Komporativna analiza bežičnih pristupnih točaka u IoT okruženju

Bakrač, Sven

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

KOMPARATIVNA ANALIZA BEŽIČNIH PRISTUPNIH TOČAKA U IOT OKRUŽENJU

COMPARATIVE ANALYSIS OF WIRELESS ACCESS POINTS IN IOT ENVIRONMENT

Mentor: doc. dr. sc. Ivan Cvitić

Student: Sven Bakrač

JMBAG: 0135255099

Zagreb, lipanj 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 28. ožujka 2024.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Terminalni uređaji**

ZAVRŠNI ZADATAK br. 7537

Pristupnik: **Sven Bakrač (0135255099)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Komparativna analiza bežičnih pristupnih točaka u IoT okruženju**

Opis zadatka:

Završnim radom potrebno je prikazati i poisati arhitekturu koncepta IoT te pružiti pregled karakteristika komunikacijskih tehnologija primjenjivih u tom konceptu. Nadalje, potrebno je analizirati postojeće sustave za nadzor i upravljanje u IoT mreži te provesti usporednu analizu pristupnih točaka primjenjivih za povezivanje IoT uređaja.

Mentor:

doc. dr. sc. Ivan Cvitić

Predsjednik povjerenstva za završni ispit:

Sažetak

U ovom radu analizira se povezivanje pametnih uređaja na Internet. Na početku je objašnjena ideja IoT-a („Internet of Things“ eng.), kao i njene izvedbe i načini umrežavanja uređaja. Navedeno je nekoliko pametnih uređaja koji se koriste u svakodnevnici, te njihova funkcija u izvedbi IoT. Prikazani su različiti načini i izvedbe komunikacijskih tehnologija koje pametni uređaji koriste za međusoban rad. Objašnjena je funkcija nadzora u IoT mreži, te kako se njena sigurnost može poboljšati i osigurati. Analiziran je način rada bežičnih pristupnih točaka i njihove izvedbe. Posebni osvrt je dan na Cambium Networks i Aruba Networks pristupne točke.

Ključne riječi IoT, Cambium Networks, Aruba Networks, Pristupne točke

Abstract

This paper analyzes the connection of smart devices to the Internet. At the beginning, the idea of IoT (Internet of Things) was explained, as well as its implementation and ways of networking devices. Several smart devices used in everyday life and their function in IoT implementation are listed. Different methods and implementations of communication technologies used by smart devices for mutual work are presented. It explains the monitoring function in an IoT network and how its security can be improved and ensured. The mode of operation of wireless access points and their performance were analyzed. A special review is given to Cambium Networks and Aruba Networks access points.

Key words: IoT, Cambium Networks, Aruba Networks, Access points

SADRŽAJ

1 Uvod

Razvojem digitalnog svijeta, povećava se količina postojećih pametnih uređaja koji se spajaju na Internet. Svaki od tih uređaja ima opciju spajanja s drugim pametnim uređajima na mreži, te oni međusobno komuniciraju kako bi se poboljšao i maksimizirao njihov rad. Centralna uloga ovog koncepta je bežična pristupna točka koja im omogućuje međusobnu komunikaciju i povezivanje s drugim mrežama. Te će se u ovome radu analizirati i objasniti način rada bežičnih pristupnih točaka i njihove izvedbe kroz sljedeća poglavlja:

1. Uvod
2. Analiza koncepta IoT
3. Pregled karakteristika komunikacijskih tehnologija
4. Analiza postojećih sustava nadzora i upravljanja u IoT mreži
5. Komparativna analiza Cambium Networks i Aruba Networks pristupnih točaka
6. Zaključak

U drugom poglavlju će se objasniti ideja IoT-a („*Internet of Things*“ eng.), te također njene izvedbe i načini umrežavanja uređaja. Također će se proći nekoliko pametnih uređaja koji se koriste u svakodnevnici kao i njihova funkcija u izvedbi IoT.

Treće poglavlje prolazi kroz različite načine i izvedbe komunikacijskih tehnologija koje pametni uređaji koriste za međusoban rad.

