforce, Cisco WebEx, SAP Concur i GoToMeeting [13].

2.3. Tipovi računalnih oblaka

Tržište računalnih oblaka je brzo rastuće i sve više zastupljeno u poslovanju. Dolazi do sve veće, potražnje za pohranom i infrastrukturom preko oblaka, zbog efikasnosti i ekonomičnosti [4]. Glavni kapacitet, koji pružatelj usluga osigurava, je pružanje resursa poput hardvera i softvera preko Interneta [4]. Korisnicima se isporučuju u oblaku i brojni drugi resursi. Postoje različite izvedbe računalnih oblaka, koje se koriste ovisno o kontekstu uporabe i potrebe. Tipovi (izvedbe) računalnih oblaka su: javni, privatni, hibridni i oblak zajednice [6].



Slika 6. Prikaz tipova računalnih oblaka [6].

2.3.1. Javni oblak

Javni oblak je tip računalnog oblaka, koji je namijenjen bilo kojoj organizaciji i isporuka infrastrukture i usluga je javna te se ti resursi dijele, između ljudi diljem svijeta [4]. Takvi oblaci su široko dostupni pa ih mogu koristiti gotovo svi korisnici. Sva kontrola, Back End arhitekture oblaka je u rukama pružatelja usluga.

Glavne prednosti javnog oblaka su: jeftiniji od ostalih tipova oblaka, cjelokupno održavanje oblaka pod kontrolom pružatelja usluga, lakše se integrira pa potrošačima nudi fleksibilniji pristup, neovisan o lokaciji, izrazito velika skalabilnost po zahtjevu računalnih resursa i dostupnost širokoj populaciji svijeta pa nema ograničenja broja korisnika [6].

Nedostaci javnog oblaka su: slaba sigurnost zbog javnog dijeljenja resursa, perfomanse ovise o brzini korisničkog Interneta i korisnik nema kontrolu nad podacima [6].

Iz ovog se jasno očituje, da javni oblak nudi mnoštvo pogodnosti, međutim sigurnost je vrlo mala pa stoga i garancija nad korisničkim podacima. Isto tako je upitna, prikladnost za poslovanje organizacija. Više je namijenjen običnim korisnicima, koji zajedno koriste te usluge. Primjeri javnih oblaka su općenito, javno dostupne usluge računarstva u oblaku. Neke od njih su: Amazon Elastic Compute Cloud (EC2), Microsoft Azure, IBM's Blue Cloud, Sun Cloud, and Google Cloud [6].

2.3.2. Privatni oblak

Privatni oblak je tip računalnog oblaka, namijenjen specifičnoj organizaciji. Glavna karakteristika istog je visoka sigurnost i privatnost. „Naziva se još interni ili korporativni oblak“ [6]. Usluge samoga se pružaju preko interne mreže organizacije, odabranim korisnicima [6]. Vrlo je pogodan za poslovanje organizacija i sve se više koristi u tom segmentu. Sigurnost i privatnost se ostvaruju pomoću vatroštita i internog hostinga te također osigurava da osjetljivi podaci nisu dostupni trećoj strani [6].

Glavne prednosti privatnog oblaka su: veća kontrola nad resursima zbog prava pristupa odabranim korisnicima, visoka sigurnost i privatnost i bolje perfomanse (veće brzine i prostorni kapacitet) [6].

Nedostaci privatnog oblaka su: izrazito visoka cijena, ograničeno područje djelovanja (dostupan samo unutar organizacije), ograničena skalabilnost i potreba za kvalificiranim ljudima zbog održavanja i upravljanja uslugama u oblaku [6].

Dakle, kada se govori o privatnim oblacima, misli se na orijentiranost prema specifičnoj organizaciji i sigurnost. Ovakav tip oblaka, mnoge organizacije preferiraju, zbog sigurnosti i izolacije informacija u vezi poslovanja. Tipični primjeri istih su: HP Data Centers, Microsoft, Elastra-private cloud i Ubuntu [6]. Ovaj tip oblaka će u nastavku, biti detaljno analiziran i opisan, s naglaskom na najvažniju komponentu istoga, sigurnost.

2.3.3. Hibridni oblak

„Hibridni oblak je kombinacija javnog i privatnog oblaka“ [4]. „Sve nekritične aktivnosti obavlja javni oblak, a kritične aktivnosti privatni oblak“ [6]. Glavna svrha ovog tipa oblaka je da se objedine prednosti privatnih i javnih oblaka te se implementira zadovoljavajuće okruženje. Najčešće se koristi u područjima: financije, zdravstvo i sveučilište [6]. Korisnici takvih oblaka su organizacije i krajnji korisnici usluga.

Glavne prednosti hibridnog oblaka su: fleksibilnost i sigurnost (sadrži usluge privatnog oblaka), jeftiniji od privatnog oblaka, pružanje usluga javnog i privatnog oblaka i pogodan za upravljanje rizikom kod organizacija [6].

Nedostaci hibridnog oblaka su: mrežni problemi zbog složenosti i kombiniranja privatnog i javnog oblaka, problem kompatibilnosti infrastrukture (privatni oblak pod kontrolom organizacije, a javni oblak pod kontrolom treće strane) i pouzdanost ovisi o pružateljima usluga u oblaku [6].

Iako bi hibridni oblak trebao biti savršeni primjerak računalnog oblaka, isti ima mnogo poteškoća kod kompatibilnosti i mreže. Međutim, on se i dalje koristi, ali ne u tolikoj mjeri, koliko bi se koristio, da je bez nedostataka. Najbolji pružatelji takvih oblaka su: Amazon, Microsoft, Google, Cisco i NetApp [6].

2.3.4. Oblak zajednice

„Oblak zajednice je tip oblaka, koji se pruža organizacijama sa sličnim interesima (zajednica)“ [4]. Upravljanje, koordiniranje i vlasništvo samog oblaka, može biti pod kontrolom više organizacija u zajednici, treće strane ili kombinacije prethodno navedenog [6]. Koristan je kod poslovanja između poslovnih partnera (organizacija).

Glavne prednosti oblaka zajednice su: isplativost zbog podjele financija između organizacija u zajednici, fleksibilnost i skalabilnost, veća sigurnost od javnog oblaka, ali manja od privatnog i dijeljenje infrastrukture, resursa i informacija između svih u zajednici [6].

Nedostaci oblaka zajednice su: nije prikladan za svaku organizaciju, fiksna količina pohrane podataka i propusnosti je podijeljena između svih sudionika zajednice, skuplji od javnog oblaka, teža podjela odgovornosti između organizacija i slabo usvajanje podataka [6].

Ovakav tip oblaka je pogodan, za sve one organizacije, koje posluju u zajednici i preferiraju takav način poslovanja. Sigurnost takvih oblaka je veća od javnih i hibridnih oblaka, a manja od privatnih. Može se reći da ovaj oblak, pruža sasvim korektnu sigurnost.

2.4. Sigurnosne komponente i rizici

Računarstvo u oblaku je sve više zastupljena tehnologija u svijetu poslovanja. Porastom broja usluga i sve većim razvojem istoga, dolazi do sve većih sigurnosnih prijetnji. Ono postaje glavna meta hakera jer sadrži mnogo osobnih i poslovnih informacija i podataka. Zato korisnici zahtijevaju, određenu sigurnost svojih podataka. Što se tiče javnih oblaka, vrlo je teško osigurati potpunu sigurnost jer se isti dijeli između korisnika diljem svijeta i upravljanje sigurnosnim mehanizmima, bi bilo izrazito skupo i zahtjevno. Zbog toga su se razvili privatni oblaci, koji služe upravo toj svrsi. Ako organizacije odaberu model usluge IaaS od pružatelja usluga, tada se podrazumijeva, da one same upravljaju većim dijelom sigurnosti jer se većina sigurnosnih značajki nalazi u softveru, a pružatelj usluge samo isporučuje infrastrukturu [17]. Ukoliko organizacija odabere model usluge SaaS, tada je pružatelj usluge, zadužen za sigurnost aplikacija i podataka, a organizacija ima manje posla i kontrole nad sigurnošću [17]. Za pružanje upravljanih usluga u oblaku, svi sigurnosni mehanizmi su pod kontrolom pružatelja usluge, što ne garantira potpunu sigurnost informacija [17]. Zato bi organizacije trebale voditi računa o arhitekturi računalnih oblaka, kako bi bile upoznate i svjesne s mogućim sigurnosnim prijetnjama. Time bi one mogle znati, gdje je još potrebno, osigurati određenu razinu izolacije i zaštite [17].

Za sigurnost usluge računarstva u oblaku su najčešće zaduženi: organizacija i pružatelj usluge [18]. Kao što je ranije navedeno, sigurnost aplikacija, podataka i informacija je ključna. Postoje 4 vrste sigurnosnih kontrola, koje se koriste kod zaštite računalnih oblaka i često se koristi samo jedna od njih [18]. One su:

- Kontrole odvraćanja – upozoravaju na posljedice zbog uzrokovanja sigurnosnih prijetnji i prate prošle aktivnosti zaposlenika, jer su oni moguća unutarnja prijetnja sigurnosti [18].

- Preventivne kontrole – one uključuju radnje uklanjanja ranjivosti sustava računalnih oblaka poput: pisanje programskog koda, koji isključuje neaktivne portove i time onemogućava ulazne točke za hakere, održavanje snažnog sustava autentifikacije [18].

- Kontrole detekcije – uključuju identificiranje i reagiranje na sigurnosne prijetnje i događaje [18]. Za to koriste sustave za otkrivanje napada i razne mrežne nadzorne alate [18].

- Korektivne kontrole – aktiviraju se prilikom sigurnosnog napada [18]. Njihova uloga je smanjenje štete od nastalog napada i pisanje koda, koji će u slučaju istoga, odspojiti podatkovne poslužitelje iz mreže, zbog prevencije gubitka podataka [18].

Iz ovoga se jasno zaključuje, da sve sigurnosne kontrole, nastoje spriječiti sigurnosne prijetnje, a organizacija i pružatelj usluge sami biraju jednu od njih ovisno o potrebi i važnosti. Preventivne kontrole bi trebale nuditi najveću razinu zaštite. Uspješan tim za sigurnost bi trebao spriječiti događanje napada, brzo reagirati na iste i smanjiti njihov utjecaj te ponovno uspostaviti funkcionalnu i stabilnu uslugu oblaka [18].

2.4.1. Sigurnosne komponente

Postoji nekoliko sigurnosnih komponenata, koje se mogu implementirati, unutar usluge računarstva u oblaku. One su:

- Segmentacija mreže – kada se pruža ista usluga SaaS više korisnika, tada je potrebno odrediti i izolirati korisničke podatke od vlastitih (podataka pružatelja usluge) [18].

- Upravljanje pristupom – lagano za implementiranje, odnosi se na pristup uslugama u oblaku od strane korisnika, ovisno o ulogama i to se cijelo vrijeme nadzire i revidira [18].

- Kontrola lozinke – osnovni sigurnosni protokol računarstva u oblaku [18]. Ovdje nije poželjno koristiti dijeljene lozinke, nego iste kombinirati s alatima za autentifikaciju [18].

- Enkriptiranje podataka – kriptiranje podataka u mirovanju i prijenosu [18]. Vrlo visoka razina sigurnosti.

- Skeniranje i upravljanje ranjivostima – redoviti sigurnosni pregledi i popravljanje mogućih ranjivosti sustava [18].

- Upravljanje neprekidnošću usluge – uspostavljanje plana i alternativne platforme za sigurnosno kopiranje, zadržavanje i oporavak podataka [18].

- Sigurnosno nadziranje, bilježenje i upozoravanje – stalno praćenje svih usluga računarstva u oblaku, a za tu svrhu se sve više koristi platforma Sumo Logic [18].

Za potpunu sigurnost računalnih oblaka, potrebno je implementirati većinu sigurnosnih komponenata. To predstavlja veliki izazov za organizacije, zbog izrazito velike cijene i potrebe za kvalificiranim ljudima. Organizacije danas većinom koriste pružanje upravljanih usluga u oblaku pa je sigurnost prepuštena pružatelju usluge. To za organizacije i nije baš najveća garancija sigurnosti podataka i informacija u vezi poslovanja. Na neki način, moguće rješenje za ove probleme je platforma Sumo Logic. Navedena platforma analizira, prikuplja i bilježi sve podatke i događaje iz računalnih oblaka te pomoću njih nastoji identificirati sigurnosne prijetnje [18]. Nudi organizacijama također, veću vidljivost i kontrolu nad infrastrukturom oblaka [18]. Iz ovog se jasno očituje, da je opisana platforma vrlo pogodna za organizacije. Najčešće se kombinira s hibridnim oblacima, koji imaju srednju razinu sigurnosti [4].

Postoji i 5 elemenata sigurnosti računalnih oblaka, koji su na neki način povezani sa sigurnosnim komponentama i organizacije bi ih trebale osigurati. Oni su: sve veća važnost sigurnosti računalnih oblaka porastom broja hakerskih napada, sigurnost počinje izgradnjom sigurnosti arhitekture oblaka (vatroštit i sustavi za prevenciju nedopuštenog upada), poštivanje i provjera standarda privatnosti u zemljama svojih korisnika, nadzor i vidljivost su ključni za pravovremeno otkrivanje napada i sustavi autentifikacije kao prva linija obrane od napada [17].

2.4.2. Sigurnosni rizici

Računarstvo u oblaku sadrži sigurnosne rizike, koji se najviše odnose na korisnike. Oni proizlaze iz rastućeg broja sigurnosnih napada. Korisnici su naravno zabrinuti za sigurnost svojih podataka i informacija. Prema Gartneru postoji nekoliko sigurnosnih rizika računalnih oblaka, a oni su: nepovlašteni pristup korisniku (manjak informacija o ljudima,

koji upravljaju oblacima korisnika), odgovornost korisnika za sigurnost i integritet podataka, iako ne upravljaju njima, korisnik ne može znati, gdje su mu u oblaku pohranjeni podaci, šifriranje korisničkih podataka nije uvijek sigurno, pogotovo kod šifriranja u stanju mirovanja, gdje može doći do otežane dostupnosti, korisnici ne znaju, što će se dogoditi s njihovim podacima u slučaju katastrofe ili napada, vrlo otežano istraživanje neprimjerenih i ilegalnih aktivnosti jer se smještaj korisničkih podataka, stalno mijenja na drugi skup podatkovnih poslužitelja i pitanje dugoročne održivosti usluge računarstva u oblaku [19].

Općeniti sigurnosni rizici računarstva u oblaku su: gubitak podataka (prilikom hakerskih napada ili neispravnosti arhitekture oblaka), hakirana sučelja i nesigurni API, kršenje podataka (treća strana bez ikakvog odobrenja, pregledava ili krade povjerljive podatke i pritom hakeri hakiraju podatke organizacije), prijenos usluga organizacija s jednog dobavljača prema drugom dobavljaču oblaka, povećana složenost opterećuje zaposlenike za održavanje usluga u oblaku, napadi uskraćivanja usluga legitimnim korisnicima (tzv. DoS), krađa korisničkog računa i „Spectre&Meltdown“ [6].

Ovakvi sigurnosni rizici se javljaju većinom kod javnih oblaka. Vrlo je važno za napomenuti, da je korisnik upućen prema istima, prihvaćanjem uvjeta korištenja računalnih oblaka. Svakako, idealno rješenje za eliminiranje sigurnosnih rizika, bi bilo implementiranje privatnih oblaka, ali je znatno skuplje i manje fleksibilno od javnih oblaka.

2.5. Pozitivne i negativne značajke

Računarstvo u oblaku je tehnologija koja je u visoravni produktivnosti, što se tiče životnog ciklusa suvremenih tehnologija. Ona je ušla u sastavne dijelove našeg života i znatno je olakšala poslovanje. Prema tome, ona sadrži mnoštvo pozitivnih značajki. Neovisna je o jačini hardvera i softvera koji se posjeduje, već je za istu potrebna, samo dobra brzina Interneta. To je ujedno glavna prednost same.

Pozitivne značajke računarstva u oblaku su: sigurnosna kopija i vraćanje podataka pomoću oblaka, poboljšana kolaboracija između ljudi, zbog mogućnosti dijeljenja informacija putem zajedničke pohrane, odlična pristupačnost (moguće pristupiti usluzi iz bilo koje lokacije i u bilo koje vrijeme), smanjenje troškova održavanja za organizacije, mobilnost (pristup usluzi preko mobilnog uređaja), plaćanje usluge ovisno o korištenju

odnosno tzv. „pay-per-use“ model plaćanja, neograničeni kapacitet za pohranu na jednom mjestu i sigurnost podataka (privatni oblaci) [6].

Iako sadrži mnoge pozitivne značajke, postoje i neki nedostaci, koji se nipošto ne smiju zanemariti. Nedostaci su: oblaku se ne može pristupiti bez pristupa Internetu, prijenos usluga organizacije iz jednog dobavljača usluge prema drugome, ako oni koriste različite cloud tehnologije, ograničena kontrola nad uslugom oblaka (njome u potpunosti upravlja pružatelj usluga) i upitna sigurnost, osjetljivih poslovnih informacija organizacija, koje su pohranjene kod pružatelja usluge [6].

2.6. Povijesni osvrt

Računarstvo u oblaku se postepeno razvijalo, tj. evoluiralo iz različitih vrsta tehnologija poput: mrežnog računarstva, uslužnog računarstva, pružanje usluga aplikacije i softver kao usluga [20]. Sada je ono postalo samostalna vrsta tehnologije, koja integrira ranije navedene tehnologije. Smatra se najinovativnijom tehnologijom našeg vremena [20]. Prva naznaka istog je bila ranih 1960-ih, idejom informatičara Johna McCarthya, koji je predložio koncept dijeljenja vremena i iznio tezu, da se računarstvo može prodavati kao usluga, slično prodaji struje i vode [6]. Teza se pokazala istinitom 1999. godine, kada je tvrtka Salesforce.com, počela sa isporukom aplikacija korisnicima preko Interneta [6]. Prije 1999. godine, ideja o „Intergalaktičnoj računalnoj mreži“ i razvoj softvera za virtualizaciju (npr. VMware) su također doprinijeli razvoju računalnih oblaka [20]. Tvrtka Amazon je prva započela isporuku usluge računarstva u oblaku još 2002. godine, a komercijalno dostupna svima je bila 2006. godine, pod nazivom „Elastic Compute Cloud“ [6]. Kasnije su ostale tvrtke: Google, Microsoft, Oracle, HP itd., počele razvijati i isporučivati usluge u oblaku [6]. Tako je računarstvo u oblaku postao standard u svijetu računalne tehnologije.

2.7. Razlozi potrebe za domenom

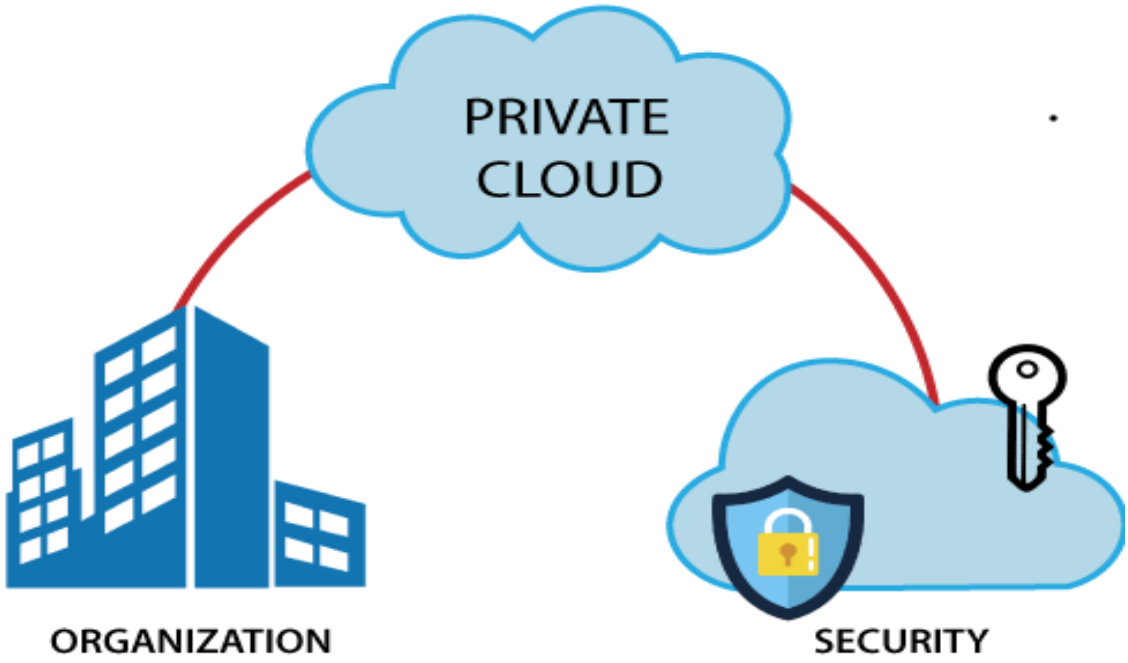
Kao što je ranije opisano, računarstvo u oblaku je vrlo važna tehnologija u svijetu računalstva. Uvelike je promijenio način poslovanja organizacija i ono je budućnost računalnog svijeta. Vrlo je potrebno i korisno za tehnologije, kao što su: Big Data i Internet of Things. Najvažniji razlozi potrebe za istim su: jednostavnija i sigurnija pohrana podataka, korištenje i testiranje softvera preko Interneta, veća efikasnost i lakše poslovanje za organizacije (nisu obvezne održavati i ulagati u infrastrukturu, nego je koriste prema potrebi,

preko oblaka) i upravljanje neprekidnošću usluge. Isto tako je važno, da ona organizacija, koja koristi usluge oblaka ima stratešku prednost na tržištu. U budućnosti se očekuje još veći razvoj računalnih oblaka, a najviše u području sigurnosti.

3. Privatni oblaci

Privatni oblak je tip računalnog oblaka, gdje se svi resursi i usluge oblaka isporučuju virtualno preko Interneta, točno određenoj organizaciji, pritom se koristi interni hosting organizacije i vlastiti Internet i podatkovni centar [21]. Dakle, sve usluge oblaka su ekskluzivne za određenu organizaciju, u odnosu na javni oblak, gdje iste usluge koristi više korisnika (organizacija) [21]. Glavni razlog implementiranja privatnog oblaka leži u sigurnosti i izolaciji poslovnih, privatnih i osjetljivih informacija. Organizacije žele sigurnost svojih internih informacija vezanih uz poslovanje, bez dijeljenja istih s drugim organizacijama, tj. korištenja javnog oblaka. Isto tako obični korisnici, kod pohrane privatnih podataka, žele određenu dozu privatnosti i sigurnosti. Iz toga se zaključuje, da je sigurnosna komponenta, najvažniji dio privatnih oblaka. Drugi naziv privatnog oblaka je interni ili korporativni oblak [6]. To jasno upućuje na činjenicu, da je namijenjen određenoj korporaciji ili korisniku.

Kod privatnih oblaka, uslugama se pristupa preko privatne (sigurne) mreže organizacije, a zaštićene su vatroštitom [21]. Privatni oblak ima baznu arhitekturu: Front End i Back End istu, kao i ostali tipovi oblaka. Svi resursi i usluge se kombiniraju u zajedničke bazene i isporučuju pomoću softvera za virtualizaciju [21]. Specifičnost u tome je, da se pritom koristi Internet tvrtke ili virtualna privatna mreža (VPN) [21]. Ugrađivanje sigurnosnih mehanizama je također još jedna specifičnost. Vlasnik (organizacija) privatnog oblaka u potpunosti kontrolira isti i time može osigurati veću sigurnost i skalabilnost, ali to zahtijeva određenu stručnost i kompetencije ljudi. Privatne oblake koriste one organizacije, kojima je potrebna tajnost i sigurnost podataka, kao npr. zdravstvene ustanove i njima je ovaj tip oblaka jedina opcija [22]. Organizacije isto tako, same trebaju procijeniti potrebu za ovom vrstom oblaka [22]. Privatnim oblacima su organizacijama osigurani vlastiti cloud poslužitelji, što daje veću kontrolu, sigurnost i prilagodbu (personalizaciju). Ukoliko krajnji korisnik ima problem s pouzdanošću i povjerljivošću javnih oblaka, on može sam u svojem domu, implementirati privatni oblak koristeći tehnologije poput: Seafile, ownCloud, NextCloud itd. Takva rješenja su izrazito korisna i vrlo pogodna.