Četvrto poglavlje opisuje i objašnjava funkciju nadzora u IoT mreži, te kako se njena sigurnost može poboljšati i osigurati.

Peto poglavlje analizira dvije bežične pristupne točke od različitih vodećih proizvođača u proizvodnji uređaja za mrežu.

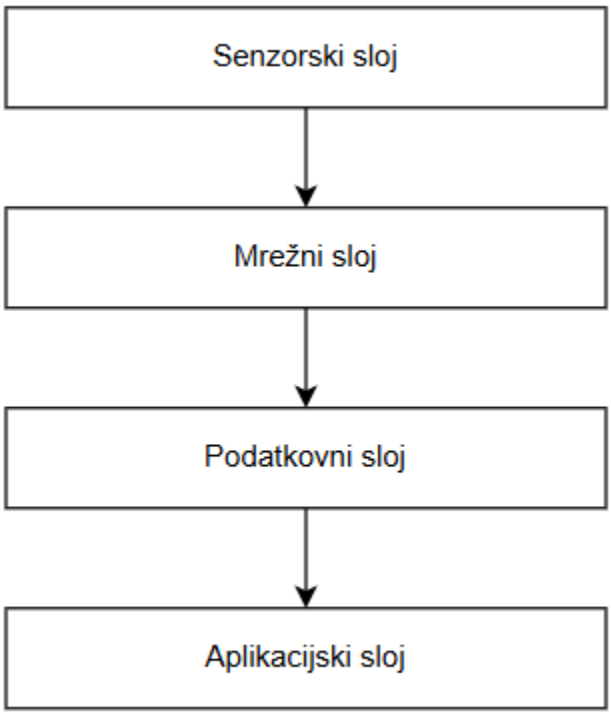
2 Arhitektura koncepta IoT

Internet of Things (IoT) predstavlja mrežu fizičkih uređaja, vozila, kućnih uređaja, te ostalih uređaja koji su opremljeni sa senzorima, softverima i mogućnostima povezivanja na postojeće mreže [1]. To su takozvani „pametni uređaji“, oni mogu varirati od najobičnijih uređaja koji se mogu naći u kućanstvima poput satova, perilica za rublje, termostata, itd., sve do kompleksnijih uređaja koji se koriste u raznim tvornicama za proizvodnju. IoT omogućuje pametnim uređajima međusobni rad i komunikaciju kako bi prikupljali podatke u stvarnome vremenu i odrađivali svoju ulogu u različitim „pametnim“ okruženjima.

Na primjer u „pametnim domovima“ se mogu kontrolirati svjetla putem interneta, na način gdje ih korisnik može upaliti ili ugasiti sa udaljenosti. Također postoje različiti senzori koje imaju uređaji poput senzora svjetlina, te se rasvjeta može sama upaliti ako je dovoljno tamno u prostoriji. Postoje i kompleksnije izvedbe „pametnih“ okruženja poput zdravstvene skrbi, gdje uređaji mogu javljati pacijentu ili doktoru trenutnu realnu situaciju u pacijentovom tijelu.

2.1. Slojevi arhitekture koncepta IoT-a

Kako bi IoT iskoristio svoj potpuni potencijal on se sastoji od različitih slojeva koji rade skupa kako bi se omogućila besprijekorna komunikacija i razmjena podataka. Slojevi od kojih se IoT sastoji su senzorski, mrežni, podatkovni i aplikacijski, te se to može vidjeti na slici broj 1.