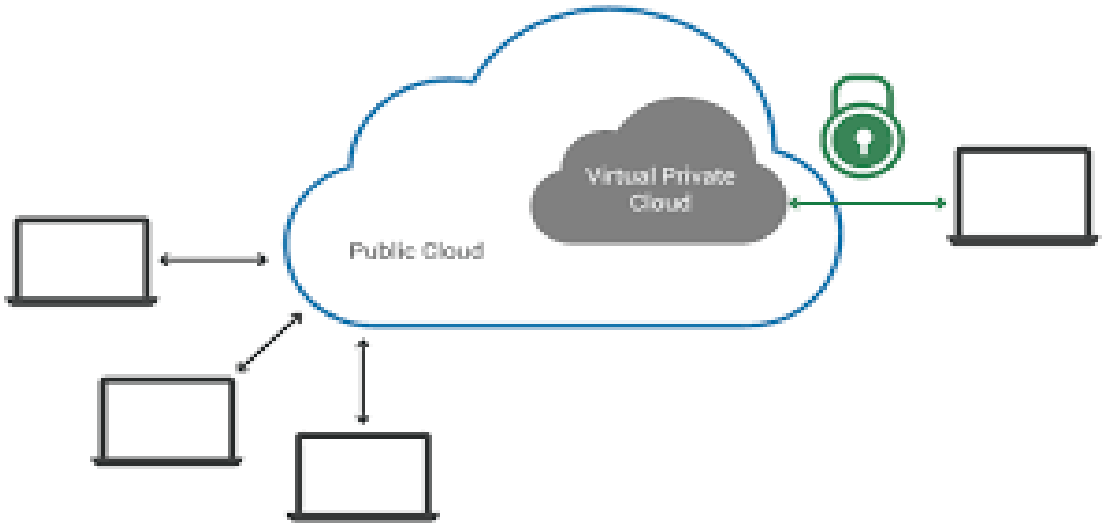
Slika 7. Privatni oblak [6].

Gornja slika jasno prikazuje, specifičnosti privatnih oblaka: orijentiranost određenoj organizaciji i sigurnost. Nedostaci takvim specifičnostima su: potreba za kvalificiranim ljudima, pružatelj usluga ima visoke troškove održavanja, nabave, uvođenja i podrške, hosting privatnih oblaka od treće strane, zahtijeva pretplatu korisnika (organizacija), što može biti vrlo skupo za iste [23]. Prilagođena okruženja se također osiguravaju privatnim oblacima.

3.1. Tipovi privatnih oblaka

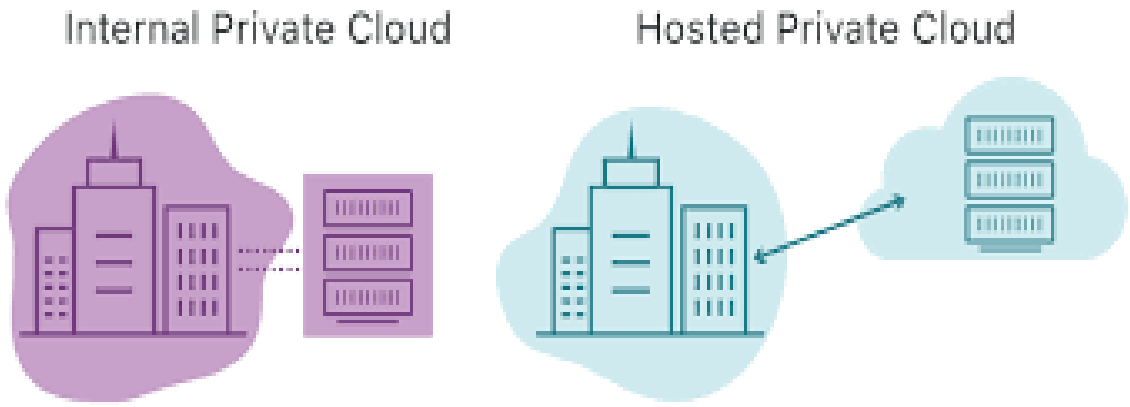
Postoje različiti tipovi privatnih oblaka ovisno o načinu upravljanja, kontekstu, potrebi organizacije i hostingu [23]. Svaki od njih daje različitu razinu usluga. Svi modeli usluga se mogu isporučiti privatnim oblacima. Tipovi privatnih oblaka su:

- Virtualni privatni oblak – različit od klasičnih privatnih oblaka, gdje pružatelji javnih oblaka unutar istih, osiguravaju privatno i izolirano okruženje za određene vrste korisnika (organizacije) [21]. Poslužitelji se dijele između više organizacija, zbog javnog oblaka, ali neki računalni resursi su privatni za određene vrste organizacija [23].



Slika 8. Prikaz virtualnog privatnog oblaka [24].

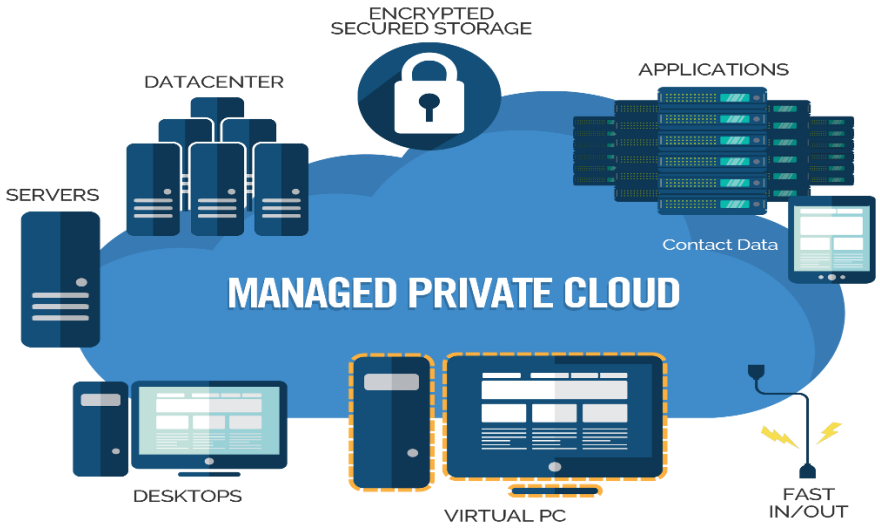
- Udomaćeni (hosted) privatni oblak – poslužitelj zauzima jedna organizacija i ne dijeli se između više organizacija [23]. Pružatelj usluga u oblaku je zadužen za konfiguriranje mreže, održavanje hardvera za privatni oblak i ažuriranje softvera [21]. Ova vrsta privatnih oblaka je idealna za organizacije, koje trebaju sigurnost i dostupnost, bez troškova ulaganja u interni podatkovni centar [21].



Slika 9. Prikaz udomaćenog privatnog oblaka [25].

- Upravljani privatni oblak – u ovom hostiranom okruženju, pružatelj usluge oblaka upravlja svim aspektima privatnog oblaka, kao npr. upravljanje identitetom i pohrana podataka [23]. Prikladan je za organizacije, koje žele uštedu vremena i IT

resursa [21]. Isto tako, koriste ga organizacije, koje nemaju dovoljno kvalificiranog osoblja za upravljanje privatnim oblacima [23].



Slika 10. Prikaz upravljanog privatnog oblaka [26].

Vlastiti privatni oblak može implementirati i sama organizacija. Međutim, u današnje vrijeme, navedeno se sve manje koristi, zbog visokih troškova, potrebe za stručnim ljudima i brige oko održavanja i upravljanja privatnim oblakom. Organizacije često biraju, jedan od opisanih, triju tipova privatnih oblaka. Upravljani privatni oblak nudi najveću razinu usluge. Rješenja za privatne oblake poput ownCloud-a, služe za jednostavnu implementaciju „self-hosted“ privatnog oblaka. Takva rješenja su pogodna za krajnje korisnike i organizacije te nude visoku razinu kontrole i sigurnosti. Ista će biti implementirana kasnije. Prema tome, postoje ranije spomenuta, dva konteksta privatnih oblaka: upravljanje privatnim oblakom (zadužen pružatelj usluga) i vlastito održavanje privatnih oblaka (zadužena sama organizacija). „Self-hosted“ privatni oblak bi pripadao kontekstu, vlastitog održavanja privatnih oblaka. Tipovi privatnih oblaka su većinom oblik upravljanja privatnim oblakom s većom ili manjom kontrolom korisnika (organizacije).

3.2. Korisnost

Privatni oblaci su vrlo učinkovito rješenje za pojedine organizacije. Glavne pogodnosti i koristi koje isti donose su:

- Potpuna kontrola i time bolja sigurnost – organizacija koja je vlasnik privatnog oblaka ima potpunu kontrolu sustava i povećanu sigurnost putem hardvera i fizičke infrastrukture [21].

- Bolje perfomanse – hardver koristi jedna organizacija i zbog toga poslužitelj neće biti opterećen, u odnosu kada ga koristi više organizacija [21].

- Dugoročna ušteda – ukoliko organizacija već posjeduje hardver i mrežu za hosting, tada vlastito implementiranje privatnog oblaka će biti dugoročno isplativije od plaćanja mjesečne pretplate za korištenje usluga hostinga [21].

- Skalabilnost – lagano dodavanje novih hardverskih resursa, ako dolazi do premašivanja postojećih [21].

- Predvidivi troškovi – kod privatnih oblaka su troškovi svaki mjesec jednaki, bez obzira na količinu opterećenja odnosno količinu korištenja, za razliku od javnih oblaka [21].

- Bolja prilagodba – potpuna kontrola nad privatnim oblakom, rezultira prilagodbom pojedinačnim zahtjevima organizacije [21]. „IT menadžeri imaju pristup svakoj razini postavki u svom privatnom okruženju u oblaku“ [21].

Sve su ovo koristi koje se dobivaju privatnim oblacima. Postoje i neki, ranije spomenuti nedostaci koji također utječu, kod odabira ovog tipa oblaka. Najveća prednost privatnih oblaka je sigurnost. Privatni oblaci nude najveću razinu sigurnosti u odnosu na ostale tipove računalnih oblaka. Najveća korisnost privatnih oblaka, sigurnost će biti detaljnije obrađena u nastavku.

4. Sigurnost privatnih oblaka

Primarni dio privatnih oblaka je svakako sigurnost. Sve većim razvojem tehnologija i Interneta, raste broj hakerskih napada pa je potrebna određena garancija i izolacija kritičnih informacija i podataka. Izgradnja sigurnosnog sustava tj. sigurnosnih mehanizama je izuzetno složen proces. Sigurnosni sustav koji nema niti jedne ranjivosti je danas rijedak. U budućnosti se očekuje, još veći napredak u sigurnosnim mehanizmima za privatne oblake. Međutim, isti su danas najsigurnija opcija na tržištu oblaka. Više ulaganja i troškova, za sigurnost osjetljivih podataka i informacija se uvijek isplati. Naime, tzv. „Cyberattack“, može prouzročiti značajne štete za organizacije i korisnike i time bi troškovi i gubitak, prerasli troškove ulaganja u sigurnost.

Sigurnost privatnih oblaka odnosno sigurnosne probleme privatnih oblaka, možemo podijeliti u 3 kategorije: Sigurnost od strane pružatelja usluge, sigurnost infrastrukture i sigurnost od strane krajnjeg korisnika [27]. One vrijede u svim vrstama oblačnih okruženja.

- Sigurnost od strane pružatelja usluge – *upravljanje identitetom i pristupom* (praćenje autorizacije, autentifikacije i revizije (tzv. AAA) korisnika, koji pristupaju uslugama u oblaku i ovdje se koriste mehanizmi poput: IDS, IPS i VPN, zbog sprječavanja neovlaštenog i nepoželjnog pristupa), *privatnost* (ovisi o standardima privatnosti u zemljama korisnika, za osiguranje same se koriste: upravljanje identitetom, sigurnosna pohrana podataka, usklađenost sa standardima i slično), *zaštita podataka u prijenosu* (korištenje protokola SSL/TLS za kriptiranje podataka, što uključuje integritet (MAC) i autentifikaciju), *identitet korisnika* (dopuštanje korištenje cloud usluga, samo autoriziranim korisnicima, što se ostvaruje praćenjem aktivnosti prijava korisnika) i *revizija i usklađenost* [27].

- Sigurnost infrastrukture – *sigurnost pohrane podataka* (najveći problem kod sigurnosti privatnih oblaka, odnosi se na način pristupa podacima i pohrane istih, zahtjeve revizije, usklađenost, zahtjeve obavijesti, troškove gubitka ili krađe podataka. Kriptiranje podataka u mirovanju i prijenosu je moguće rješenje za ovaj problem), *mreža i poslužitelj* (korištenje virtualnih vatroštita za izolaciju i razdvajanje, produkcijskih (timovi za virtualne mašine) od razvojnih timova („hosted“ timovi) i slično) [27].

- Sigurnost od strane krajnjeg korisnika – *SECaaS*, *sigurnost web-preglednika* (korištenje TLS protokola i autentifikacije), *autentifikacija* (tip autentifikacije „username i password“ nije toliko siguran, već bi se trebao koristiti TPM (Trusted Platform Module)), *gubitak upravljanja* (korisnik prepušta aspekte sigurnosti u ruke pružatelja usluge), *„Lock-In“* (slaba portabilnost podataka, aplikacija i usluga, tj. problem kod prijenosa istih iz jednog prema drugome pružatelju usluga), *zaštita podataka* (korisnik ima malo informacija oko obrade, sigurnosti i nadziranja svojih podataka) [27].

Kod svih modela usluga oblaka, sigurnost korisničkih informacija i podataka je najvažnija [27]. Izgradnja sigurnosti kod privatnih oblaka, uvijek kreće od operativne razine (vatroštit, IDS i IPS), zatim implementiranje virtualnih privatnih mreža (VPN) i nakon toga se razrađuje sigurnost podataka i informacija te API-ja. Izgradnja i održavanje, takvih sustava sigurnosti je uvijek izazov i rizik za organizacije.

4.1. Sigurnost podataka i informacija (InfoSec)

Sigurnost podatak i informacija (eng. *InfoSec*) je najvažniji aspekt sigurnosti privatnih oblaka. S druge strane aspekti sigurnosti podataka su: podaci u mirovanju i prijenosu, obrada podataka, podrijetlo podataka (eng. *Data lineage*), izvor podataka (eng. *Data provenance*) i zadržavanje podataka (eng. *Data remanence*) [28].

Za zaštitu podataka u prijenosu se koriste protokoli: FTPS (FTP preko TLS-a), HTTPS (HTTP preko TLS-a) i SCP (Secure Copy Program) [28]. Podaci se enkriptiraju i putuju u takvom obliku, Internetom do odredišta. Protokol TLS je standard za zaštitu podataka u prijenosu. On bi trebao osigurati integritet, autentifikaciju i povjerljivost (tajnost). On se koristi za uspostavu sigurne komunikaciju putem Interneta, tipično između klijenta i poslužitelja. Tajnost se ostvaruje kriptiranjem podataka, pomoću dogovorenog sjedničkog ključa između klijenta i poslužitelja, a najčešće korišteni algoritam kriptiranja je AES. Integritet se ostvaruje pomoću tzv. MAC protokola, u kojem se koristi MAC (Message Authentication Code) ključ, koji se tvori iz zajedničke tajne, kod rukovanja TLS-a. Autentifikacija se ostvaruje pomoću certifikata javnih ključeva (PKI). Za razmjenu zajedničkog sjedničkog ključa, mogu se koristiti algoritmi: RSA i Diffie-Helman. Danas se najviše koristi algoritam Diffie-Helman, zbog buduće sigurnosti (eng. Forward secrecy).

Kod zaštite podataka u mirovanju se javljaju neki problemi. Ako se podaci koriste isključivo za pohranu u oblaku, tada se isti kriptiraju kod pohrane i ostaju pohranjeni u kriptiranom obliku [28]. Takav pristup je poželjno i moguće koristiti, kod modela usluge IaaS i oblaka za pohranu podataka. Međutim, za modele usluga: PaaS i SaaS, takvo što nije moguće [28]. Razlog tome je, da u takvim okruženjima se nalazi aplikacija bazirana na oblaku i pristupanje kriptiranim podacima, u smislu indeksiranja ili pretraživanja od strane iste je prilično teško [28].

Kod obrade podataka, bilo kakvo kriptiranje u mirovanju i prijenosu nije moguće [28]. Zato jer u protivnome aplikacija, ne može raditi svoj posao. Ovdje leži glavni problem sigurnosti privatnih oblaka. Kao reakcija na takvo stanje, znanstvenici i istraživači razvijaju homomorfnu shemu kriptiranja, koja bi omogućila obradu kriptiranih podataka, ali ona je još uvijek računski vrlo zahtjevna [28]. U budućnosti se očekuje značajan napredak u ovom segmentu.

Podrijetlo podataka uključuje praćenje mjesta i vremena kretanja korisničkih podataka [28]. Pružatelj usluga bi trebao korisnicima, osigurati navedeno, za potrebe revizije i usklađenosti, međutim takav proces zahtijeva, mnogo vremena i kod privatnih oblaka [28].

Izvor podataka je povezan s integritetom istih, ali integritet potvrđuje da podaci nisu neovlašteno mijenjani, dok izvor podataka još uključuje datum promjene, detalje uz valjanost i ishodište podataka [29]. Izvor podataka je širi pojam, koji uključuje integritet podataka. Kod privatnih oblaka takvo što je moguće, zbog toga jer se ne koriste dijeljeni resursi. Ponekad, ako se koristi upravljani privatni oblak, tada je sva kontrola u vezi toga, prepuštena pružatelju usluga.

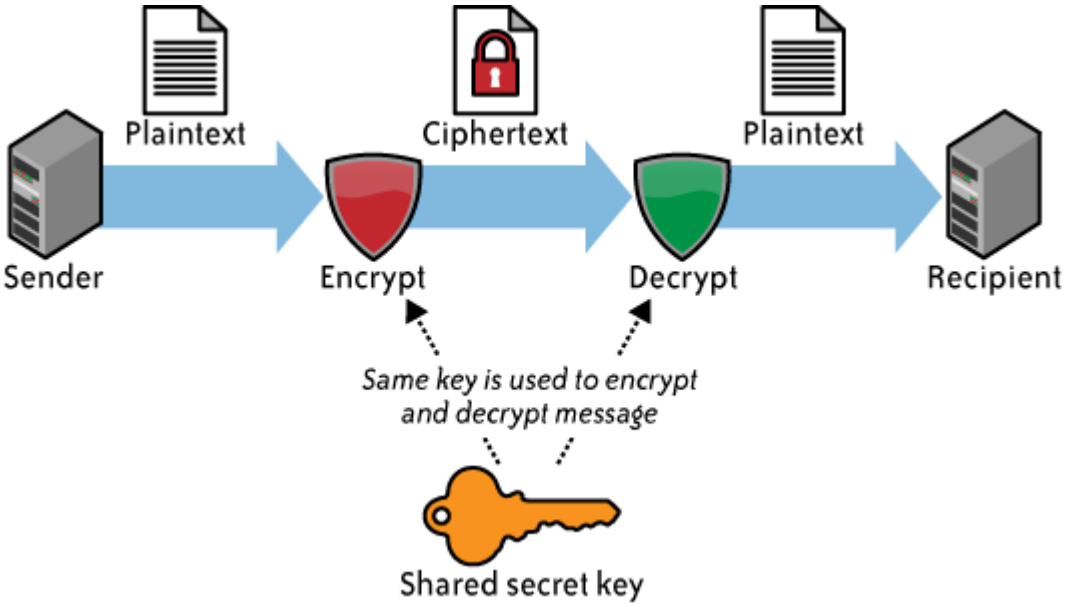
Zadržavanje podataka je aspekt, kojemu većina pružatelja usluga, ne pridodaje pažnju i vrlo često ga ne spominje u ugovoru o razini usluge [28]. Problem je u tome, da prilikom nominalnog brisanja podataka ili zbog fizičkih svojstava medija za pohranu, isti i dalje ostaju sačuvani (zadržani) [28]. To je vrlo rizično i nesigurno, osobito ako su oni premješteni u koš za smeće ili predani trećoj strani [28]. Zadržavanje osjetljivih, poslovnih informacija organizacija u oblaku je veliko narušenje sigurnosti. Za izbjegavanje takvog problema, potrebno je provesti proces čišćenja ili sanitizacije nad medijem za pohranu podataka, kako bi obrisani podaci zauvijek nestali [28].

4.1.2. Sigurnost pohrane podataka

Danas je još uvijek pohrana podataka, najviše korištena usluga oblaka. Pod uslugom pohrane podataka, podrazumijevamo: model usluge IaaS i usluge pohrane podataka u oblaku [28]. Takva pohrana podataka, treba biti na neki način, zaštićena od neovlaštenog korištenja. Ako se pohrana podataka koristi za poslovne svrhe, tada se sigurnost odnosi na, zaštitu povjerljivih podataka od hakerskih napada [30]. U drugom slučaju osobne pohrane podataka, sigurnost je zapravo privatnost i spriječavanje prisluškivanja [30]. U oba slučaja, podatke je potrebno zaštititi kriptiranjem. Glavna tri aspekta sigurnosti pohrane podataka su: povjerljivost (tajnost), integritet i dostupnost [28].

Za osiguranje povjerljivosti potrebno je osigurati dvije stvari: autentifikaciju i autorizaciju te zaštitu podataka kriptiranjem [28]. Autentifikacija oblika: „username i password“ u privatnom oblaku je vrlo rizična varijanta za korištenje [28]. Dvofaktorska autentifikacija (eng. *2-factor authentication*) je sigurnija varijanta autentifikacije, gdje neovlaštena krađa lozinke (uslijed krađe podataka, utjecaja SpyWare-a i slično), nije dovoljna za neovlaštenu prijavu u račun [30]. Autorizacija se odnosi na dozvolu pristupa nakon korisničke prijave. Za navedeno se koristi ranije spomenuta dvofaktorska autentifikacija, virtualne privatne mreže (VPN), IPS i IDS [28]. Autorizacijom se korisniku dozvoljavaju, određena prava pristupa sučelju, ovisno o ulozi.

Što se tiče zaštite pohranjenih podataka, ista se ostvaruje pomoću algoritama simetričnog kriptiranja [28]. Preporučljivo je, da se enkriptiranje, provodi pomoću 256-bitnog ključa [30]. Razbijanje tako velikih ključeva je gotovo neizvedivo. Simetrično kriptiranje je brže i jednostavnije od asimetričnog jer zahtijeva manje računalnih resursa i samo jedan ključ za enkriptiranje i dekriptiranje [28]. Najčešće korišteni standard za simetrični algoritam kriptiranja je AES. Zajednički ključ dijele pružatelj usluga u oblaku i krajnji korisnik. Ovdje se javlja problem upravljanja ključem (eng*. key management*) odnosno čuvanje ključa [28]. Pružatelji usluga vrlo često kriptiraju, podatke svih korisnika, jednim ključem jer je čuvanje više korisničkih ključeva, vrlo zahtjevno i naporno [28]. Ovo predstavlja veliki sigurnosni problem. Čuvanje ključa od strane krajnjeg korisnika je isto tako, zahtjevno i naporno [28]. Rješenje za ovakve probleme je korištenje OASIS Key Management Interoperability Protocol (KMIP) [28]. OASIS KMIP se odnosi na poslužitelja, koji čuva ključeve i pruža usluge enkriptiranja i dekriptiranja.



Slika 11. Simetrični algoritam kriptiranja [28].

Osiguranje povjerljivosti nije dovoljno za osiguranje integriteta. Može postojati garancija nad povjerljivošću podataka, ali ne i da podaci nisu mijenjani [28]. Za ovu svrhu se koristi MAC ključ i najjednostavnije ga je implementirat, nad već kriptiranim podacima, pomoću simetričnog načina kriptiranja: CBC (Cipher Block Chaining) i jednosmjerne hash funkcije [28]. Korisnici moraju biti sigurni, da njihovi podaci nisu neovlašteno mijenjani ili su cjeloviti, zbog česte fluktuacije istih. Češće se koristi drugi način provjere potpunosti podataka (integriteta), matematički dokaz dohvatljivosti (eng. proof of retrievability) [28]. Zato jer se podaci dinamički pohranjuju u oblak pa izvođenje MAC-a svaki puta, nije baš najefikasnije rješenje [28].

Zadnji aspekt sigurnosti pohrane podataka, dostupnost predstavlja mjeru koliko vremena korisnici mogu, pristupiti svojim pohranjem podacima i mogući gubitak istih. Dostupnost mogu narušiti mrežni napadi (npr. DoS napad) i ne pretjerano visoka raspoloživost usluge od strane pružatelja iste [28]. Pružatelj usluge bi trebao osigurati kapacitete, za što veću dostupnost, ali dostupnost od 99.999% (tzv. „five 9s“) je poprilično neizvediva, zbog mnogo korisnika usluge u oblaku. Pružatelj usluge bi isto tako trebao osigurati, oporavak od gubitka podataka, uslijed različitih okolnosti [28]. Sigurnosna kopija podataka u slučaju gubitka istih, bi trebala biti standard za privatne oblake. Neki pružatelji usluga u oblaku, još dodatno naplaćuju takvu uslugu ili obavještavaju korisnike o nadolazećem gubitku podataka [28]. Kod privatnih oblaka, takav scenarij bi trebao biti rijedak.

Dakle, sve ove aspekte je potrebno osigurati, za potpunu sigurnost pohrane podataka. Iz ovog se jasno vidi, velika odgovornost pružatelja usluge i povjerenje korisnika u sigurnosne usluge samoga.

4.2. API sigurnost

API sigurnost je podjednako važna kao i sigurnost podataka i informacija. API je sučelje za interakciju, tj. skup definicija i protokola za komunikaciju između usluga i resursa [31]. On je zapravo sve ono čime korisnik upravlja, tijekom korištenja usluge oblaka. Sigurnosna prijetnja, koja se može javiti nepravilnim osiguranjem API-a je neovlašteno preuzimanje kontrole nad njime i zatim njegovo korištenje, za krađu podataka ili prisluškivanje komunikacije [31]. Postoje različite metode zaštite API-a, korištene od strane različitih pružatelja usluga u oblaku.

Prva metoda je korištena od strane AWS (Amazon Web Services). Koriste se dva različita načina: API pristupnik i upravljanje identitetom i pristupom [31]. „API pristupnik je usluga koja omogućuje stvaranje, održavanje, nadgledanje, osiguranje i objavljivanje API-a, za usluge i aplikacije“ [31]. Pritom se koristi infrastruktura bez poslužitelja [31]. Sigurnosni mehanizmi API pristupnika su: *API ključevi* (žetonski nizovi koji se daju korisnicima ili programerima za ovlašteno povezivanje na API, kreirani od strane API pristupnika) i *Lambda prilagođeni autorizatori* (funkcije za autorizaciju i upravljanje ključevima) [31]. Drugi način, upravljanje identitetom i pristupom, se odnosi na ranije opisanu autentifikaciju i autorizaciju.

Druga metoda je korištena od strane Azure-a. Koriste se tri različita načina: autorizacijski ključevi, OAuth i JSON web tokeni i autentifikacija putem klijentskog certifikata [31]. Pristup API-u je zaštićen pomoću autorizacijskih ključeva, koji se dodjeljuju i ponekad regeneriraju korisnicima [31]. OAuth i JSON web tokeni je isto vrlo često korišteni način. Provodi se pomoću autorizacijskog poslužitelja. Korisnik putem HTTPS-a, upućuje zahtjev prema autorizacijskom poslužitelju za OAuth token ili JSON web token i nakon korisničkog autentificiranja se isti dodjeljuje korisniku [31]. Nakon toga je API vrlo siguran za korištenje. Zadnji način je autentifikacija putem klijentskog certifikata, koja se ostvaruje pomoću sigurnosnog protokola, TLS-a.

Treća metoda je korištena od strane Google Cloud-a. Koristi se posebna usluga za upravljanje i razvijanje API-a, Apigee Edge [31]. Apigee Edge nudi ranije opisane API ključeve za pristup API-u i autentifikaciju korisnika, provjeru autentičnosti i autorizacije aplikacija putem SAML tokena i ranije opisani OAuth 2.0 [31].

Iz ovog se jasno zaključuje, da su OAuth i API ključevi, najčešće korištene metode za API sigurnost.

4.3. Sigurnosni izazovi

Sigurnost privatnih oblaka pruža garanciju korisniku, ali zahtijeva mnogo napora i odgovornosti. Ukoliko organizacija u potpunosti upravlja privatnim oblakom, tada je potrebno stalno održavanje istoga. Prednost tome je veća kontrola i veća sigurnost podataka [32]. Naime, time su na neki način osigurani, svi ranije opisani aspekti sigurnosti podataka i informacija. Ako organizacija koristi, pružanje upravljanih usluga privatnih oblaka (upravljanje privatnim oblacima), tada bi pružatelj usluge trebao osigurati, izolaciju poslovnih podataka organizacije od podataka drugih organizacija, koje su korisnici iste usluge [32]. Problem koji se isto tako javlja, kod pružanja upravljanih usluga privatnih oblaka je lokacija podataka i sigurnosni aspekti istih [32]. Upravljanje identitetom je fundamentalno za sigurnost privatnih oblaka [32]. Odnosi se na ranije opisanu autentifikaciju i autorizaciju, koje obuhvaćaju kojim ulogama korisnika je dopuštena koja razina pristupa. Problemi koji se također javljaju, kod svih vrsta privatnih oblaka su: upitno povjerenje u osoblje i nepovjerenje u korisničke podatke (aplikacije) [32].

Sve su ovo izazovi s kojima se treba suočiti, prilikom implementiranja ili korištenja privatnih oblaka. Izrazito veliki napori oko održavanja, u slučaju vlastite implementacije i povjerenje u treću stranu, u slučaju korištenja upravljanih privatnih oblaka su dva najveća izazova. Međutim, oni i dalje nude veću garanciju sigurnosti od ostalih tipova oblaka.

5. Penetracijsko testiranje oblaka

„Penetracijsko testiranje je praksa testiranja računalnog sustava, mreže ili „hosted“ aplikacije, zbog otkrivanja ranjivosti, koje bi hakeri mogli iskoristiti prilikom napada“ [42]. Takva testiranja bi trebala biti pomno planirana i odobrena. Ona pomažu u pronalasku svih mogućih sigurnosnih problema sustava i time daju uvid pružateljima usluga u oblaku, što u istome treba ispraviti i poboljšati u kontekstu sigurnosti. Predmet penetracijskog testiranja oblaka mogu biti: eksterna i interna infrastruktura, „hosted“ aplikacija i sama konfiguracija oblaka [43]. Najlakše je sigurnosno probiti zaštitu eksterne infrastrukture, a primjeri ranjivosti su: izložene baze podataka ili softver s poznatim ranjivostima te ostala internetski orijentirana infrastruktura [43]. Toj kategoriji pripadaju web-bazirane aplikacije [43]. One su danas, najčešći predmet pentracijskog testiranja oblaka. Razlog je u tome, da svi oblaci nude korisnicima, neki segment API-a, koji je lako dostupan i često ranjiv. Hakerski pristup internoj infrastrukturi, na kojoj je izgrađen oblak je moguć, nakon probijanja sigurnosti eksterne infrastrukture [43]. Stoga je najveća važnost, zaštita „prve linije obrane“ odnosno eksterne infrastrukture (web-baziranih aplikacija). Kod pentracijskog testiranja javnih oblaka, javljaju se neke pravne i tehničke prepreke, koje moraju biti riješene [42]. Kod privatnih oblaka, takvo što je rjeđe jer usluge oblaka, ne dijeli i ne koristi veliki broj ljudi, a ponekad ga samo koriste zaposlenici pružatelja usluga (organizacije).

5.1. Penetracijsko testiranje aplikacija baziranih na oblaku

Ova vrsta testiranja je često korištena, zbog korisničke učestalosti korištenja aplikacija odnosno API-a. Za potrebe penetracijskog testiranja oblaka, treba pronaći odgovarajući tim stručnjaka. Poželjno je da oni budu iz drugih organizacija, radi veće objektivnosti testiranja. Nakon toga je potrebno definirati i usuglasiti plan testiranja. To uključuje stvari koje će biti testirane, kao što su: aplikacija (identificiranje API-a), podatkovni pristup (da li će penetracijsko testiranje podataka, ići preko aplikacije ili direktno preko baze podataka), mrežni pristup (koliko dobro mreža štiti aplikaciju i podatke), virtualizacija (virtualne mašine), usklađenost (propisi unutar aplikacije ili baze podataka), automatizacija (odabir alata za penetracijsko testiranje) i pristup (hoće li administratori aplikacija, biti uključeni u testiranje) [42]. Takav plan se mora slijediti i biti prihvaćen od strane, svih članova tima za penetracijsko testiranje oblaka [42]. Penetracijsko testiranje oblaka se može provesti i bez alata, pomoću ljudske stručnosti i kompetencija, ali se takav pristup

danas rjeđe koristi. Danas se vrlo često koriste, alati koji nisu bazirani na oblaku. Međutim, alati bazirani na oblaku se počinju sve više koristiti, zbog smanjenja troškova [42]. Obje vrste spomenutih alata, mogu simulirati stvarne hakerske napade poput: neprekidnog pogađanja lozinke ili traženje API-a koji mogu pružati direktni pristup podacima [42]. Nakon primjene alata za penetracijsko testiranje oblaka, potrebno je osim ranjivosti, dokumentirati i ljudske te automatizirane odgovore, koji su zapravo reakcija na takvo testiranje [42]. Ljudski odgovori su reakcije korisnika i administratora aplikacije na penetracijsko testiranje [42]. S druge strane, automatizirani odgovori su reakcija samog sigurnosnog sustava na takvo testiranje, a primjeri radnji (reakcija) su: blokiranje IP adrese koju generira alat za testiranje i potpuno isključivanje aplikacije [42].

Glavni cilj penetracijskog testiranja oblaka je pronalazak ranjivosti sustava. Najčešće pronađene ranjivosti su: omogućen pristup aplikacijskim podacima preko API-a, dozvoljen pristup API-u nakon 10 pokušaja, virtualna mašina ne pruža traženu razinu izolacije, aplikacijska lozinka se pogađa pomoću automatskog generatora za lozinke, VPN omogućuje pristup izvana, ukoliko je DNS isključen, kriptiranje nije u skladu s novim propisima i drugi problemi [42]. Ispravljanjem ranjivosti aplikacija, smanjuje se mogućnost probijanja interne infrastrukture i to je još jedan razlog, sve češćeg korištenja, penetracijskog testiranja aplikacija baziranih na oblaku.

6. Rješenja za privatne oblake i njihova sigurnost

Postoje mnoga rješenja za privatne oblake. Ona se implementiraju pomoću posebnih klijentsko-poslužiteljskih softvera. Glavna prednost istih je da su open-source i omogućuju kreiranje „self-hosted“ privatnih oblaka, tj. privatnih oblaka kojima upravlja sam korisnik. Omogućen je korisnicima vlastiti, interni hosting, što povećava sigurnost i kontrolu. Takva rješenja sadrže također, visoku razinu sigurnosti odnosno nude mnogo sigurnosnih komponenata. Neki softveri nude, osim usluge pohrane u oblaku i usluge raznih aplikacija. To znači da se na vlastiti poslužitelj, može dodati i funkcionalnost aplikacija. Takvi softveri su pogodni za krajnje korisnike i organizacije. Organizacija može implementirat, kontekst vlastitog održavanja privatnih oblaka i omogućiti krajnjim korisnicima usluge, korištenja sigurnog privatnog oblaka, uz interni hosting iste. Ovo je velika pogodnost za organizacije, međutim zahtijeva održavanje i odgovornost. Sigurnosne komponente su implementirane pomoću softvera, pa organizacije ne moraju o tome brinuti. Svakako, ovakvi softveri su bolje i puno jednostavnije rješenje od vlastite izgradnje privatnih oblaka. Oni su za privatne oblake, trenutno najbolje dostupno rješenje. Najpoznatiji softveri su: Nextcloud, ownCloud, Seafile, FileRun i Pydio. Oni će u nastavku biti opisani i sigurnosno uspoređeni, komparativnom tabličnom analizom. Svi navedeni softveri daju pristup svojim instancama, koje organizacije (korisnik) isporučuju svojim krajnjim korisnicima, uz vlastito održavani poslužitelj (interni hosting). Time dolazi do značajne uštede novca i vremena za organizacije. Kasnije će biti implementirana, testirana i sigurnosno razrađena, dva najpopularnija softvera (tehnologije): Nextcloud i Pydio (Pydio Cells).

6.1. Nextcloud

„Nextcloud je open-source paket klijentsko-poslužiteljskog softvera za stvaranje i korištenje usluga hostinga datoteka“ [33]. Sličnog je oblika kao Dropbox, ali je za razliku od njega, besplatan i open-source, što omogućuje korištenje istoga svima i upravljanje njime na vlastitom poslužitelju [34]. Nextcloud se razvio iz ownClouda, tj. njegov je „fork“ [34]. Danas je Nextcloud bitno drugačiji, a po nekima i popularniji od ownClouda. Glavni moto Nextclouda, ali i svih sličnih softvera je: „trebali biste kontrolirati svoje podatke“ [35]. Prema popularnosti je Nextcloud danas, jedan od vodećih softvera svoje vrste. Najveća prednost Nextclouda u odnosu na konkurenciju je sigurnost [35]. Naime i druge tehnologije sadrže sasvim zadovoljavajuću razinu sigurnosti, ali Nextcloud je podiže na nivo više prema ISO/IEC 27001. Nextcloud-u se može pristupiti preko PC-a i mobilnih uređaja [35]. Sadrži

snažne mogućnosti kriptiranja i ugrađenu kontrolu pristupa datotekama [35]. Omogućuje i dijeljenje datoteka između korisnika, uz javni link, koji je zaštićen zaporkom te zaključavanje datoteka [35]. Nextcloud softver se može proširiti pomoću plugina, drugim vrstama funkcionalnosti aplikacija, kao što su: kontakti, razgovor, vijesti, uređivač teksta temeljen na web-pregledniku, galerija, dvorazinska autentifikacija i slično. Sve se to isporučuje krajnjim korisnicima u privatnom oblaku.

Slika 12. Logo Nextcloud-a [36].

6.2. ownCloud

„ownCloud je open-source softver za sinkronizaciju i dijeljenje datoteka, kolaboraciju sadržaja, koji omogućuje timovima lagan rad nad podacima s bilo kojeg mjesta i na bilo kojem uređaju“ [37]. Postoji u četiri izdanja: izdanje zajednice, standardno, izdanje za poduzeća i SaaS. Za razliku od Dropboxa, nudi pohranu podataka, kojom se upravlja preko vlastitog poslužitelja. ownCloud omogućuje sigurnu kolaboraciju preko funkcionalnosti: integracija Office-a, dijeljenje datoteka i mapa s drugim korisnicima ownClouda-a, praćenje aktivnosti korisnika nad datotekama i mapama i komentari [37]. Uslugama ownCloud-a moguće je pristupiti preko PC-a (macOS, Windows i Linux) i mobilnih uređaja (Android i iOS) [37]. ownCloud sadrži mnoštvo sigurnosnih funkcija, kao što su: FaceID, vatroštit za datoteke, zaključavanje datoteka, multifaktorska autentifikacija, Ransomware zaštita, dijeljenje javnog linka koji je zaštićen zaporkom, OAuth 2.0, „enkripcija od kraja do kraja“, jednokratna prijava preko SAML-a i sveobuhvatna enkripcija [37]. Neke spomenute

sigurnosne funkcije su dostupne, samo preko izdanja za poduzeća, ali standardno izdanje ownCloud-a, sadrži i dalje sasvim dovoljnu razinu sigurnosti. Opis ownCloud-a glasi: „spremi, dijeli i radi“, što upućuje na široki spektar mogućnosti istoga [37]. Na ownCloud-u je moguće također, upravljanje kontaktima, kalendarom i online izmjena dokumenata [37].

Slika 13. Logo ownCloud-a [37].

6.3. Seafile

„Seafile je open-source rješenje za sinkronizaciju i dijeljenje datoteka, dizajniran za visoku dostupnost, perfomanse i produktivnost“ [38]. Moguće je izgraditi timsku bazu znanja, pomoću ugrađene Wiki značajke [38]. Koristi se za izgradnju „self-hosted“ privatnih oblaka, što smanjuje vrijeme i novac za organizacije (korisnike). Dostupan je na svim platformama, kao i Nextcloud te ownCloud. On sadrži izrazito brzu i pouzdanu sinkronizaciju datoteka, koja može sinkronizirati 10 tisuća malih datoteka, u roku od 1 minute [38]. Moguće je i pristupati datotekama u oblaku na lokalnom disku, bez potrebe za sinkronizacijom [38]. Što se tiče sigurnosnih komponenata, Seafile ima ugrađeno enkriptiranje datoteka, dvorazinsku autentifikaciju, kontrolu pristupa po mapi, dijeljenje javnih linkova zaštićenih zaporkom, skeniranje virusa, zaključavanje datoteka, čuvanje prijašnjih verzija datoteka i mapa, upravljanje ulogama korisnika, jednokratna prijava i sigurnosna kopija i oporavak podataka [38]. Isto tako, još neke korisne funkcionalnosti, koje Seafile nudi su: online izmjena office dokumenata i praćenje sustava preko logova (zapisnika) [38]. U usporedbi s Nextcloud-om i ownCloud-om, Seafile nema toliko funkcionalnosti aplikacija, ali je i dalje jedno od najboljih rješenja za privatne oblake.

Slika 14. Logo Seafile-a [39].

6.4. FileRun

„FileRun je alternativa Google disku/fotografijama/glazbi, koja pripada „self-hosted“ vrsti privatnih oblaka [44]. On je zapravo web-upravitelj datoteka s izvrsnim korisničkim sučeljem i mi ga „hostamo“ na svom vlastitom poslužitelju [44]. Zahtjev za datotekama je jedna vrlo korisna opcija FileRun-a. Korisnik FileRun-a pošalje drugom korisniku, koji možda ne koristi isti, link s zahtjevom za datotekom i nakon toga taj drugi korisnik, jednostavno ubaci traženu datoteku, koja se automatski sprema na FileRun server prvog korisnika [45]. Ovo je brza i efikasna razmjena datoteka s ostalim korisnicima te ne zahtijeva, da oni imaju konfigurirani FileRun. Opcija „Guest korisnici“ omogućuje brzo dijeljenje datoteka. Ona koristi privatno dijeljenje linka i kreiranje privremenih „guest“ korisnika [45]. Za dijeljenu datoteku se kreira privremeni „guest“ korisnik i šalje se privatni link, na korisnikov E-mail [45]. Korisnik klikom na link je preusmjeren na FileRun i može dijeljenu datoteku vidjeti, skinuti itd., a nakon toga kreirani, privremeni račun korisnika je automatski obrisan ili se može nadograditi u regularni račun [45]. FileRun ima već automatski ugrađeni, WebDAV poslužitelj pa konfiguracija poslužitelja nije potrebna, ali nema podršku za eksternu pohranu podataka [45]. FileRun također dolazi s već automatski ugrađenim pluginovima: Google-ov uređivač i preglednik dokumenata, Office-ov web prikaz, CloudConvert, Autodesk, ONLYOFFICE itd. [45]. Sigurnosne komponente FileRun-a su: API osiguran s OAuth2, automatski sustav za obnavljanje datoteka koji sprječava prepisivanje postojećih datoteka, ugrađena mapa za smeće prije trajnog brisanja datoteka,

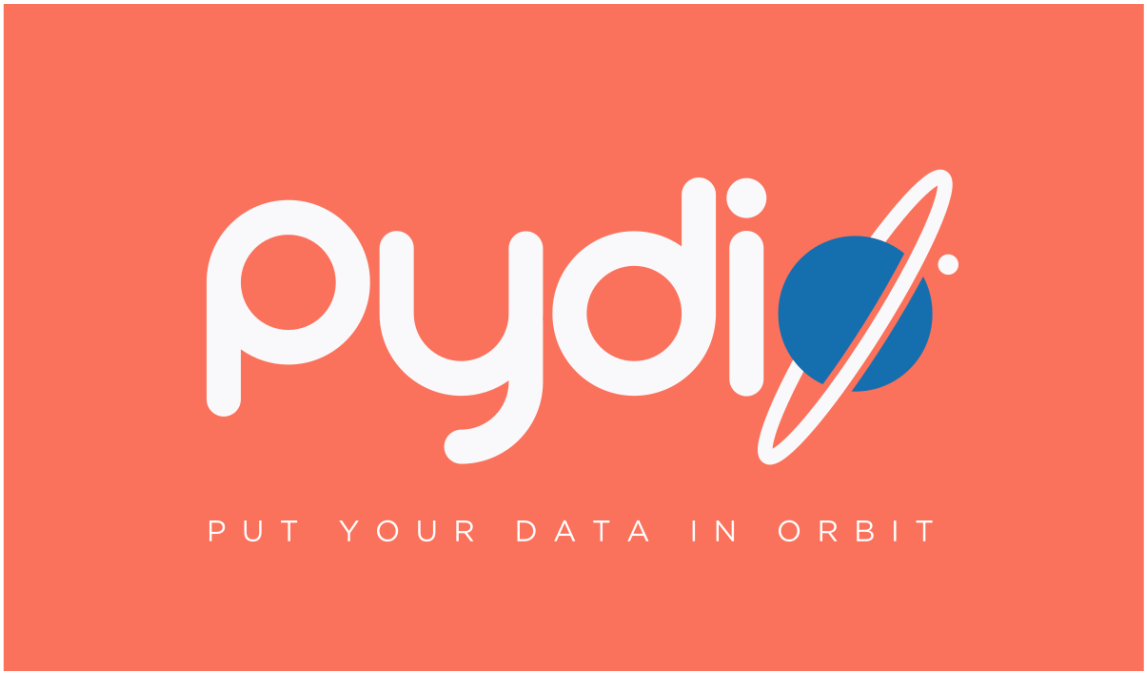
podrška za HTTPS/TLS, zaštita prijave korisnika od „Brute-Force“ napada, zaštita od krađe sesije, pohrana datoteka izvan javnog područja web-poslužitelja i zaštita od „SQL-injection“ i „Cross-side scripting“ [45]. FileRun nema ugrađenu trgovinu aplikacija za proširenja, kao što imaju Nextcloud i ownCloud, već je on primarno baziran na razmjeni datoteka.

Slika 15. Logo FileRun-a [46].