Slika 1 Prikaz slojeva u IoT-u

Senzorski sloj je prvi sloj i odgovoran je za skupljanje podataka od različitih izvora. Sastoji se od senzora postavljenih u okolini koji skupljaju informacije o temperaturi, vlazi zraka, svjetlosti, zvuku i drugim fizičkim parametrima. Senzori pretvaraju fizičke veličine u digitalne signale koji se mogu prenijeti ili pohraniti u memoriju uređaja. Kroz bežične ili žične komunikacijske protokole su ovi uređaji povezani s mrežnim slojem. Učinkovitost senzorkog sloja igra ključnu ulogu u IoT okruženju. Pouzdanost i kvaliteta senzora ovisi o ispravnosti podataka koji će se koristiti za donošenje odluka i upravljanjem drugih uređaja. Naprimjer senzorski sloj bi koristio senzor svjetlosti za otkrivanje jačine prirodnog svjetla i ovisno o tome podešavao umjetnu rasvjetu, te na taj način štedio energiju. U poljoprivredi se koristi senzor vlage kako bi se kontrolirala vlaga zemljišta, te ovisno o tome može poslati podatke sustavu za navodnjavanje i osigurati zdravlje usjeva [2].

Mrežni sloj je zadužen za pružanje komunikacije i povezivanje uređaja u IoT sustavu. On uključuje razne protokole i tehnologije koje dozvoljavaju uređajima povezivanje i međusobnu komunikaciju. Mrežni sloj ima ključnu ulogu u prijenosu prikupljenih podataka od strane senzora do odredišta. Odgovoran je za uspostavu i održavanje komunikacije između uređaja u IoT-u. Svaki uređaj u mreži ima jedinstvenu IP adresu, koju onda koristi mrežni sloj za usmjeravanje podataka Koristi komunikacijske protokole poput TCP/IP ili posebne IoT protokole za pouzdano prenošenje podataka. Važnu ulogu igra za optimiziranje performansi IoT sustav. Sastoji se od pristupne točke i usmjerivača koji funkcioniraju kao posrednici između uređaja i Interneta. Mrežni sloj može uključivati sigurnosne značajke poput šifriranja i autentifikacije kako bi se zaštitilo od neovlaštenog pristupa [2].

Podatkovni sloj ima važnu ulogu u upravljanju i pripremi podataka koji su prikupljeni iz senzorskog sloja i prenose se mrežnim slojem. Podaci primljeni od senzora mogu biti u različitim formatima ovisno o tipu senzora. Ovaj sloj ima zadaću primanja sirovih podataka s uređaja, njihovu obradu, te činjenje tih podataka dostupnim za daljnju analizu ili akciju [2]. Podatkovni sloj može dodati meta podatke podacima prikupljenim iz senzora. Meta podaci su dodatne informacije koje opisuju podatke, poput lokacije i vremena prikupljanja informacija, te se na taj način poboljšava njegova korisnost. Važnu ulogu ima u zaštiti podataka od neovlaštenog pristupa. Osigurava da se podaci mogu što bolje prenositi, analizirati, pohranjivati i pretvoriti u korisne informacije za donošenje odluka.

Aplikacijski sloj je zadnji sloj, te je on zadužen za komunikaciju s krajnjim korisnikom, zadaća mu je pružiti korisničko sučelje i funkcionalnosti koje omogućuju korisnicima pristup i kontrolu nad IoT uređajima. On pretvara sirove podatke iz senzora u korisne informacije koje ljudi mogu razumjeti. Ovaj sloj uključuje različite softvere i aplikacije poput mobilnih aplikacija, web portala i drugih korisničkih sučelja koji su osmišljeni za interakciju s osnovnom IoT infrastrukturom [2]. Pruža alat za upravljanje IoT sustavom, uključujući dodavanje i uklanjanje uređaja i ažuriranje sustava. Aplikacija koja služi za upravljanje pametnim domom dozvoljava korisnicima da pregledaju temperaturu i vlažnost u svojoj kući, zaključavaju vrata i kontroliraju svjetlo, sve putem jednog uređaja. Kvalitetan aplikacijski sloj ima važnu ulogu u pružanju dobre i

jednostavne korištenosti IoT-a. Omogućuje korisnicima da razumiju podatke koje su uređaji prikupili i iskoriste ih za poboljšanje života.

2.2. Pregled elemenata koncepta IoT

Postoje različite komponente koje omogućuju kvalitetnu funkciju IoT-a. Te komponente su:

- uređaji,
- oblak,
- povezanost,
- sigurnost i
- korisnička sučelja.