6.5. Pydio (Pydio Cells)

„Pydio je platforma za razmjenu datoteka, koja zaštićuje privatnost korisnika i povezuje sve timove na jednom mjestu“ [47]. Pripada „self-hosted“ vrsti privatnih oblaka jer mi upravljamo njime, na vlastitom poslužitelju. Glavna značajka Pydio-a su ćelije. Ćelije osiguravaju kontrolu, sigurnost i privatnost svim korisnicima istih [47]. Svi korisnici ćelija mogu timski poslovati, razmjenjivati datoteke, komunicirati preko ugrađenog chata i slično [47]. Pydio se može koristiti u osobne i poslovne svrhe, ali je više poslovno orijentirana varijanta privatnog oblaka. On sadrži iznimno moćnu, nadzornu ploču za administratore. Sigurnosne značajke koje se definiraju i prate preko nje su: praćenje svih aktivnosti korisnika i kontrola neželjenih radnji, zaštita pohranjenih podataka pomoću vlastito definiranog ključa, sigurnosna komunikacija preko SSL-a, API sigurnost pomoću: Open ID Connect-a, OAuth2-a ili SAML-a, podrška za GDPR (alat za usklađivanje s najnovijim propisima o privatnosti korisnika), podrška za eksternu pohranu podataka, razna prava

pristupa po korisniku ili grupi i upravljanje složenošću lozinke [47]. Pydio ne sadrži aplikacijska proširenja, kao Nextcloud i ownCloud.



Slika 16. Logo Pydio-a [48].

6.6. Sigurnosna usporedba rješenja za privatne oblake

Rješenja za privatne oblake: Nextcloud, ownCloud, Seafile, FileRun i Pydio, sadrže mnogo sigurnosnih aspekata. Međutim, neka rješenja sadrže malo veći oblik istih, ali zajedničko je svima, da omogućuju izolaciju i kontrolu informacija preko internog hostinga. Interni hosting je već prva linija sigurnosti, a ista se još može povećati, pomoću VPN-a. Većina sigurnosnih aspekata je ugrađena u sama rješenja, što je ekonomičnije i nudi olakšanje za korisnike istih. Dakle, rješenja se implementiraju unutar vlastitog poslužitelja. U nastavku će biti prikazana komparativna tablična analiza, rješenja za privatne oblake sa aspektom sigurnosti.

Tablica 1. Komparativna tablična analiza rješenja za privatne oblake u kontekstu glavnih sigurnosnih aspekata [autorski rad].

Tehnologija	Zaštita podataka u mirovanju	Zaštita podataka u prijenosu	API sigurnost
Nextcloud	Šifriranje na poslužitelju (AES-256/CTR)	HTTPS/SSL	OAuth2, SSO/SAML
ownCloud	Šifriranje na poslužitelju (AES-256/CTR)	HTTPS/SSL	OAuth2, SSO/SAML
Seafile	Šifriranje na poslužitelju, šifriranje na klijentu (AES-256/CBC)	HTTPS/SSL	OAuth2
FileRun	Nema	HTTPS/SSL	OAuth2
Pydio	Šifriranje na poslužitelju (klijent upravlja ključem; AES-256/GCM)	HTTPS/SSL	OAuth2, Open ID Connect, SAML

Tablica 2. Komparativna tablična analiza rješenja za privatne oblake u kontekstu ostalih sigurnosnih aspekata (1) [autorski rad].

Tehnologija	Upravljanje identitetom i pristupom	Zaštita od virusa/zlonamjernih programa
Nextcloud	Dvofaktorska autentifikacija, LDAP, opcija "Guests", otkrivanje sumnjivih prijava, Brute-Force zaštita	Skeniranje virusa (Clam AntiVirus), zaštita od Ransomwarea (vlastiti algoritam)
ownCloud	Dvofaktorska autentifikacija, LDAP, opcija "Guests", Brute-Force zaštita	Skeniranje virusa (Clam AntiVirus), zaštita od Ransomwarea (vlastiti algoritam)
Seafile	Dvofaktorska autentifikacija, LDAP, upravljanje ulogama korisnika, jednokratna prijava	Skeniranje virusa (Kaspersky Anti-Virus/Clam AntiVirus)
FileRun	"Third-party" autentifikacija, upravljanje korisnicima i ulogama, "Guest korisnici", Brute-Force zaštita, zaštita od krađe sesije	Nema
Pydio	Upravljanje postavkama prijave, LDAP, upravljanje korisnicima i ulogama	Nema

Tablica 3. Komparativna tablična analiza rješenja za privatne oblake u kontekstu ostalih sigurnosnih aspekata (2) [autorski rad].

Tehnologija	Sigurnosni povrati lozinke	Broj ranjivosti prema CVE	Podrška za eksternu pohranu podataka
Nextcloud	da (e-mail)	122	Da
ownCloud	da (e-mail)	152	Da
Seafile	da (e-mail/admin resetiranje)	5	Ne
FileRun	da (e-mail)	9	Ne
Pydio	da (e-mail)	33	Da

Rješenja koja sadrže zaštitu podataka u mirovanju, koriste algoritam simetričnog kriptiranja, AES-256 uz različiti način kriptiranja (CTR, CBC, GCM). Za zaštitu podataka u prijenosu sva rješenja koriste HTTPS/SSL, što je danas i standard za istu. Za sigurnost API-a prevladava OAuth 2 standard. Kod upravljanja identitetom i pristupom, opcija „Guests“ ili varijante te opcije (upravljanje korisnicima i ulogama, upravljanje ulogama korisnika) su zastupljene u svim rješenjima, što naglašava njihovu važnost i trend kod „self-hosted“ privatnih oblaka. Postoje ovdje i mnogi drugi važni mehanizmi za upravljanje identitetom i pristupom, koji su zastupljeni kod nekih rješenja, a oni su: dvofaktorska autentifikacija, LDAP i Brute-Force zaštita. Kod zaštite od antivirusa, unutar rješenja koja je sadrže prevladava open-source softver, Clam AntiVirus, koji može prepoznati razne vrste računalnih virusa. Nextcloud i ownCloud imaju također zaštitu od Ransomwarea i pritom koriste vlastito implementiran algoritam prepoznavanja sumnjivih datotečnih imena i ekstenzija za istu.

Sigurnosni povrati lozinke, kod svih rješenja, idu standardno, putem korisničkih e-mail računa. Poznata ranjivost koja se pojavljivala u vezi istih je bila u ownCloud rješenju i zabilježena u CVE. Ona je javljala različite pogreške ovisno o ispravno unesenom korisničkom imenu, što je omogućilo napadačima, da saznaju Brute-Force napadom, listu korisničkih imena [49]. Naime, vrlo je važna poruka, koja se generira nakon izvršavanja sigurnosnog povrata lozinke. Poruka može sadržavati informaciju, da je korisničko ime ispravno ili nije ispravno i time napadaču omogućuje, enumeraciju korisničkih imena tj. otkrivanje korisnika aplikacije. Ovime se napadaču skraćuje posao oko Brute-Force napada, budući da zna već validnu listu korisničkih imena i posebice je opasno, ukoliko aplikacija nema zaštitu protiv Brute-Force napada. Dakle, glavni sigurnosni napad kod sigurnosnog povrata lozinke je tzv. „Napad nabrajanjem korisnika“, koji olakšava napadaču Brute-Force napad.

Broj ranjivosti prema CVE (Common Vulnerabilities and Exposures) je najveći za rješenja: Nextcloud i ownCloud. Iako ova rješenja sadrže najviše sigurnosnih značajki, ona su i dalje vrlo sigurnosno ranjiva. Kod ownCloud-a intenzitet broja ranjivosti je prilično varijabilan. Naime, on je puno manji u odnosu na 2014 godinu, kada je bilo zabilježeno 56 ranjivosti, ali je porastao u odnosu na protekle 3 godine [50]. Kod Nextcloud-a intenzitet broja ranjivosti je također varijabilan. Broj ranjivosti za 2021. godinu je najmanji do sada, ali 2020. godina je imala zabilježen najveći broj ranjivosti i iznenađujuće veći od proteklih godina [51]. Seafile ima samo 5 zabilježenih ranjivosti u CVE. Intenzitet broja ranjivosti je 1 ranjivost po godini [52]. FileRun ima 9 zabilježenih ranjivosti i zanimljivo, zadnje zabilježene su iz 2019. godine [52]. Pydio sadrži 33 zabilježenih ranjivosti i pokazuje veći intenzitet tj. veći broj ranjivosti u 2019. i 2020. godini u odnosu na prijašnje godine, dok za 2021. godinu nema još zapisa u CVE [53]. Zaključno, sva rješenja imaju ranjivosti, kod nekih je broj istih manji, što zbog manjeg broja korisnika (trenutne popularnosti) ili kvalitetnije integrirane sigurnosti.

Podrške eksterne pohrane podataka povećava dozu sigurnosti i kontrole jer se ona nalazi na vlastitom poslužitelju, a ne u aplikacijskoj memoriji. Istu sadržavaju rješenja: Nextcloud, ownCloud i Pydio.

Opisana rješenja pružaju zadovoljavajuću razinu sigurnosti, ali i dalje je slaba sigurnost eksterne infrastrukture tj. Web aplikacije, što se zaključuje iz velikog broja zapisa u CVE o napadima: SQL Injection, XSS, krađa informacija i izvršenje koda [52]. Postoje još neka također popularna rješenja: Tonido, Syncthing i Cozy koja nisu sigurnosno

uspoređena, pošto pružaju vrlo malo informacija oko sigurnosnih značajki i zapisa u CVE pa se iz toga zaključuje, da sadrže manje sigurnosnih komponenata od opisanih rješenja. Ona zbog toga nisu ogledan primjer za sigurnosnu usporedbu.

6.7. Penetracijsko testiranje rješenja za privatne oblake

Penetracijsko testiranje je ispitivanje sustava (privatnih oblaka) koristeći simuliranje sigurnosnih napada s ciljem pronalaska njegovih sigurnosnih ranjivosti. Rješenja za privatne oblake sadrže mnogo ranjivosti u kontekstu eksterne infrastrukture (Web aplikacije). Pomoću ovog testiranja, broj ranjivosti se može drastično smanjiti. U praksi, proces penetracijskog testiranja, najčešće sadrži sljedeći niz koraka:

- Priprema (revizija sustava, određivanje koje sigurnosne ranjivosti će biti procijenjene)
- Izrada plana napada (izrada tj. dizajniranje „Cyber“ napada koji će biti izvršeni)
- Odabir tima (angažiranje stručnjaka ili specijalista za „Cyber“ sigurnost je preporučeno, iako mogu biti i certificirani zaposlenici organizacije za tu domenu, ukoliko ih ona sadrži)
- Određivanje vrste podataka za krađu (korisnički podaci za autentifikaciju, poslovni podaci organizacije, pohranjeni podaci korisnika itd.)
- Izvršenje testa (ključni korak u kojem se mogu koristiti, razni automatski programski alati, npr. Kali Linux, Burp, Nmap, Metasploit i Wireshark)
- Integriranje rezultata izvještaja (potrebno za analizu i uvid u ranjive sigurnosne točke, koje treba zaštititi)

[56].

Najvažniji od navedenih koraka je svakako, izvršenje testa u kojem je potrebno odabrati, kvalitetne automatske programske alate [56]. Kali Linux, Metasploit i Burp su jedni od pouzdanih alata, koji se mogu koristiti za penetracijsko testiranje [57]. Na kraju testiranja, dostupni su rezultati u obliku izvještaja, koji pomažu ispravljanju sigurnosnih ranjivosti.

6.8. Smjernice za zaštitu rješenja za privatne oblake

Kvalitetno sigurnosno zaštićena eksterna infrastruktura privatnih oblaka je ključna, zbog toga što sprječava prodor u njegovu internu infrastrukturu (poslužitelj;podatkovni centar). Prodor u internu infrastrukturu, uzrokovao bi značajne štete organizaciji. Stoga potrebno je zaštiti Web aplikaciju tj. eksternu infrastrukturu, koristeći sljedeće smjernice:

- Korištenje dvofaktorske autentifikacije
- Korištenje snažnih lozinki [55]
- Korištenje zaštite od Brute-Force napada
- Izbjegavanje korištenja sigurnosnih poruka u kojima napadač, lako može doći do informacija o tome je li korisničko ime ili lozinka ispravno, prilikom pokušaja prijave ili sigurnosnog povrata lozinke (sprječavanje „napada nabrajanjem korisnika“) [54]
- Korištenje LDAP ili sličnih autentifikacijskih servisa
- Korištenje OAuth 2.0
- Korištenje HTTPS/SSL protokola za stranicu prijave [55]
- Korištenje antivirusne zaštite [55]
- Često sigurnosno kopiranje svih podataka [55]
- Penetracijsko testiranje
- Korištenje OWASP preporuka

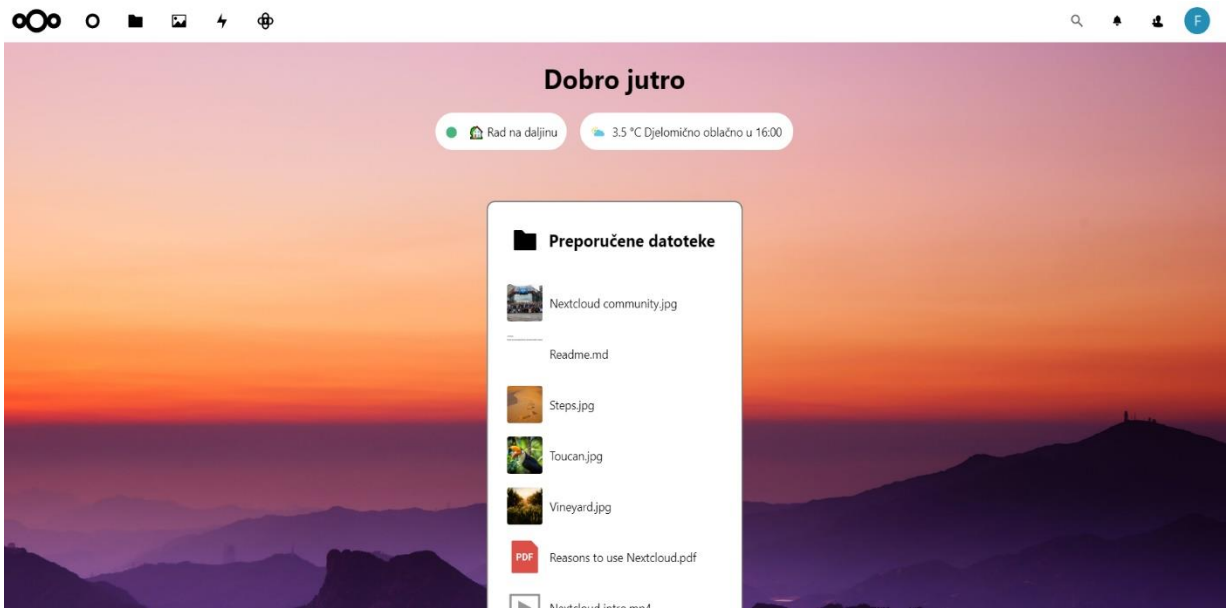
Za potpuniju zaštitu cjelokupne infrastrukture privatnih oblaka, poželjno je napraviti zaštitu interne infrastrukture implementacijom IDS (Intrusion detection system), IPS (Intrusion prevention system), vatroštita i VPN-a (Virtual Private Network). Važno je za napomenuti, da većina sigurnosnih smjernica, dolazi implementirana sa samim rješenjima za privatne oblake, iz čega se vidi njihova korisnost. Međutim, neka rješenja i dalje imaju mnogo sigurnosnih ranjivosti pa je poželjna česta provedba penetracijskih testiranja, za postizanje što kvalitetnije i potpunije sigurnosne zaštite.

7. Implementacija i testiranje sigurnosti rješenja za privatne oblake

Sada će ranije opisana rješenja za privatne oblake, biti implementirana i razrađene te testirane će biti njihove sigurnosne komponente. Ona su primjer jednostavnog kreiranja privatnih oblaka uz vlastiti, interni hosting. Za hosting će biti korišten, Ubuntu Server i Windows 10 u VirtualBox-u. Na vlastitom Ubuntu Serveru i Windows 10 serveru će se upravljati tim programima i njihovom pohranom. Iz toga se jasno vidi visoka doza kontrole i sigurnosti, što su karakteristike privatnih oblaka. Ova rješenja su vrlo efikasna za korisnike i organizacije. Sve što je potrebno osigurati za ista su: mrežna infrastruktura i poslužitelj, a održavanje programa i sigurnosti je integrirano s istima.

7.1. Implementacija i testiranje sigurnosti Nextcloud-a

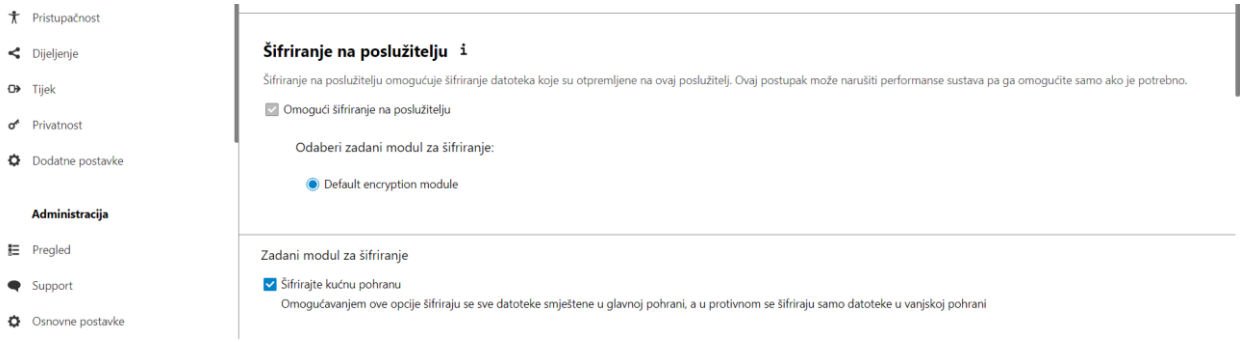
Nakon instaliranja Ubuntu Servera u VirtualBoxu, slijedi instalacija Nextcloud-a. Instalacija Nextcloud-a se provodi jednostavnim upisom naredbe: sudo snap install nextcloud, unutar terminala servera [40]. Snap služi za kreiranje okruženja, unutar Ubuntu Servera, potrebnog za Nextcloud. Nakon instalacije, mi imamo potpunu kontrolu nad Nextcloudom, zahvaljujući snap-u. Zatim se kreira administrativni račun za upravljanje programom [40]. Zadnji korak se odnosi na sigurnost. Dodaje se SSL pomoću „self-signed certificate“, kako bi Nextcloud server, imao osiguranu sigurnosnu komunikaciju preko HTTPS-a te se otvaraju web portovi, kako bi bio dostupan za korištenje preko Interneta [40]. Budući da se Nextcloud nalazi na localhost serveru, pristupiti mu je moguće, preko URL-a: https://localhost ili se može postaviti neka druga „trusted“ domena, ali je potrebno na usmjerniku, konfigurirati tzv. port forwarding. Sada slijedi konfiguriranje i testiranje sigurnosnih komponenata Nextcloud-a.



Slika 17. Sučelje Nextcloud-a [autorski rad].

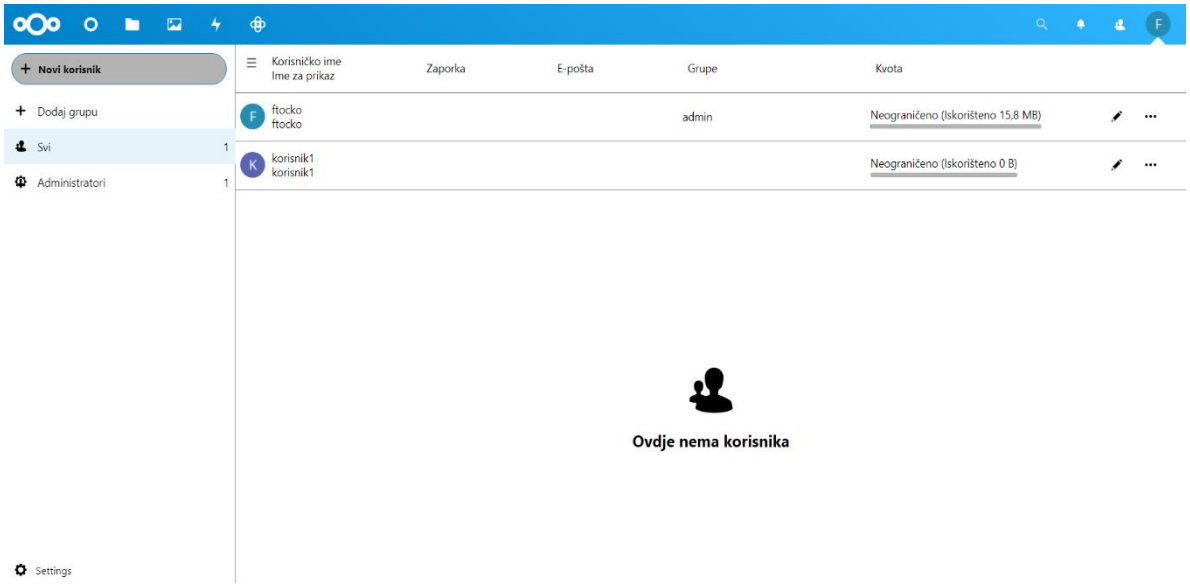
Prilikom konfiguracije Nextcloud-a, implementirana je sigurnost transportnog sloja i koristi se protokol SSL (TLS). Zaštita podataka u prijenosu je time osigurana HTTPS protokolom. Radi se o „enkriptiranju od kraja do kraja“.

Zaštita podataka u mirovanju je moguća, pomoću opcije šifriranja na strani poslužitelja. Prvo je potrebno omogućiti, u već integriranim aplikacijskim modulima Nextcloud-a, Default Encryption Module. Nakon toga je potrebno u administrativnim postavkama sigurnosti, omogućiti šifriranje na strani poslužitelja. Time su sve datoteke, šifrirano pohranjene na poslužitelj. Osim šifriranja na strani poslužitelja, Nextcloud ima već na početku korištenja, automatski uključen zadani modul za šifriranje kućne pohrane (unutarnje pohrane Nextcloud programa).



Slika 18. Šifriranje na strani poslužitelja i šifriranje kućne pohrane [autorski rad].

Za sigurnost podataka i informacija je još potrebna autentifikacija i autorizacija korisnika aplikacije. Administrator može sam kreirati korisnike u obliku gosta, pomoću aplikativnog proširenja „Guests“. Moguća je i registracija korisnika, ali je opcija „Guests“ sigurnija. Pomoću te opcije, mi upravljamo korisničkim računima, a ne sam korisnik. Prilikom kreiranja korisnika, možemo upravljati sljedećim opcijama: postavljanje zaporke, dodavanje maksimalne kvote (koliki kapacitet pohrane je na raspolaganju korisniku), dodavanje E-pošte i dodavanje u grupu. Korisniku nakon prijave, dopušten je reducirani sadržaj API-a (bez mogućnosti mijenjanja postavki sustava ili instaliranja proširenja aplikacija).

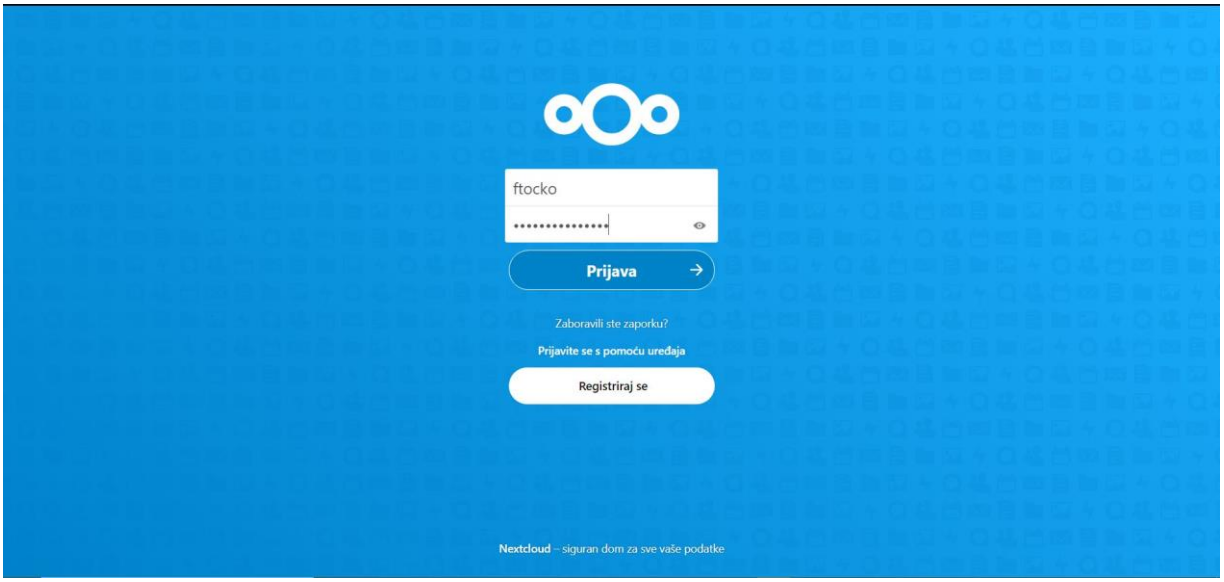


Slika 19. Zaslon dodavanja i izmjene korisnika [autorski rad].

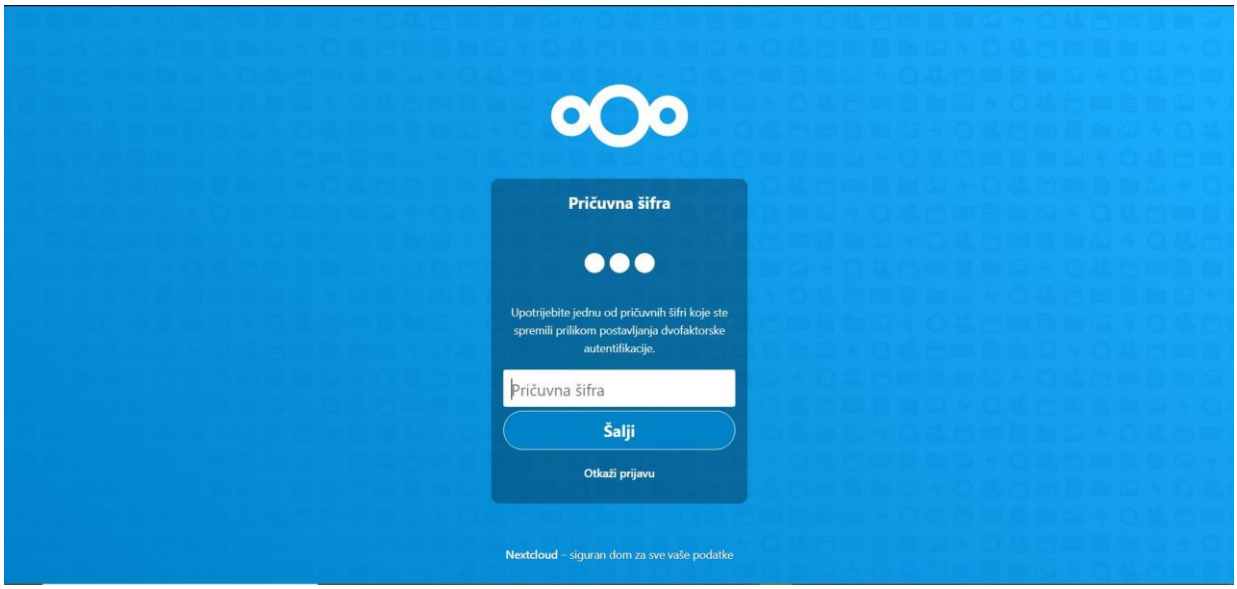
Nextcloud podržava dvofaktorsku autentifikaciju. U postavkama sigurnosti računa, moguće je uključiti istu. Ona se sastoji od dva koraka: unos korisničkog imena i lozinke te unos pričuvne šifre (generira se 10 takvih šifri, koje korisnik lokalno sprema i svaku može samo jedanput iskoristiti, a ukoliko ih sve potroši, iste se mogu ponovo generirati i spremiti). Ovaj tip dvofaktorske autentifikacije je primjenjiv samo za račun administratora.

Slika 20. Dvofaktorska autentifikacija [autorski rad].

Pričuvna šifra nije jedina opcija za dvofaktorsku autentifikaciju, nego unutar aplikacijske trgovine Nextcloud-a, se nalazi još nekoliko proširenja aplikacija za istu. Pomoću tih proširenja, moguće je dodati dvofaktorsku autentifikaciju i za kreiranu grupu korisnika. Postupak dvofaktorske autentifikacije je prikazan na sljedeće dvije slike.



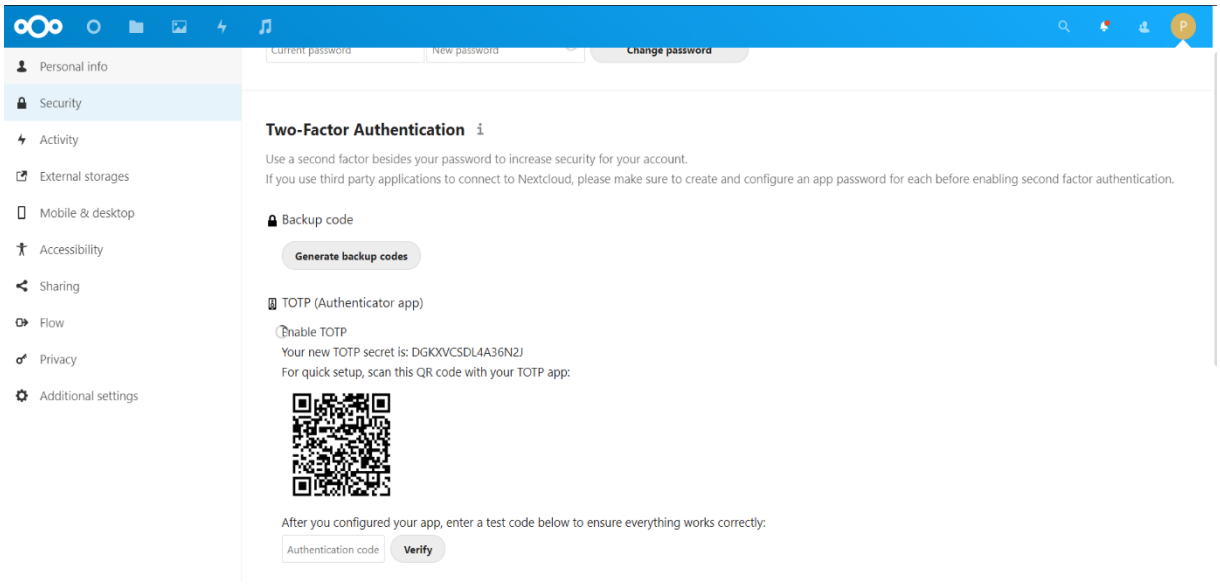
Slika 21. Prvi faktor dvofaktorske autentifikacije [autorski rad].



Slika 22. Drugi faktor dvofaktorske autentifikacije [autorski rad].

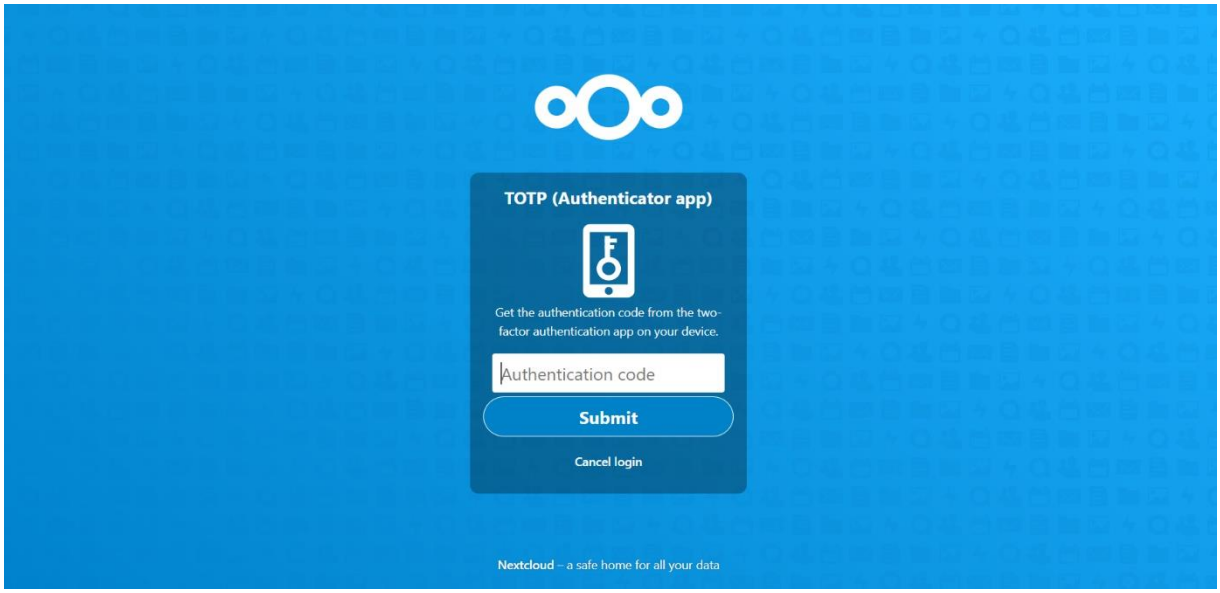
Još jedno vrlo pogodno, aplikacijsko proširenje za dvofaktorsku autentifikaciju se sastoji od TOTP (Time-based One-Time Password), koje izvodi posebna autentifikacijska aplikacija. TOTP je skraćenica za vremenski jednokratnu lozinku, koja je uvijek jedinstvena i generira se algoritmom, koji koristi trenutno vrijeme kao ulaz [58].

Prvi faktor ovog tipa dvofaktorske autentifikacije je naravno, unos korisničkog imena i lozinke, a drugi faktor se konfigurira u sigurnosnim opcijama aplikacije, odjeljak TOTP (Authenticator app), što se može vidjeti na slici 23. Ovaj drugi faktor dvofaktorske autentifikacije može konfigurirati, svaki korisnik aplikacije za sebe, nakon što administrator uključi, da ista bude vidljiva u sigurnosnim opcijama. Korisnik preuzme aplikaciju, „TOTP Authenticator“ na svoj mobilni uređaj iz Trgovine Play. Nakon toga, unutar navedene aplikacije, potrebno je dodati novi račun za TOTP, koristeći ugrađeni QR kod čitač. Skenira se QR kod vidljiv u sigurnosnim opcijama Nextcloud-a i zatim mobilna aplikacija za TOTP, automatski generira jedinstvenu lozinku za taj Nextcloud račun, koju je potrebno unijeti u polje, „Authentication Code“ i klikom na gumb „Verify“, dvofaktorska autentifikacija je uspješno konfigurirana.



Slika 23. Konfiguracija drugog faktora dvofaktorske autentifikacije (TOTP) [autorski rad].

Prvi faktor dvofaktorske autentifikacije je uvijek isti i sastoji se od unosa korisničkog imena i lozinke. Na slici 24. prikazan je drugi faktor dvofaktorske autentifikacije, gdje korisnik treba unijeti lozinku (kod) dobivenu iz mobilne aplikacije, „TOTP Authenticator“ za svoj Nextcloud račun. Svaki puta se generira nova lozinka (kod) nakon proteka određeni broj sekundi.

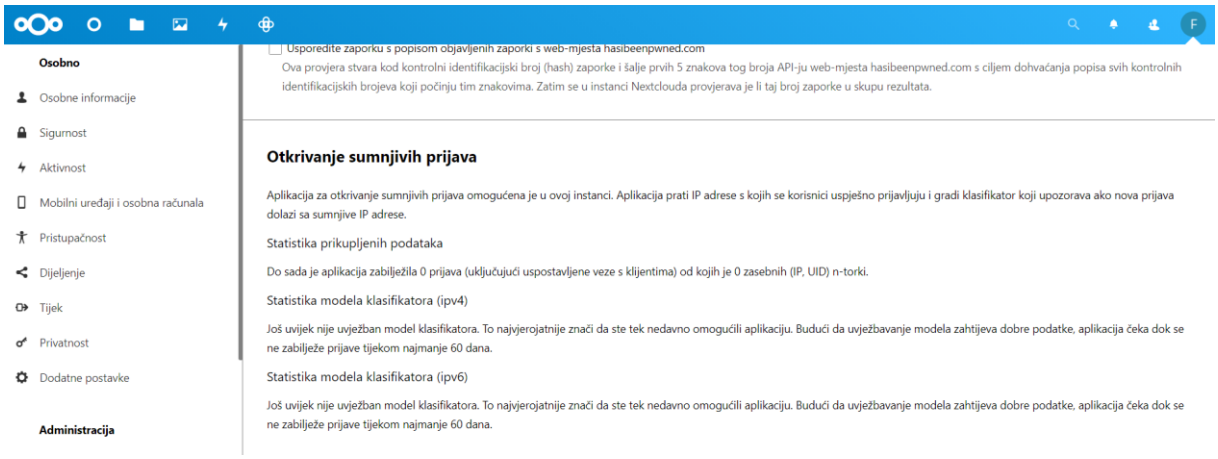


Slika 24. Drugi faktor dvofaktorske autentifikacije (TOTP) [autorski rad].

U Nextcloud-u postoje pravila za upravljanje zaporkama. Time mi (administrator) možemo mijenjati postavke zaporka, a to uključuje, npr. minimalna dužina zaporke, broj pokušaja prijave prije blokiranja korisničkog računa, zabrana čestih zaporki, obavezna uporaba velikih i malih slova, broj dana do isteka zaporke itd. Time se povećava sigurnost zaporka korisnika. Za upravljanje identitetom, dvofaktorska autentifikacija, snažna zaporka i opcija „Guests“ su krucijalne jer neovlaštenom provalom u račun korisnika, može doći do narušenja njihove privatnosti (gubitka podataka ili slično).

Slika 25. Pravila za upravljanje zaporkama [autorski rad].

Opcija „otkrivanje sumnjivih prijava“ prati s koje IP adrese, se korisnici prijavljuju u Nextcloud i šalje upozorenje, ako prijava dolazi sa sumnjive IP adrese.

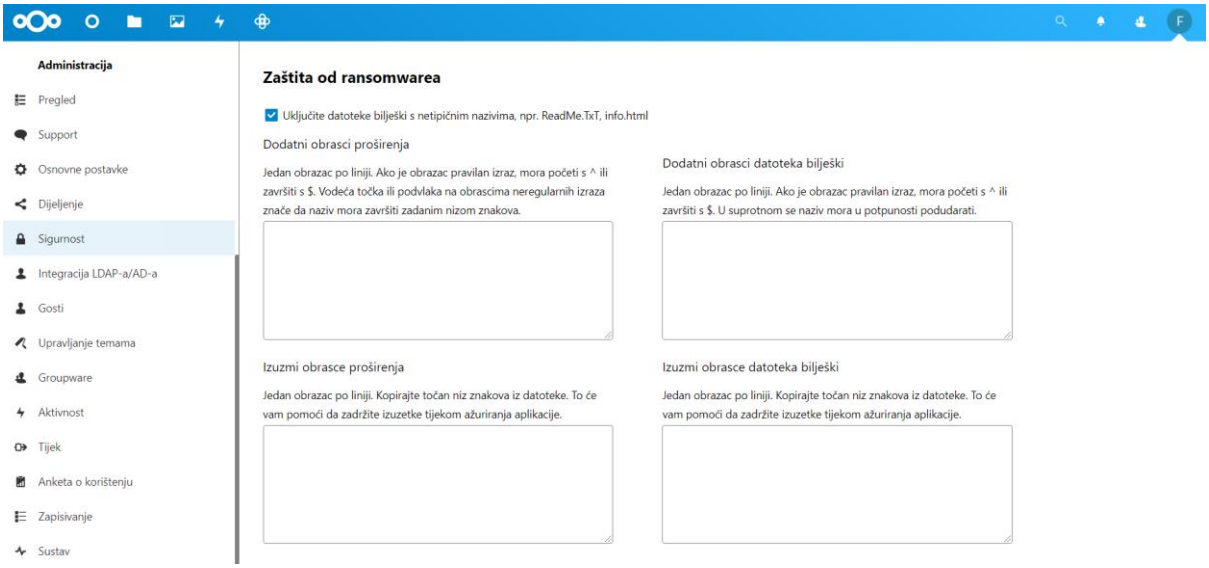


Slika 26. Otkrivanje sumnjivih prijava [autorski rad].

Što se tiče API sigurnosti, Nextcloud ima opciju dodavanja OAuth 2.0 klijenta. Može se dodati aplikacija, iz koje se preusmjerava prema Nextcloud-u ili koja komunicira s istim, bez otkrivanja zaporka, već koristeći autentifikacijski token, koji Nextcloud dodijeljuje toj aplikaciji, nakon uspješne autentifikacije preko certifikata.

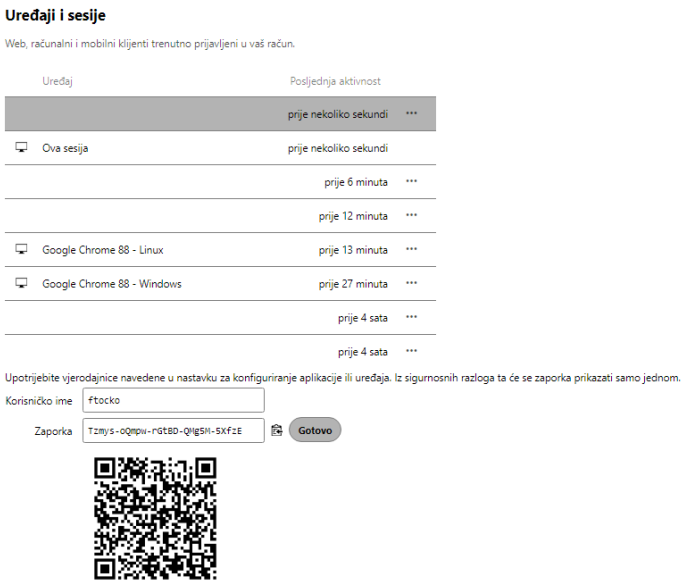
Slika 27. OAuth 2.0 [autorski rad].

Nextcloud ima podršku, tj. proširenje aplikacije za zaštitu od ransomwarea. To je vrsta zlćudnog programa, koji zaražava korisničko računalo, u smislu zaključavanja računala ili kriptiranja korisničkih datoteka i pritom traži naknadu (novčani iznos), koju korisnik (meta) treba podmiriti, za potrebe otključavanja računala ili dekriptiranja datoteka [41]. Ovakav zlćudni program, može korisniku zaključati API Nextcloud-a ili njegove datoteke na istom. Zato aplikacija za zaštitu od ransomwarea, skenira i analizira sve datoteke, koje korisnik pohranjuje na Nextcloud jer iste mogu biti zaražene tom vrstom zlćudnog programa i narušiti sigurnost Nextcloud-a. U Nextcloud-u postoji i proširenje aplikacije za skeniranje virusa (analizira i skenira sve uploadane, korisničke datoteke).



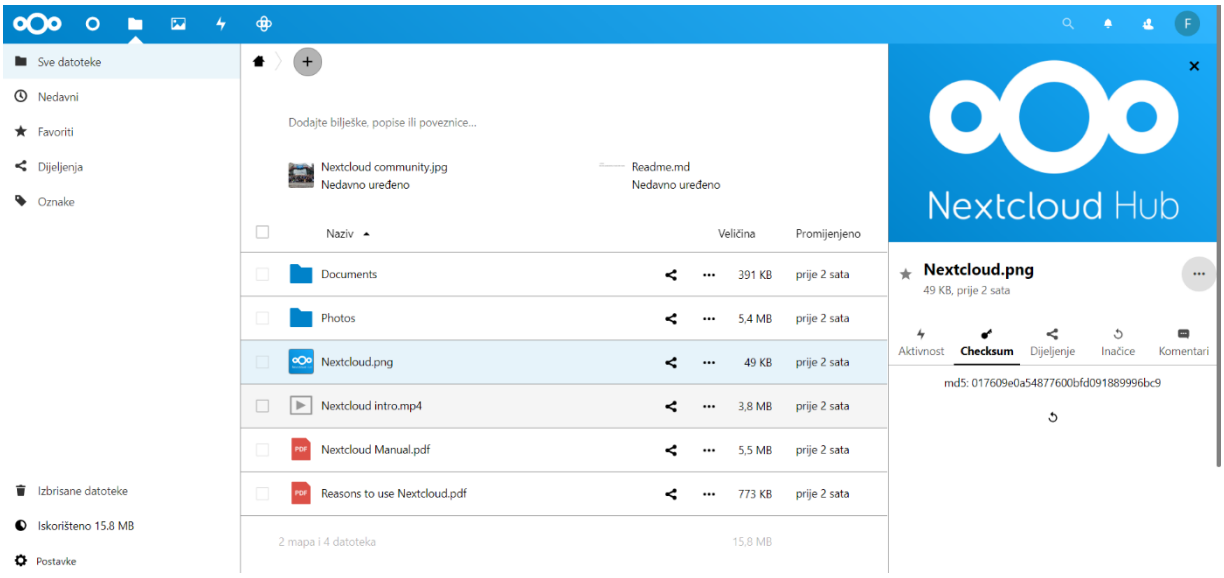
Slika 28. Zaštita od ransomwarea [autorski rad].

Za prijavu na Nextcloud preko mobilne aplikacije, postoji opcija „Uređaji i sesije“. Kod te opcije se stvori zaporka ili QR kod, pomoću kojih se automatski prijavljujemo na korisnički račun Nextcloud-a, preko mobilne aplikacije. Ovo je siguran način komunikacije između PC i mobilne aplikacije Nextcloud-a.



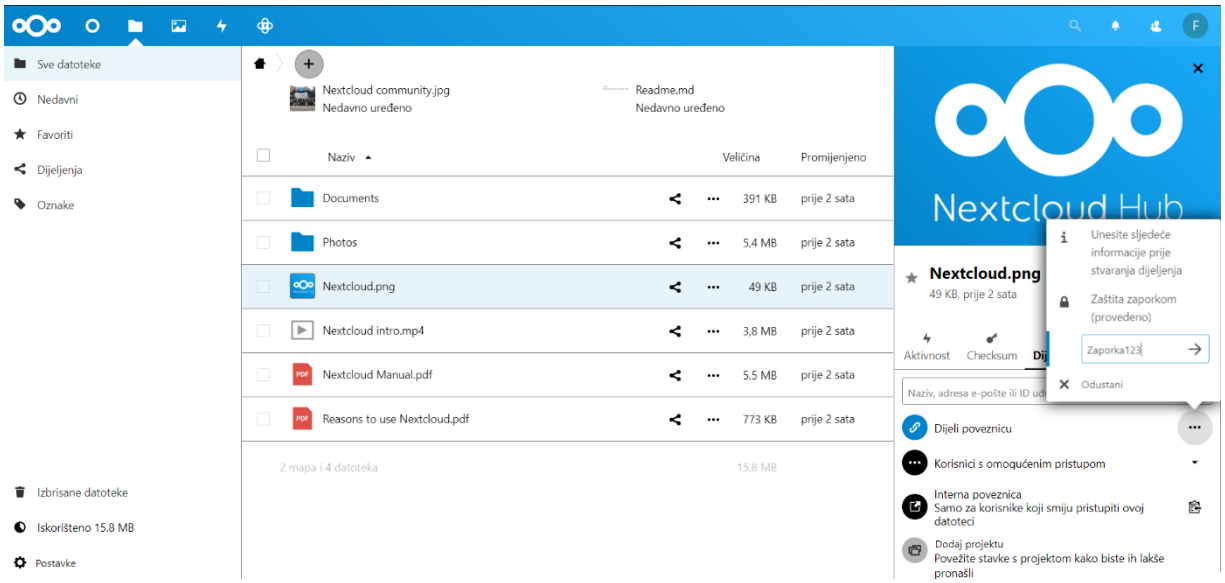
Slika 29. Opcija „Uređaji i sesije“ [autorski rad].