Uređaji su fizički uređaji koji se sastoje od različitih senzora koji prikupljaju informacije iz okoline u trenutnom vremenu. Oni moraju biti sposobni za povezivanje na mrežu i za slanje prikupljenih podataka drugim uređajima. Jedan od primjera komunikacije tih uređaja je kada korisnik dođe blizu svojih ulaznih vrata, pametna brava bi to trebala prepoznati i otključati se sama bez potrebe za korisnikom. Također ona javlja drugim uređajima da su se vrata otključala te se upali rasvjeta, itd.

„Cloud“ ili računalstvo u oblaku je logičan izbor kada se govori o pohrani velike količine podataka koje generiraju IoT uređaji, a koje treba skladištiti, analizirati te osigurati da je usluga dostupna od svukuda i u bilo koje vrijeme [3]. Pruža skalabilnost jer kako broj uređaja raste oni generiraju sve više podataka, te je oblak odličan jer pruža gotov neograničene resurse. Omogućuje brzo i jednostavno ažuriranje i implementiranje IoT aplikacija. Oblak pruža sigurnosne mjere za zaštitu podataka od neovlaštenog pristupa i manipulacije. Platforme na oblaku omogućavaju administratorima lako provjeravanje statusa uređaja i upravljanje konfiguracijama, te centralizirano upravljanje uređajima. Oblak se može koristiti za pohranjivanje i analizu podataka o zdravlju prikupljenih nosivim uređajima. Ukratko, oblak pruža resurse i funkcionalnosti za upravljanje i dobivanje bitnih informacija iz ogromnih količina podataka koje generiraju IoT uređaji.

Povezivanje uređaja je ključna komponenta u IoT izvedbi koja omogućuje uređajima pravilnu i preciznu komunikaciju u realnom vremenu. Komunikacija mora biti precizna iz razloga kako se ne bi dostavile pogrešne informacije korisniku. Neke od najzastupljenijih komunikacijskih tehnologija u pametnim okruženjima su:

- RFID,
- Zigbee,
- Z-wave,
- Wi-Fi,
- NFC,
- LoRaWAN,

- Bluetooth,
- 5G i
- MiWi.

Postoje razni načini za povezivanje uređaja u IoT okruženju, te je izbor odgovarajuće metode ovisno o nekoliko faktora. Za izbor je bitna vrsta uređaja, poput pametnih telefona koji imaju ugrađene Wi-Fi ili Bluetooth komunikacijske tehnologije. Drugi uređaji poput industrijskih senzora, možda zahtijevaju specijalizirane protokole za komunikaciju na veće udaljenosti. Udaljenost komunikacije između uređaja će također utjecati na izbor komunikacijske tehnologije. Na primjer Bluetooth je dobar izbor za kratke domete, dok LoRaWAN može odlično raditi na velikim udaljenostima. Neki od uređaja u IoT-u imaju ograničenja u pogledu baterije, te je iz tog razloga potrebno odabrati tehnologiju s niskom potrošnjom energije.

Sigurnost u IoT izvedbi je od velike važnosti iz razloga što je sve veći broj uređaja povezanih na Internet. Iz tog razloga uređaji koji nemaju kvalitetnu sigurnost mogu postati laka meta za zlonamjerne aktere. U IoT-u je ključna visoka razina kvalitete sigurnosti, kako ne bi došlo do provala u domove ili krađe osobnih podataka od korisnika. Radi toga se sve više proizvođači pametnih uređaja baziraju na vrhunskoj sigurnosti i obrani. Neki od načina poboljšavanja sigurnosti [3]:

- autentifikacija ili autorizacija,
- segmentacija mreže,
- enkripcija,
- edukacija i
- procjena rizika.