Za provjeru integriteta podataka (datoteka), postoji opcija „Checksum“. Klikom na pojedinosti pohranjene datoteke i zatim klikom na „Checksum“, moguće je izračunati zaštitnu sumu datoteke pomoću algoritama, npr. MD5, SHA256, CRC32 itd.

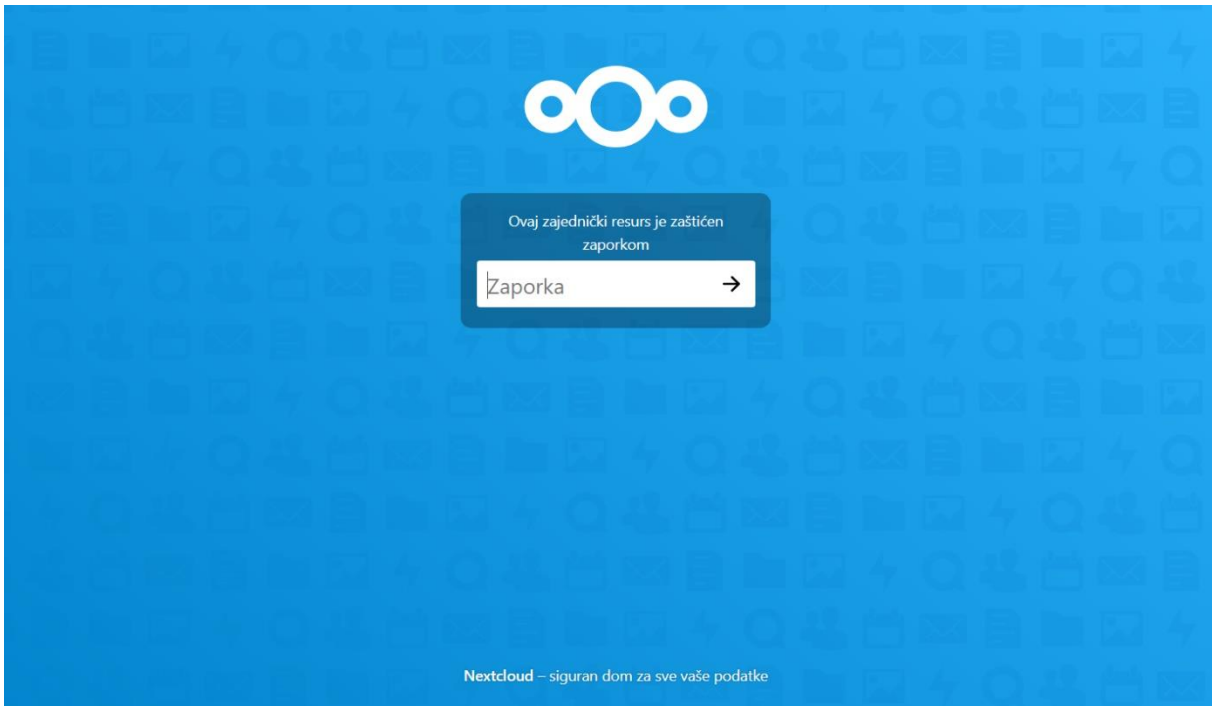


Slika 30. Opcija „Checksum“ [autorski rad].

U Nextcloud-u je moguće i šifrirano dijeljenje poveznica. Za željenu datoteku se stvori javna poveznica, u kojoj se pristup resursu (datoteci) zaštićuje zaporkom i pomoću toga je on dostupna, samo korisnicima, koji posjeduju traženu zaporku. Postupak je ilustriran na sljedeće dvije slike.

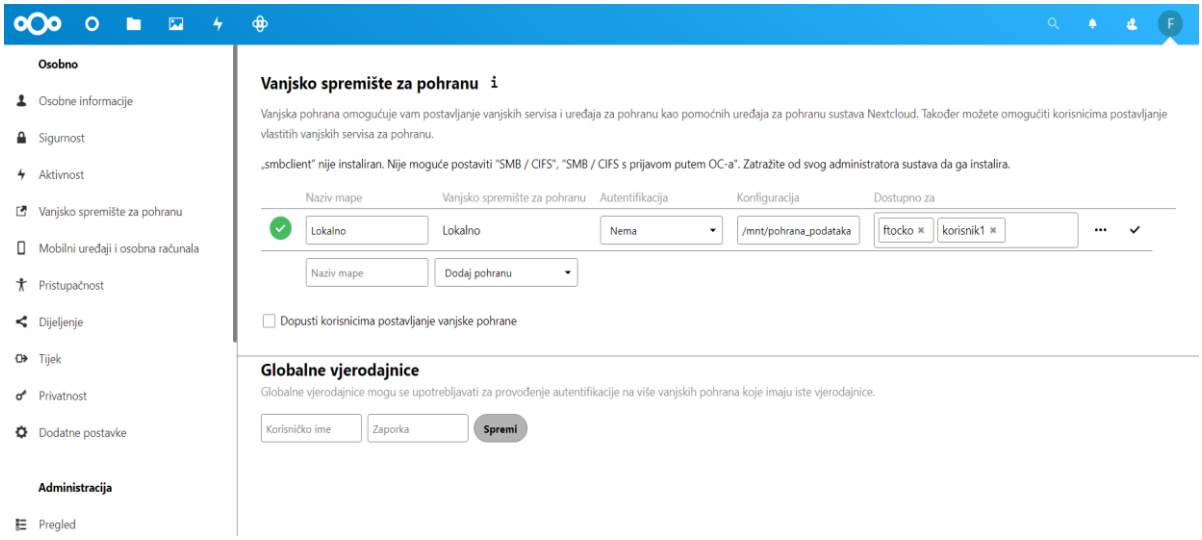


Slika 31. Stvaranje dijeljene poveznice i zaštita resursa zaporkom [autorski rad].

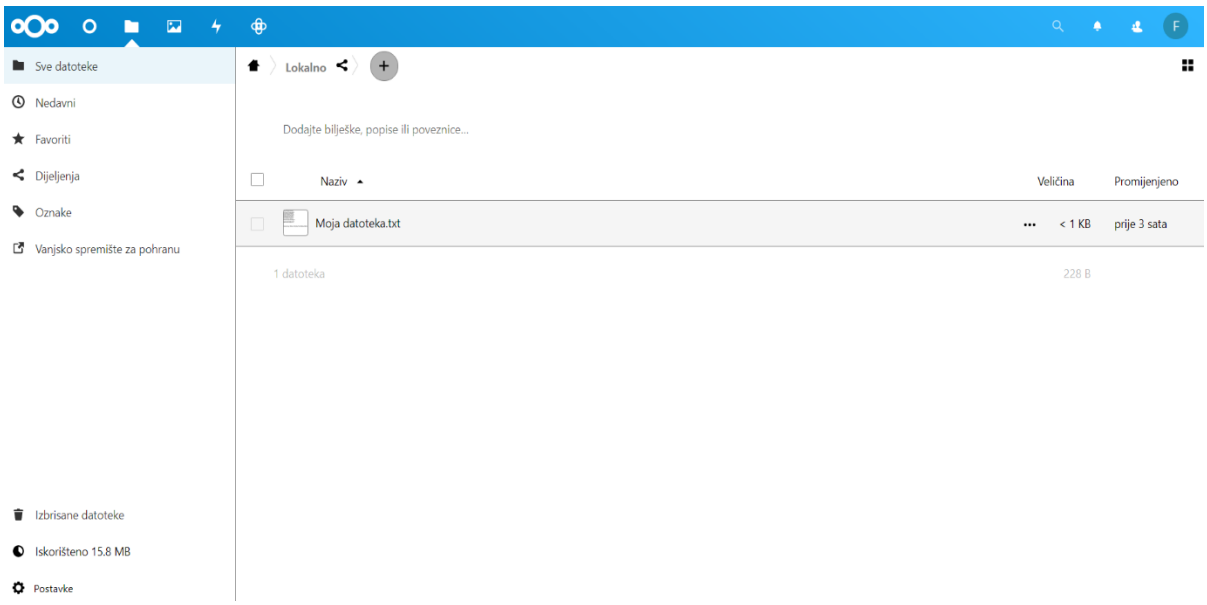


Slika 32. Prikaz zajedničkog, zaštićenog resursa (datoteke) [autorski rad].

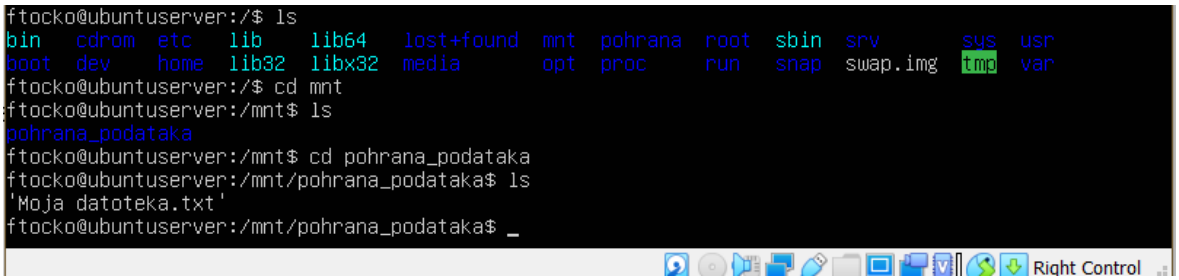
Za potpunu kontrolu nad pohranom podataka u Nextcloud je moguće, dodati opciju vanjskog spremišta za pohranu. Podaci se time mogu pohranjivati, lokalno na vlastiti server. Ovo predstavlja visoku dozu kontrole i sigurnosti. Za tu svrhu se koristi proširenje aplikacije, „External storage support“. Prvo se u terminalu Ubuntu Servera izvodi naredba: sudo snap connect nextcloud:removable-media. Zatim se u postavkama vanjskog spremišta za pohranu, konfigurira lokalna pohrana podataka. Nakon toga je kod izbornika datoteka, dodana mapa lokalno, u kojoj će sve uploadane, korisničke datoteke biti automatski pohranjene na vlastiti, u mojem slučaju, Ubuntu Server. Datoteke pohranjene na taj način su automatski šifrirane (zaštićene u mirovanju).



Slika 33. Konfiguracija vanjskog spremišta za pohranu [autorski rad].



Slika 34. Pohranjena tekstualna datoteka u mapi „Lokalno“ [autorski rad].

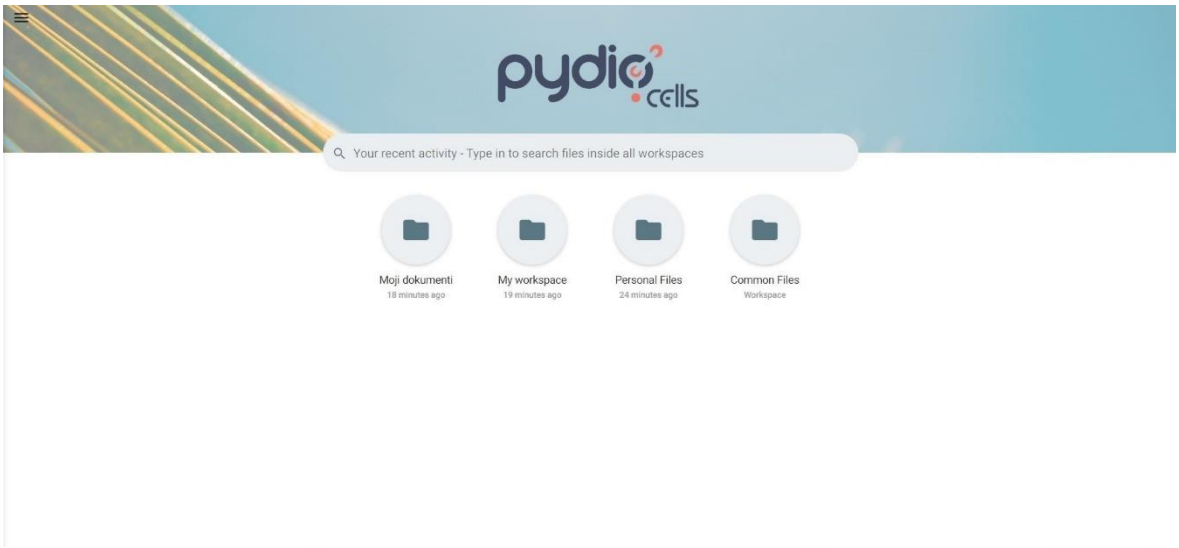


Slika 35. Pohranjena tekstualna datoteka na Ubuntu Serveru [autorski rad].

Na slikama pod rednim brojevima: 34. i 35., se vidi da tekstualna datoteka, Moja datoteka.txt nakon što je uploadana u mapu „Lokalno“, ista je automatski pohranjena lokalno na Ubuntu Server.

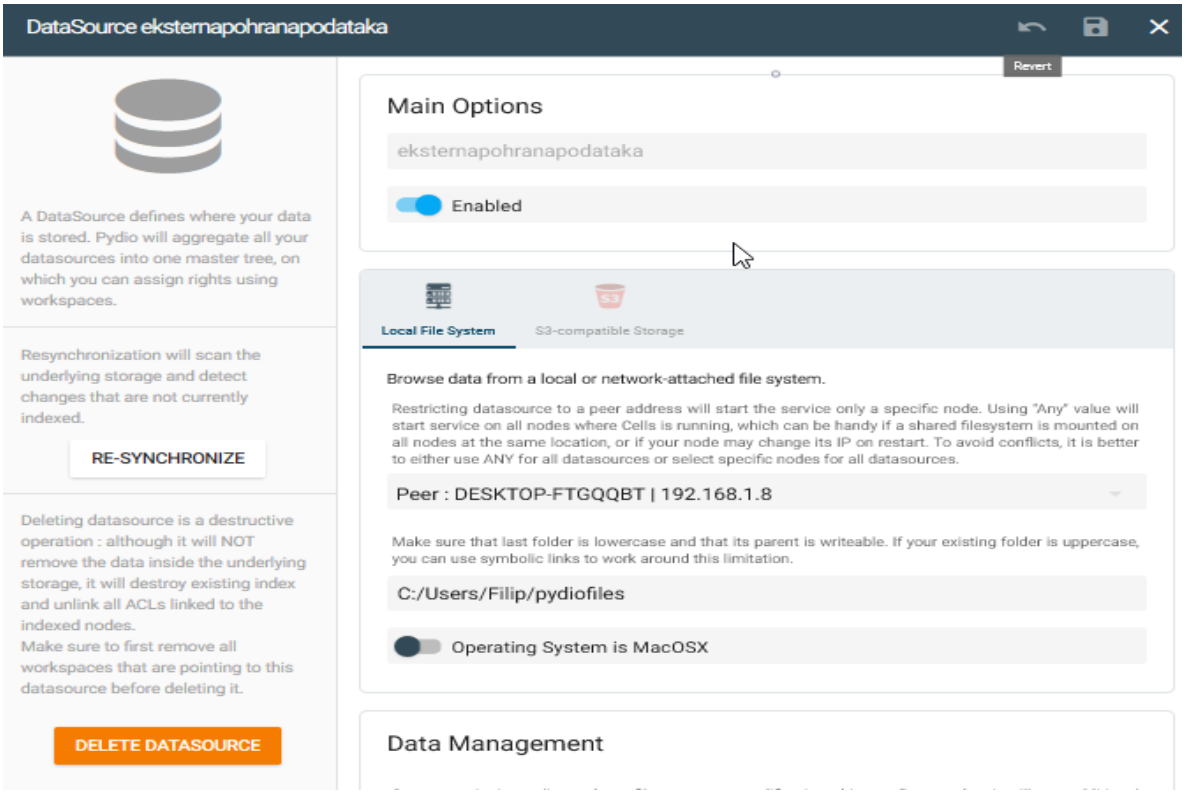
7.2. Implementacija i testiranje sigurnosti Pydio-a

Pydio (Pydio Cells) je konfiguriran na Windows 10 platformi unutar VirtualBox-a. Za implementaciju je bilo potrebno preuzeti: MySQLServer i izvršnu datoteku cells.exe. MySQLServer pruža usluge baze podataka, potrebne za Pydio, a aplikacijski podaci Pydia su spremljeni na vlastitoj Windows 10 platformi. Pokretanjem ranije navedene, izvršne datoteke u Windows PowerShell-u, kreće instalacija Pydia u web-pregledniku, gdje se konfigurira administratorski račun, povezivanje s bazom podataka i ostale stvari. Dakle, vlastiti Windows 10 služi za interni hosting Pydio programa. Pydio se pokreće unutar Windows PowerShell-a, pomoću naredbe: .\cells.exe start. Nakon toga je isti dostupan, u mojem slučaju, na domeni: https://192.168.1.8:8080. Moguće je i promijeniti broj porta, pomoću naredbe: .\cells.exe configure sites. Podrška za Windows 10 je velika prednost ovog programa jer nudi pogodniju implementaciju.



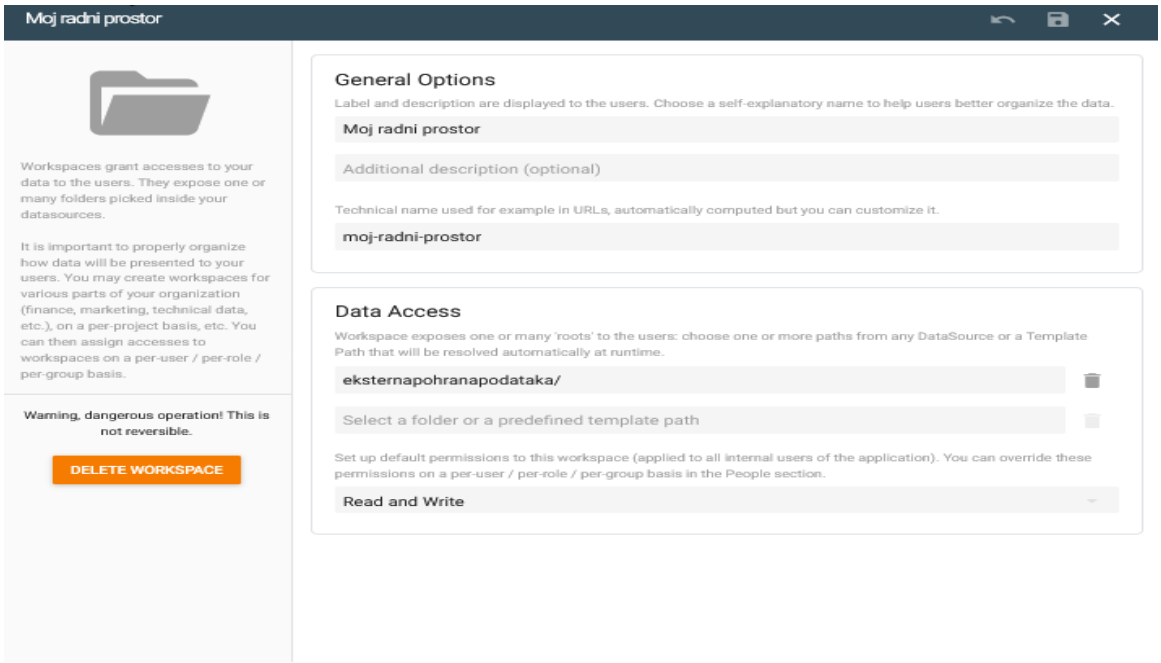
Slika 36. Sučelje Pydio-a [autorski rad].

Za potpunu kontrolu nad podacima, Pydio ima podršku za eksternu pohranu podataka. Na sljedećoj slici je prikazana konfiguracija iste. Unutar Windows 10, kreirana je mapa s dozvoljenim pristupom i odabrana kao izvor eksterne pohrane podataka u Pydio-u. Nakon toga se ovakav tip pohrane, može koristiti za „workspace“.

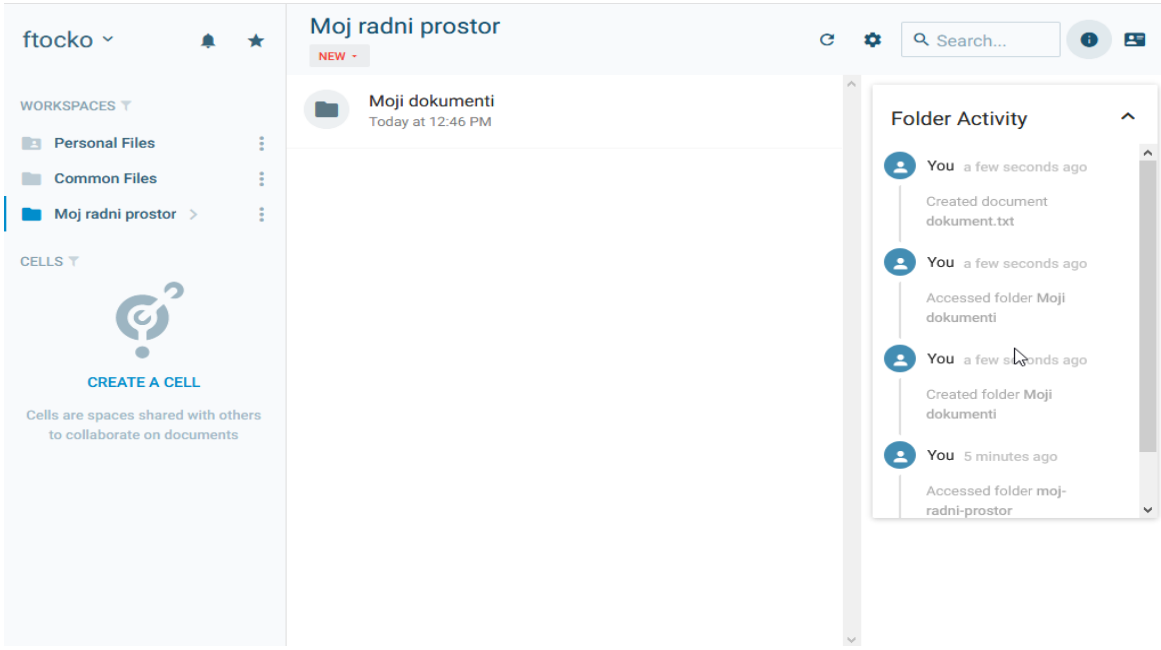


Slika 37. Konfiguracija eksterne pohrane podataka [autorski rad].

Workspace pod nazivom „Moj radni prostor“ je kreiran i pridružena mu je eksterna pohrana podataka te je dodano pravo čitanja i pisanja, kako bi se mogao isti koristiti. On služi kao glavno sjedište odnosno vlastito mjesto, gdje korisnik može pristupiti svim svojim pohranjenim datotekama. Za workspace je dostupno i praćenje aktivnosti mape.

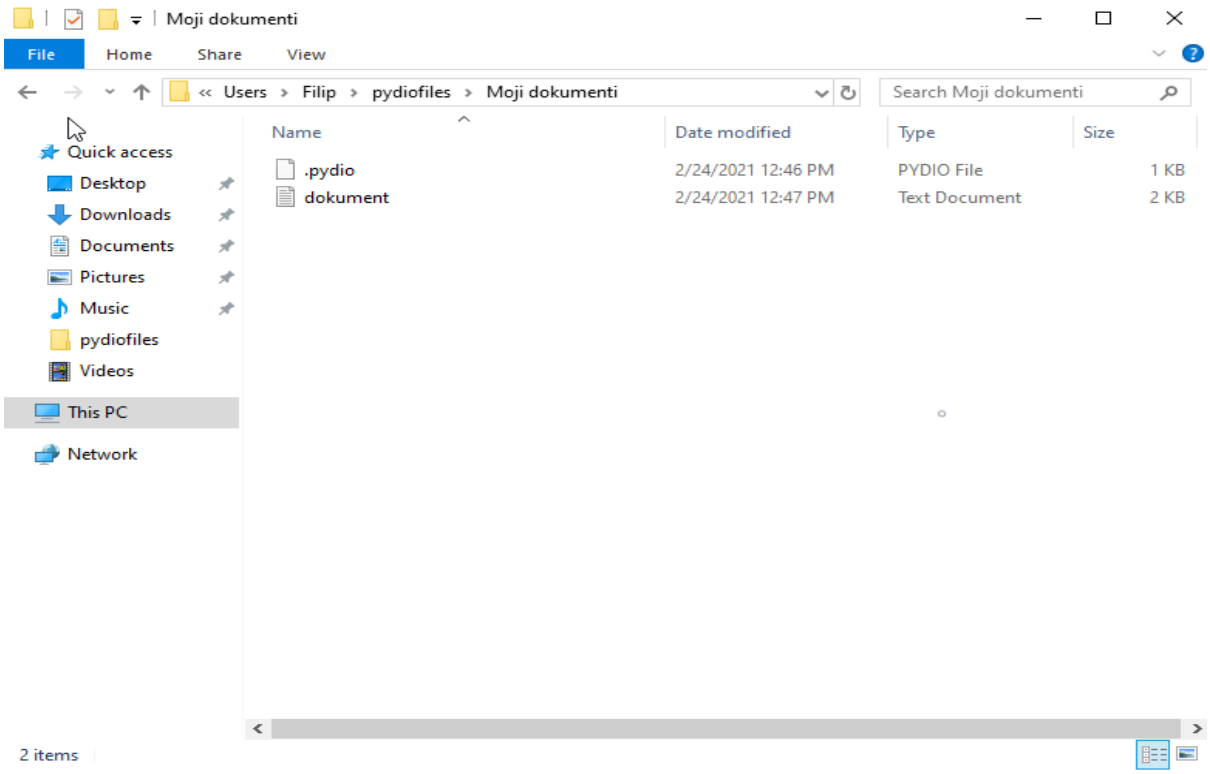


Slika 38. Konfiguracija workspace-a: „Moj radni prostor“ [autorski rad].



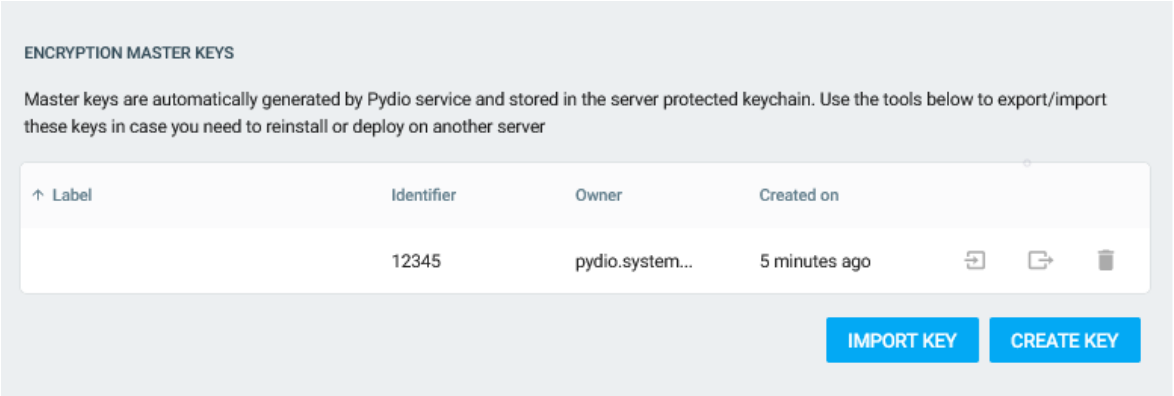
Slika 39. Workspace: „Moj radni prostor“ [autorski rad].

Unutar workspace-a, „Moj radni prostor“, kreirana je mapa „Moji dokumenti“ i uploadan dokument u istu. Na sljedećoj slici se vidi uploadani dokument u navedenoj mapi, koji su pohranjeni, lokalno na Windows 10 (eksterna pohrana podataka). Time je eksterna pohrana podataka, uspješno konfigurirana, a „Moj radni prostor“ je koristi za spremanje korisničkih podataka.



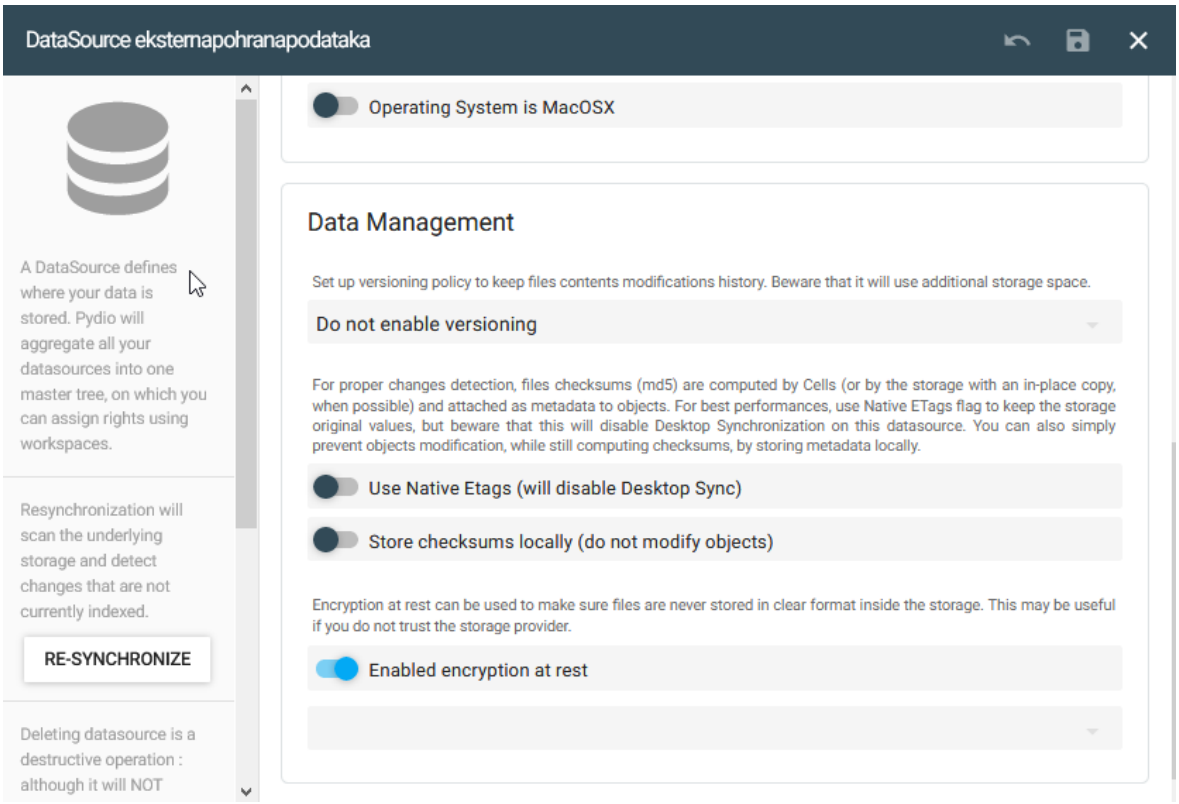
Slika 40. Eksterna pohrana podataka [autorski rad].

Zaštita podataka u prijenosu je osigurana pomoću HTTPS protokola. Koristi se „self-signed“ TLS. Pydio ima automatsku podršku za isti. Za zaštitu podataka u mirovanju, koristi se šifriranje na poslužitelju (klijent upravlja ključem). Klijent sam kreira ključ za enkriptiranje, a poslužitelj (Pydio) omogućuje algoritam enkriptiranja, pomoću navedenog ključa.



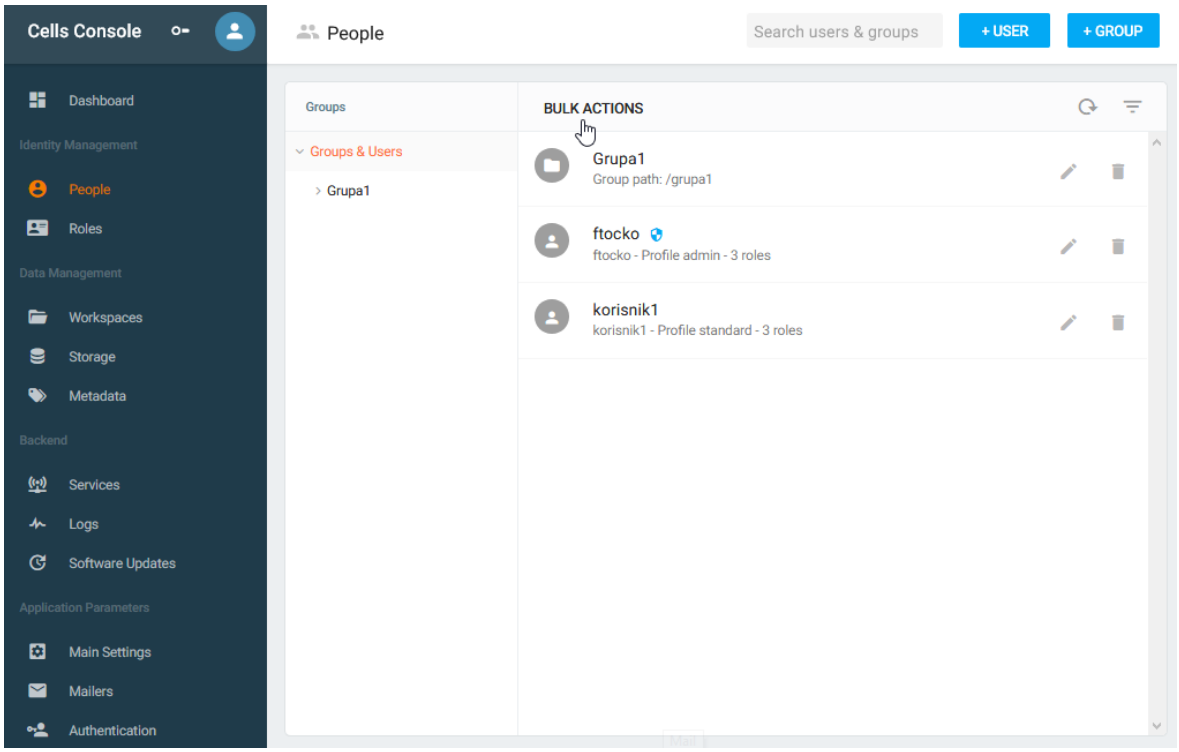
Slika 41. Konfiguracija ključa za enkriptiranje [autorski rad].

Na slici 41. se vidi vlastiti konfigurirani ključ za enkriptiranje, sa oznakom: 12345. Omogućavanjem enkriptiranja u mirovanju, ranije kreirana eksterna pohrana podataka je zaštićena u mirovanju, pomoću enkriptiranja s kreiranim ključem.



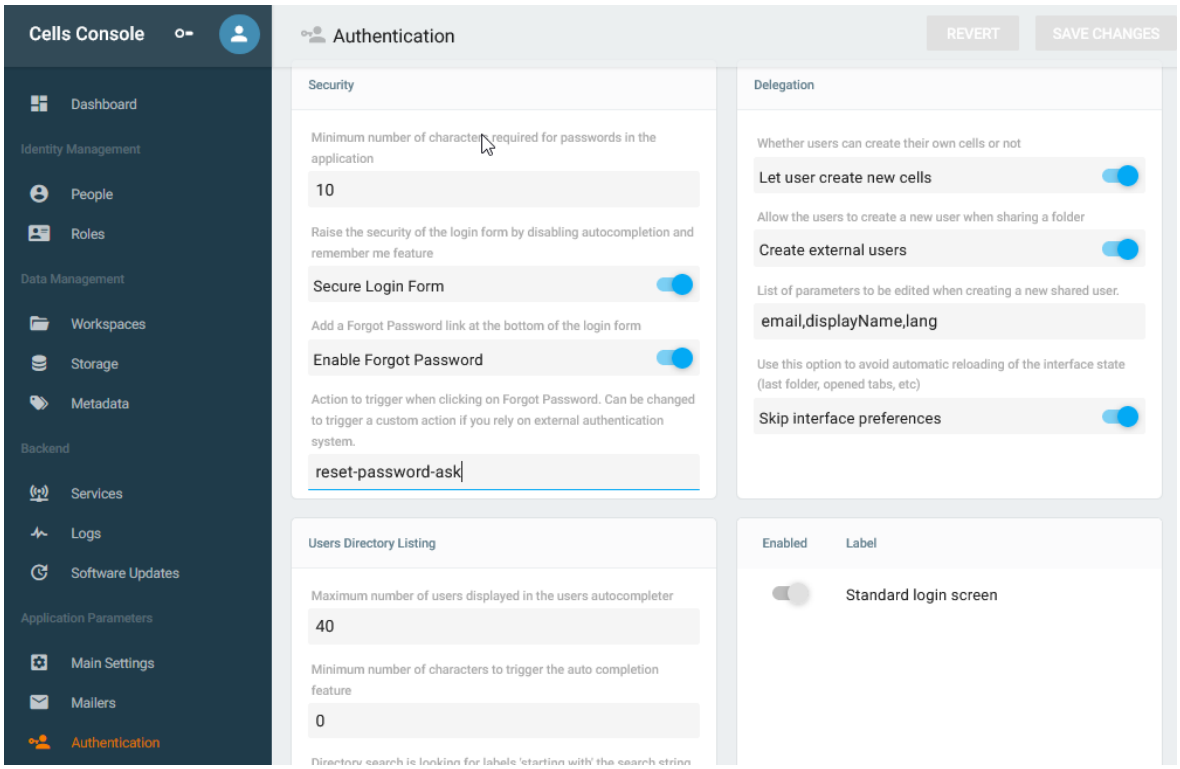
Slika 42. Konfiguracija ekriptiranja u mirovanju [autorski rad].

Administrator može sam kreirati korisnike i grupe te im pritom dodijeliti uloge. Prilikom kreiranja korisnika, definira se i šifra za prijavu, prava pristupa određenom workspace-u, te se time postiže određena doza sigurnosti.

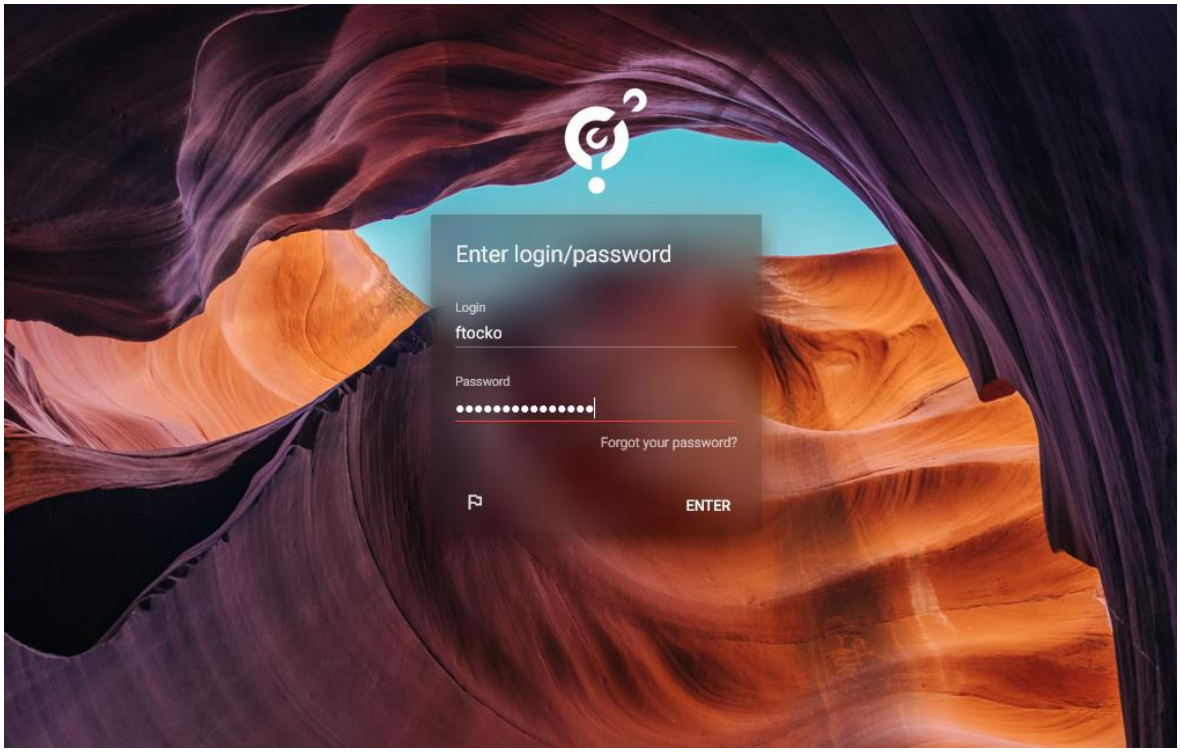


Slika 43. Zaslon upravljanja korisnicima i grupama [autorski rad].

Pydio nema podršku za dvofaktorsku autentifikaciju. Za autentifikaciju su dostupne samo određene postavke prijave. Moguće je: definiranje broja znakova zaporke, uključivanje sigurnog obrasca za prijavu (bez značajki: „remember me“ i „autocompletion“) i sigurnosnog povrata lozinke. Kod postavki delegacije, može se dopustiti kreiranim korisnicima: kreiranje ćelija i eksternih korisnika. Nepostojanje podrške za dvofaktorsku autentifikaciju je ozbiljan nedostatak Pydio-a. Uz sigurnosne postavke prijave, korisnički računi nisu i dalje u potpunosti sigurnosno zaštićeni. Na sljedećoj slici se vidi zaslon autentifikacije, koji obuhvaća: sigurnosne postavke prijave i postavke delegacije.

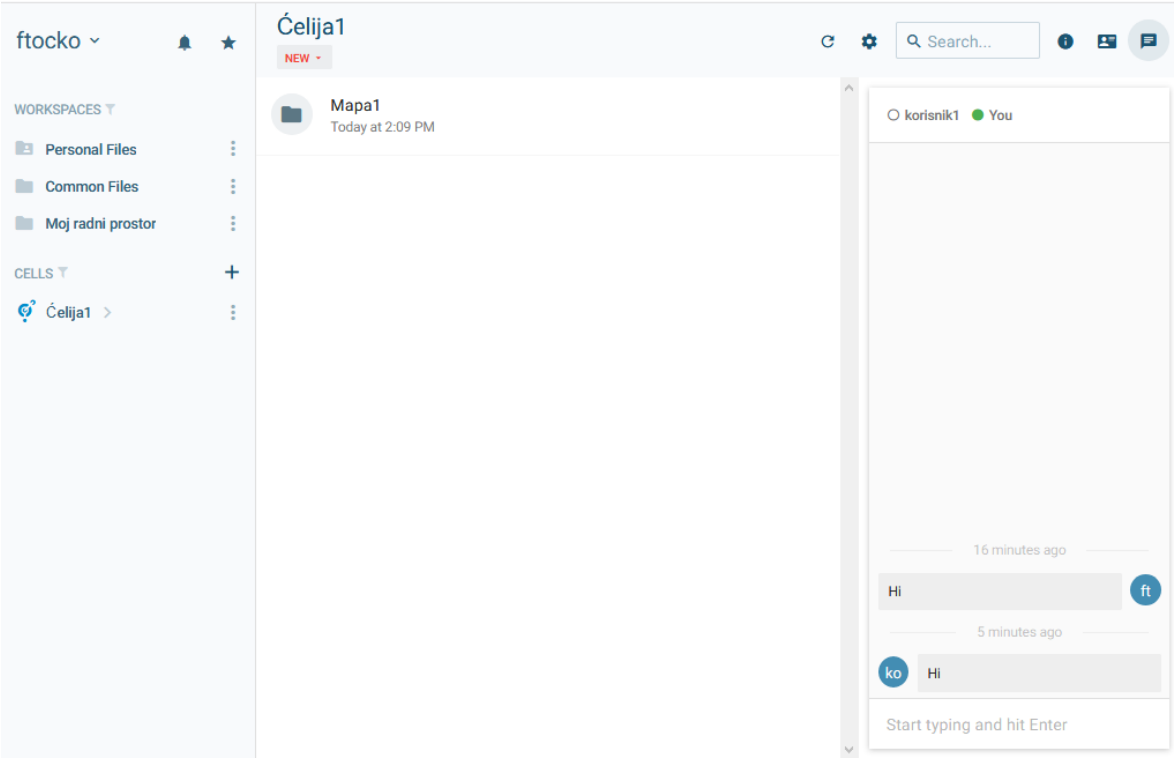


Slika 44. Zaslon autentifikacije [autorski rad].



Slika 45. Zaslon prijave [autorski rad].

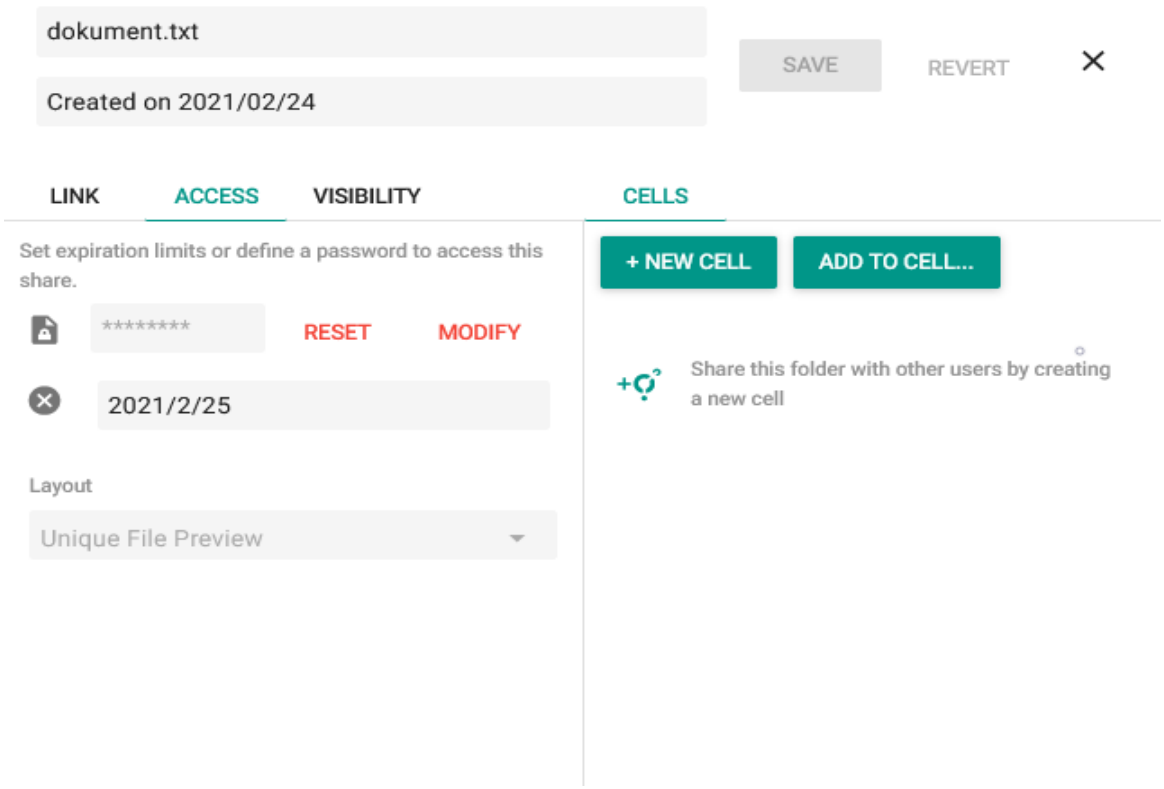
Glavna značajka Pydio-a su ćelije, a drugi naziv istoga je „Pydio Cells“, što jasno ukazuje na iste. Ćelije se koriste u osobne i poslovne svrhe. One pružaju okruženje unutar kojeg, korisnici mogu razmjenjivati datoteke i komunicirati preko chat-a.