Autentifikacija korisnika je osnovni način obrane, u kojoj se prilikom korištenja uređaja šalje korisniku poruka u kojoj on mora potvrditi svoj identitet. Poput SMS poruke s kodom koji mora upisati u aplikaciji. Enkripcija funkcionira na način gdje se informacije koje se šalju između uređaja „maskiraju“ kako bi se spriječilo presretanje i očitavanje osjetljivih informacija. Segmentacija mreže omogućuje sigurnost pojedinih dijelova mreže ukoliko dođe do kompromitacije jednog uređaja nisu svi ugroženi [3]. Edukacija korisnika omogućuje korisnicima učenje o važnosti sigurnosti uređaja, te kako se može u praksi smanjiti broj provala u IoT mreže. Procjene rizika mogu pomoći tvrtkama sa identifikacijom potencijalnih slabosti u mreži, te da na vrijeme poduzmu nešto kako bi se to osiguralo.

Korisnička sučelja omogućuju korisniku jednostavno korištenje i komunikaciju s IoT uređajima. Cilj korisničkih sučelja je što jednostavniji prikaz svega što se događa na mreži, te mogućnost pristupa svim uređajima s jedne mobilne aplikacije. Dobro dizajnirano sučelje omogućuje korisnicima lako upravljanje uređajima i razumijevanje podataka koje su prikupili. To čini IoT uređaje korisnijim i pristupačnijim za ljude s različitim tehničkim poznavanjima. Korisničko sučelje može prikazati podatke iz IoT uređaja na način koji dozvoljava korisnicima da donose bolje odluke. Na primjer, može prikazivati podatke o potrošnji energije u kući, omogućavajući korisnicima da identificiraju područja za uštedu. Većina IoT uređaja dolazi s vlastitom mobilnom aplikacijom koja se može instalirati na pametni mobitel ili tablet. Ona bi

trebala biti lako dostupna korisniku i jednostavna za korištenje. Na slici 2 se može vidjeti primjer jedne mobilne aplikacije za kontrolu pametnog doma. Također se na slici vidi i korištenje pametnog termostata, preko kojega se može kontrolirati željena temperatura u prostoru. Na slici se isto tako vidi da postoji pametni uređaj s ugrađenim senzorom koji šalje informaciju korisniku koliko se električne energije potrošilo u određenom vremenu ili koliko se kubika vode iskoristilo.

Slika 2 Primjer korisničkog sučelja na aplikaciji za kontrolu IoT-a [3]

U slučaju kad korisnik koristi pametni sat, moguće je instalirati aplikaciju putem koje se može pratiti situacija. Na nekim pametnim uređajima koji se koriste u IoT postoje tipke, te i oni predstavljaju korisničko sučelje koje omogućuje korisniku resetiranje uređaja i paljenje/gašenje.

2.3.Mogućnosti primjene koncepta IoT

IoT ima širok spektar primjene, te se koristi u različitim sektorima poput kućanstva, zdravstva, poljoprivrede, gradova, industrije i transporta. Revolucionira način na koji se integrira s našom okolinom. IoT nudi povišene efikasnosti i udobnosti do poboljšanja sigurnosti i upravljanja resursima.

2.3.1 Pametni domovi

Pametni domovi (*eng. Smart home*) koriste raznolike pametne uređaje kako bi olakšali svakodnevni život ukućanima. Korisnici često koriste termostate kako bi mogli regulirati temperaturu u domu. Također koriste nadzorne kamere kako bi mogli iz daljine gledati situaciju u kućanstvu, postoje kamere koje koriste senzor pokreta te se upale samo kada detektiraju nekakvo kretanje. Na taj način štede bateriju i omogućuju korisniku lakši pregled snimki. Postoje izvedbe u kojima nadzorna kamera javlja korisniku da se dogodio nekakav pomak u njegovom spektru gledanja, te da korisnik provjeri situaciju putem svoje aplikacije. Postoje i pametne žarulje koje se također mogu paliti ili gasiti putem aplikacije, te se mogu namještati jačine ovisno o tome kako korisnik želi. Pametni domovi mogu imati i kućne asistente koji omogućavaju korištenje govornih naredbi za kontrolu kućanskih uređaja. Primjer kućnog asistenta je „*Google Home*“ [4]. „*Google Home*“ dolazi sa svojom aplikacijom koja se može instalirati na pametni telefon ili tablet, te se putem nje mogu grupirati svi pametni uređaji u kućanstvu i mogu se putem nje koristiti. Kućni asistent reagira na glasovne naredbe, te putem ugrađenog zvučnika daje povratne informacije korisniku. Funkcionira na način da koristi „*Google*“ tražilicu i daje odgovore korisniku na njegova pitanja. Druga uloga koju ima je kontrola ostalih pametnih uređaja u domu također putem glasovnih naredbi.

2.3.2 Zdravstvo

Prije IoT-a pacijenti su bili limitirani na komunikaciju i preglede striktno na posjete liječniku uživo ili putem telefonskih poziva. Implementacijom IoT-a u zdravstvu smanjuje se potreba dolazaka pacijenta liječniku, te se omogućuje njegova kontrola putem pametnih uređaja spojenih na pacijenta [5]. Taj način omogućuje liječnicima i samim pacijentima bolju kontrolu nad pacijentima i pravovremeno reagiranje ovisno o situaciji pacijenta. Također implementacija IoT-a smanjuje gužve i ostajanje pacijenata u duljim periodima u bolnicama.

Postoje različiti uređaji za kontrolu pacijenta poput pametnih narukvica koje mjere krvni tlak i otkucaje srca u različitim periodima dana i pod različitim fizičkim naporima. Koriste se i pametni satovi koji javljaju korisniku razne informacije poput brojanja koraka i trošenja kalorija u danu. Također omogućuju korisniku obavijesti vezane uz redovito uzimanje lijekova koje im je liječnik prepisao. Omogućeno je i slanje obavijesti drugim članovima obitelji ili bliskim prijateljima o pacijentovoj situaciji ukoliko mu je potrebna pomoć, što je svakako dobra ideja kada se radi o starijim i nemoćnim osobama [5].

IoT se koristi i u bolnicama. Osim što može pratiti zdravlje pacijenta, također služi za kontrolu uređaja koji se koriste u zdravstvu. Dojavljuje trenutnu poziciju u stvarnom vremenu o lokaciji medicinskih uređaja, te korisnika obavještava o potrebnim servisima. Postoje različiti pametni uređaji s ugrađenim senzorima koji prate ukoliko dođe do širenja neke infekcije u prostorima bolnice, kako bi se mogli pacijenti prebaciti na sigurnu lokaciju [5]. IoT je rasprostranjen i u farmaciji, gdje dojavljuje ljekarnicima o lokaciji različitih lijekova i temperaturi hladnjaka koji čuvaju lijekove na određenim potrebnim temperaturama.

2.3.3 Poljoprivreda

IoT u poljoprivredi fokusiran je na pomaganje poljoprivrednicima što se tiče zadovoljavanja potražnje građana, na način kako bi se osigurala optimalna primjena resursa za postizanje visokih prinosa usjeva i smanjenje operativnih troškova. Omogućuje im kontrolu njihovih polja ili vinograda s velike udaljenosti, te im dojavljuje situaciju s usjevima. Postoje i dronovi koji pomažu poljoprivrednicima u kontroli vinograda. U Svetom Križu Začretju se koriste dronovi za špricanje i kontrolu vinograda. Rade na principu u kojem se koriste dva drona, jedan manji dron služi za „izviđanje“ i dojavljivanje situacije u vinogradu, dok se drugi veći dron koristi za prskanje i gnojidbu. Veći dron sa sobom nosi spremnik od 30 litara [7]

Služi i u optimizaciji iskorištenja vode, umjesto tradicionalnog navodnjavanja po rasporedu, senzori u IoT-u mogu precizno odrediti potrebe biljaka. Na taj način se omogućava poljoprivrednicima da automatski aktiviraju navodnjavanje samo kada je potrebno, tako se štedi i voda i novac. Također se može koristiti za rješavanje različitih zadataka na farmi, poput hranjenja životinja ili upravljanja stajama. Tako se pojednostavljuje poljoprivrednicima da se mogu fokusirati na druge važne zadatke i poboljšava se efikasnost rada. Svi ti načini korištenja IoT-a u poljoprivredi pomaže poljoprivrednicima da povećaju prinos i profitabilnost svog gospodarstva. Također s druge strane postoje razni izazovi, kao što su troškovi implementacije i potrebe za digitalnim znanjem.