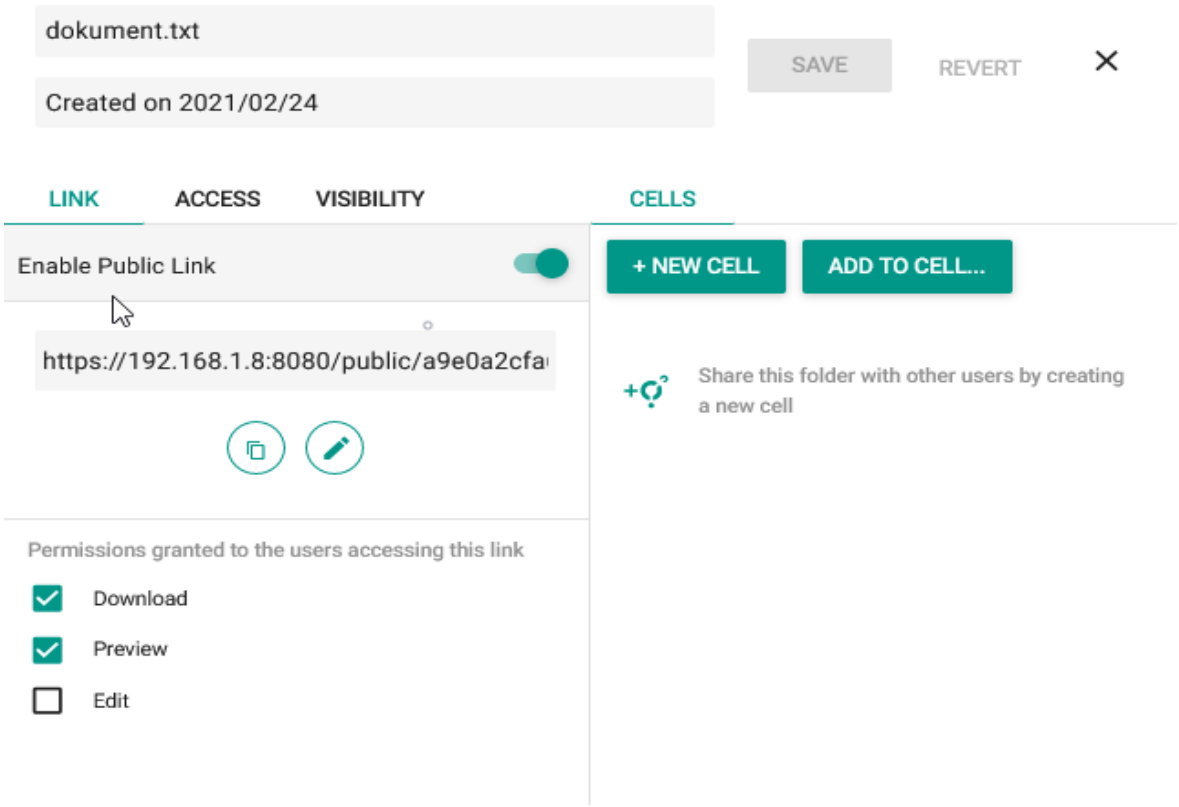
Slika 46. Prikaz ćelije [autorski rad].

Na slici 46. se nalazi prikaz kreirane ćelije, pod nazivom Ćelija1. Ćeliji je dodan korisnik: korisnik1. Time korisnik1 i administrator (vlasnik ćelije) mogu međusobno poslovati. Oni se vidi kod chat-a, kao lista aktivnih korisnika. U opcijama delegacije, moguće je omogućiti i eksternim korisnicima (npr. korisnik1) pravo kreiranja ćelija.

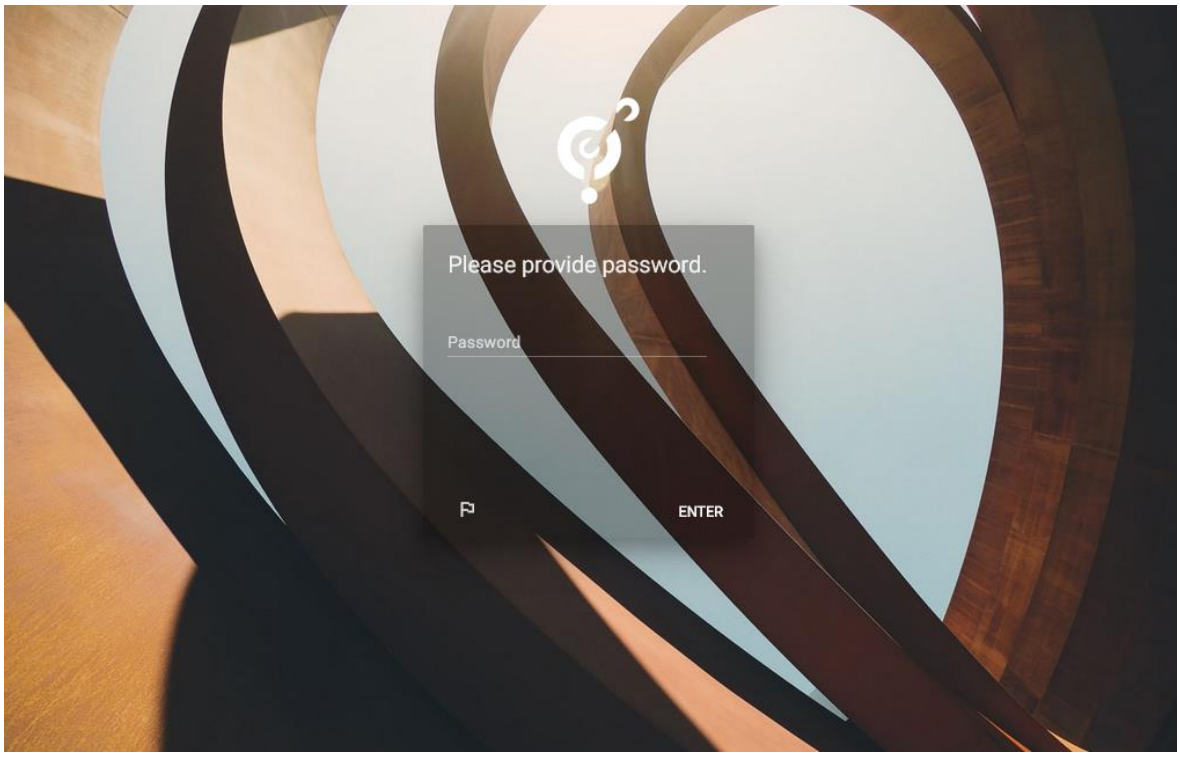
Unutar ćelija kao i workspace-a, moguće je šifrirano dijeljenje datoteka. Kreira se javna poveznica i dodaje se šifra za pristup resursu (datoteci) te datum isteka poveznice. Omogućeno je također dodati dopuštenje radnje, prilikom pristupa datoteci, poput: preuzimanje, pregled i izmjena. Postoje opcije: kreiranja nove ćelije za datoteku ili dodavanje datoteke u ćeliju (ukoliko datoteka nije dio ćelije).



Slika 47. Sigurnosne postavke dijeljenja [autorski rad].



Slika 48. Dopuštene radnje korisnicima poveznice [autorski rad].



Slika 49. Prikaz zaštićenog resursa (datoteke) [autorski rad].

Ovo je sve što Pydio nudi krajnjem korisniku u svom besplatnom izdanju. „Enterprise“ izdanje Pydio-a nudi još sigurnosnih značajki: OAuth2, Open ID Connect, LDAP i reviziju (za praćenje aktivnosti svih korisnika). U usporedbi s Nextcloud-om, Pydio nema dvofaktorske autentifikacije, ne nudi u besplatnoj verziji, OAuth2 i nema zaštite od virusa (zlonamjernih programa).

8. Zaključak

Računarstvo u oblaku je područje informatike, koje se sve više razvija. Sve što je potrebno za korištenje oblaka je dobra Internet veza i moguće mu je pristupiti s bilo kojeg uređaja i lokacije. Usluge u oblaku smanjuju troškove poslovanja i povećavaju njegovu efikasnost te nude također neograničenu osobnu pohranu podataka. Problem koji se javlja kod toga je upitna sigurnost, tako spremljenih podataka jer su korisnički podaci povjereni na čuvanje pružatelju usluga u oblaku. Zato se počinju koristiti privatni oblaci, koji imaju znatno veću sigurnost i usmjereni su točno određenoj organizaciji, za razliku od javnih oblaka. Postoje dva konteksta korištenja privatnih oblaka: upravljani privatni oblaci i vlastita implementacija privatnih oblaka. Problem kod upravljanih privatnih oblaka je upitno povjerenje u pružatelja usluge, a kod vlastite implementacije privatnih oblaka, visoki troškovi održavanja i potreba za kvalitetnim stručnjacima za sigurnost.

Rješenja (tehnologije) za privatne oblake na neki način rješavaju, navedene nedostatke konteksta privatnih oblaka. Ona omogućuju implementaciju tzv. „self-hosted“ privatnih oblaka, gdje sve što organizacija treba osigurati su: mrežna infrastruktura i poslužitelj, a sve ostalo uključujući sigurnosne značajke je integrirano u samoj Web aplikaciji za privatni oblak. Organizacija ima kontrolu nad tom aplikacijom na svojem poslužitelju i može uključiti eksternu pohranu podataka za potpuniju kontrolu. Dakle, ovo su na neki način gotova rješenja za privatne oblake, koja su vrlo jednostavna za implementirat, smanjuju troškove i vrlo su efikasna. Najpopularnija rješenja su: Nextcloud, ownCloud, Seafile, FileRun i Pydio (Pydio Cells). Kao što je navedeno, ista sadrže sigurnosne značajke, koje je moguće uključiti. One su: zaštita podataka u mirovanju i prijenosu (enkriptiranje podataka), API sigurnost (najčešće OAuth 2.0), upravljanje identitetom i pristupom (najčešće korisnici i uloge, dvofaktorska autentifikacija, zaštita od Brute-Force napada, postavke jačine zaporke, LDAP), antivirusna zaštita, sigurnosni povrati lozinke i eksterna pohrana podataka. Svako rješenje nudi veći ili manji dio navednih sigurnosnih značajki, ali ono i dalje pruža sasvim zadovoljavajuću razinu podrške sigurnosti. Ove sigurnosne značajke su ujedno i sigurnosni aspekti privatnih oblaka. Neka rješenja i dalje sadrže mnogo sigurnosnih ranjivosti u eksternoj infrastrukturi (Web aplikacija) pa je preporučljivo provoditi penetracijska testiranja, koja omogućuju identificiranje ranjivih sigurnosnih točaka.

U budućnosti se očekuje još veći napredak u području sigurnosti privatnih oblaka (osobito u sigurnosti za modele usluga PaaS i SaaS, gdje zaštita podataka u mirovanju, nije

još uvijek potpuno izvediva), ali oni i sada već pružaju znatno veću razinu sigurnosti od javnih oblaka. Svaka organizacija i korisnik bi trebali koristiti rješenja za privatne oblake, koja su puno sigurnija i nude više mogućnosti od klasičnih, javnih i privatnih oblaka. Korištenjem rješenja za privatne oblake uz vođenje računa o smjernicama za sigurnost, korisnik dobiva idealno i sigurno cloud rješenje.

Popis literature

[1] J. Frankenfield, ‘How Cloud Computing Works’, 2020. [Na Internetu]. Dostupno: https://www.investopedia.com/terms/c/cloud-computing.asp [pristupano: 02.02.2021].

[2] „What is private cloud?“ (bez dat.). U Red Hat. Dostupno: https://www.redhat.com/en/topics/cloud-computing/what-is-private-cloud [pristupano: 02.02.2021].

[3] „Managed Private Cloud“ (bez dat.). U *Apprenda*. Dostupno: https://apprenda.com/library/paas/managed-private-cloud/ [pristupano 02.02.2021].

[4] A. Rashid i A. Chaturvedi, „Cloud Computing Characteristics and Services: A Brief Review“, *INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING*, sv. 7, str. 421–426, velj. 2019, doi: 10.26438/ijcse/v7i2.421426.

[5] „How does cloud computing impact Software Testing?“ [slika] (bez dat.). Dostupno: https://astheqaworldturns.wordpress.com/2011/04/11/how-does-cloud-computing-impact-sqa/ [pristupano: 02.02.2021.].

[6] „Cloud Computing Architecture - javatpoint“ (bez dat.). U *www.javatpoint.com*. Dostupno: https://www.javatpoint.com/cloud-computing-architecture [pristupano: 02.02.2021.].

[7] „Cloud Computing“ [slika] (bez dat.). Dostupno: http://triple777.net/services/cloud-computing/ [pristupano: 02.02.2021.].

[8] „Top 10 Cloud Service Providers In 2020“ (bez dat.). U c-sharpcorner.com. Dostupno: https://www.c-sharpcorner.com/article/top-10-cloud-service-providers/ [pristupano: 02.02.2021.].

[9] R. Mukherjee i D. F., „Best cloud storage 2021“, 2021. [Na Internetu]. Dostupno: https://www.tomsguide.com/buying-guide/best-cloud-storage [pristupano: 02.02.2021.].

[10] „Characteristics of Cloud Computing“, *GeeksforGeeks*, kol. 30, 2019. https://www.geeksforgeeks.org/characteristics-of-cloud-computing/ (pristupljeno velj. 03, 2021).

[11] A. Huth i J. Cebula, „The Basics of Cloud Computing“, str. 4.

[12] „Types of Cloud Computing — an Extensive Guide on Cloud Solutions and Technologies in 2021“, *Kinsta*, svi. 04, 2020. https://kinsta.com/blog/types-of-cloud-computing/ (pristupljeno velj. 03, 2021).

[13] „BMC16_001_IIG_V2“. https://view.ceros.com/compuware/bmc16-001-iig-v2 (pristupljeno velj. 03, 2021).

[14] „What is PaaS? Platform as a Service | Microsoft Azure“. https://azure.microsoft.com/en-us/overview/what-is-paas/ (pristupljeno velj. 03, 2021).

[15] Pankaj Sareen, „Cloud Computing: Types, Architecture, Applications, Concerns, Virtualization and Role of IT Governance in Cloud“, *INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING,* sv. 3, str. 533-537, ožujak 2013, doi: https://d1wqtxts1xzle7.cloudfront.net/51531005/V3I3-0320.pdf.

[16] M. Elliott, „A Beginner’s Guide to Security as a Service“. https://blog.newcloudnetworks.com/a-beginners-guide-to-security-as-a-service (pristupljeno velj. 04, 2021).

[17] „Five Elements of Cloud Security - SDxCentral .com“, *SDxCentral*. https://www.sdxcentral.com/cloud/definitions/five-security-aspects-of-cloud-computing/ (pristupljeno velj. 05, 2021).

[18] „What is Cloud Computing Security?“, *Sumo Logic*. https://www.sumologic.com/glossary/cloud-computing-security/ (pristupljeno velj. 05, 2021).

[19] J.Brodkin, „Gartner: Seven cloud-computing security risks“, 2008. [Na Internetu]. Dostupno: https://d1wqtxts1xzle7.cloudfront.net/34194686/consumer_risk.pdf [pristupano: 05.02.2021.].

[20] S. Verma, „History and Vision of Cloud Computing“, *Times of Cloud*, lis. 13, 2013. https://timesofcloud.com/cloud-tutorial/history-and-vision-of-cloud-computing/ (pristupljeno velj. 05, 2021).

[21] „Private Cloud“, *VMware*. https://www.vmware.com/topics/glossary/content/private-cloud (pristupljeno velj. 08, 2021).

[22] J. Fellows, „What is Private Cloud?“, *Liquid Web*, lis. 30, 2018. https://www.liquidweb.com/blog/private-cloud/ (pristupljeno velj. 08, 2021).

[23] „What is a Private Cloud and What are its Advantages?“, *SearchCloudComputing*. https://searchcloudcomputing.techtarget.com/definition/private-cloud (pristupljeno velj. 08, 2021).

[24] „What Is a Virtual Private Cloud (VPC)?“, *Cloudflare*. https://www.cloudflare.com/learning/cloud/what-is-a-virtual-private-cloud/ (pristupljeno velj. 08, 2021).

[25] „What Is a Private Cloud? | Private Cloud vs. Public Cloud“, *Cloudflare*. https://www.cloudflare.com/learning/cloud/what-is-a-private-cloud/ (pristupljeno velj. 08, 2021).

[26] „HostReady - Cloud Services and Solutions - Private Cloud“. https://hostreadysol.com/cloud-services/private-cloud (pristupljeno velj. 08, 2021).

[27] G. Kulkarni, J. Gambhir, T. Patil, i A. Dongare, „A security aspects in cloud computing“, lip. 2012, str. 547–550, doi: 10.1109/ICSESS.2012.6269525.

[28] „4. Data Security and Storage - Cloud Security and Privacy [Book]“. https://www.oreilly.com/library/view/cloud-security-and/9780596806453/ch04.html (pristupljeno velj. 09, 2021).

[29] „Data provenance“, *Diffblog*, tra. 21, 2020. https://blog.diffbot.com/knowledge-graph-glossary/data-provenance/ (pristupljeno velj. 09, 2021).

[30] „MOST SECURE Cloud Storage - 5 Safest Private Cloud to Stored Files“. https://www.goodcloudstorage.net/cloud-research/most-secure-cloud-storage-on-planet-earth/ (pristupljeno velj. 10, 2021).

[31] „Moving to the Cloud? How to Secure APIs on AWS, Azure, and GCP | Nordic APIs |“, *Nordic APIs*, svi. 28, 2020. https://nordicapis.com/moving-to-the-cloud-how-to-secure-apis-on-aws-azure-and-gcp/ (pristupljeno velj. 10, 2021).

[32] Adesh Kumar, „A Comparison of Security Challenges in Public and Private Clouds“, sv. 3, str. 396-402, siječanj 2014, doi: https://www.ijltet.org/wp-content/uploads/2015/08/631.pdf.

[33] G. Khera, „16 Open Source Cloud Storage Software for Linux in 2020“. https://www.tecmint.com/free-open-source-cloud-storage-tools-for-linux/ (pristupljeno velj. 11, 2021).

[34] „Nextcloud - ArchWiki“. https://wiki.archlinux.org/index.php/Nextcloud#Create_data_storage_directory (pristupljeno velj. 11, 2021).

[35] Nextcloud, „About“, *Nextcloud*. https://nextcloud.com/about (pristupljeno velj. 11, 2021).

[36] „Nextcloud“, *Wikipedia*. velj. 04, 2021, Pristupljeno: velj. 11, 2021. [Na internetu]. Dostupno na: https://en.wikipedia.org/w/index.php?title=Nextcloud&oldid=1004868860.

[37] „Product overview: ownCloud file sync and share“. https://owncloud.com/product/ (pristupljeno velj. 11, 2021).

[38] „Seafile - Open Source File Sync and Share Software“. https://www.seafile.com/en/home/ (pristupljeno velj. 11, 2021).

[39] „How to install the Seafile file and sync system on Ubuntu - TechRepublic“. https://www.techrepublic.com/article/how-to-install-the-seafile-file-and-sync-system-on-ubuntu/ (pristupljeno velj. 11, 2021).

[40] „How To Install and Configure Nextcloud on Ubuntu 20.04“, *DigitalOcean*. https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-nextcloud-on-ubuntu-20-04 (pristupljeno velj. 12, 2021).

[41] „What is Ransomware?“, *www.kaspersky.com*, sij. 13, 2021. https://www.kaspersky.com/resource-center/definitions/what-is-ransomware (pristupljeno velj. 15, 2021).

[42] „Penetration testing cloud-based apps: A step-by-step guide“. https://techbeacon.com/enterprise-it/pen-testing-cloud-based-apps-step-step-guide (pristupljeno velj. 16, 2021).

[43] „Penetration Testing your AWS environment - a CTO’s guide“. https://www.intruder.io/blog/penetration-testing-your-aws-environment-a-ctos-guide (pristupljeno velj. 16, 2021).

[44] „filerun - Overview“, *GitHub*. https://github.com/filerun (pristupljeno velj. 18, 2021).

[45] A. AB, „FileRun - Cloud Storage & File Backup for Photos, Docs & More“. https://filerun.com (pristupljeno velj. 18, 2021).

[46] „FileRun.com (@FileRun). / Twitter“, *Twitter*. https://twitter.com/FileRun (pristupljeno velj. 18, 2021).

[47] „Pydio“, *Pydio*. https://pydio.com/en (pristupljeno velj. 18, 2021).

[48] „Pydio“, *Wikipedia*. sij. 14, 2021, Pristupljeno: velj. 18, 2021. [Na internetu]. Dostupno na: https://en.wikipedia.org/w/index.php?title=Pydio&oldid=1000313437.

[49] „CVE-2017-5865 : The password reset functionality in ownCloud Server before 8.1.11, 8.2.x before 8.2.9, 9.0.x before 9.0.7, and 9.1.x bef“. https://www.cvedetails.com/cve/CVE-2017-5865/ (pristupljeno lip. 19, 2021).

[50] „Owncloud Owncloud : CVE security vulnerabilities, versions and detailed reports“. https://www.cvedetails.com/product/22262/Owncloud-Owncloud.html?vendor_id=11929 (pristupljeno lip. 20, 2021).

[51] „Nextcloud Nextcloud : CVE security vulnerabilities, versions and detailed reports“. https://www.cvedetails.com/product/34622/Nextcloud-Nextcloud.html?vendor_id=15913 (pristupljeno lip. 20, 2021).

[52] „CVE - CVE“. https://cve.mitre.org/ (pristupljeno lip. 20, 2021).

[53] „Pydio : Products and vulnerabilities“. https://www.cvedetails.com/vendor/15057/Pydio.html (pristupljeno lip. 20, 2021).

[54] „User Enumeration Explained: Techniques and Prevention Tips | Rapid7 Blog“, *Rapid7*, lip. 15, 2017. https://www.rapid7.com/blog/post/2017/06/15/about-user-enumeration/ (pristupljeno lip. 21, 2021).

[55] „11 Ways to Improve Your Web Application Security“, *Patchstack*, velj. 27, 2021. https://patchstack.com/web-application-security/ (pristupljeno lip. 21, 2021).

[56] „What is pen testing?“, *SearchSecurity*. https://searchsecurity.techtarget.com/definition/penetration-testing (pristupljeno lip. 21, 2021).

[57] „Best Penetration Testing Tools for 2021 | eSecurity Planet“, *eSecurityPlanet*, sij. 15, 2021. https://www.esecurityplanet.com/products/best-penetration-testing/ (pristupljeno lip. 21, 2021).

[58] „What is a Time-based One-time Password (TOTP)?“ https://www.twilio.com/docs/glossary/totp?utm_source=docs&utm_medium=social&utm_campaign=guides_tags (pristupljeno lip. 30, 2021).

Popis slika

Popis tablica