2.3.4 Pametni gradovi

Pojam pametnog grada se u literaturi često navodi kao sposobnost grada da na efikasan način, u što bržem vremenu udovolji raznim potrebama građana [8]. Pametni gradovi omogućuju građanima poboljšanu kvalitetu života putem digitalnih tehnologija. Funkcioniraju na način da doprinose poboljšanju okoliša, uštedi troškova za svoje građane, poboljšanju komunikacije s građanima i optimiziranju javne usluge. Kako bi grad postao pametni grad mora imati najmanje pet od šest navedenih elemenata [8]:

- pametno upravljanje,
- pametno društvo,
- pametnu brigu za ljude i okoliš,
- pametnu infrastrukturu i mobilnost,
- pametne tehnologije i energije i
- pametne građevine.

Ideja pametnog grada je optimizacija gradske funkcije i promocija ekonomskog rasta dok se također poboljšava kvaliteta života građana. Uspjeh se oslanja na odnos između javnih i privatnih sektora, na način gdje se implementiraju pametne kamere koje prate i kontroliraju promet na cestama. Ključan je odnos javnih i privatnih sektora u ovoj situaciji, iz razloga što privatna tvrtka izrađuje i postavlja kamere, a javni sektor grada ga kontrolira i provjerava [8]. Upravljanje prometom u pametnom gradu se bazira na tome da senzori i kamere prate stanje na prometnicama u stvarnom vremenu, te pomažu u optimizaciji semaforskih regulacija kako bi se izbjeglo stvaranje gužvi. Postoje i solucije gdje javljaju vozačima situaciju na prometnicama i predlažu im alternativne rute kroz grad. Koriste se i pametne rasvjete u kojima svjetiljke na ulicama imaju

ugrađene senzore te se mogu prilagoditi uvjetima okoline. Ukoliko dođe do ranijeg smračivanja u gradovima nego je očekivano mogu se upaliti kako bi građani imali pravovremenu rasvjetu. Pametna rasvjeta omogućuje smanjenje potrošnje električne energije i građanima povećava sigurnost kretanja kroz grad. Pametni gradovi koriste i e-upravu, koja implementira digitalizaciju javnih usluga građanima te im omogućuje jednostavnije i brže rješavanje administrativnih zadataka [8]. Upravljanje otpadom je isto jedan od alternativnih izvedba u kojima se koriste pametni kontejneri za otpad koji mogu signalizirati kada su puni, te na taj način optimizirati rute sakupljanja otpada i tako poboljšati čistoću grada.

2.3.5 Industrija

Industrija koja koristi IoT u svojoj izvedbi se naziva Industrija 4.0, u kojoj se događa suradnja između ljudi i uređaja [9]. Omogućuje povećanu učinkovitost, fleksibilnost, smanjenje proizvodnih troškova, prilagodljivost tržišnim potrebama i brže donošenje odluka. Naprave dolaze s ugrađenim senzorima koji očitavaju njihove performanse i vanjske uvjete. Na taj način olakšavaju radnicima kontrolu uređaja, odnosno pravovremeni servis istih. Informacije koje uređaji šalju radnicima im omogućuju njihovu optimizaciju kako bi mogli uštedjeti na određenim troškovima. Također im dozvoljava uvid u način rada uređaja u stvarnome vremenu, kako uređaj ne bi radio nešto pogrešno, odnosno kako bi se eventualni kvar mogao popraviti.

Industrija 4.0 dozvoljava radnicima lakši pregled robe koja postoji u skladištima. Roba je označena sa senzorima koji šalju podatke o svojoj trenutnoj lokaciji. Na taj način se smanjuje vremenska potreba za potražnjom u skladištu, odnosno rad postaje efikasniji. IoT u industriji pomaže i na način da inženjeri koji su zaduženi za kontrolu uređaja mogu kontrolirati naprave s određenih udaljenosti. To je svakako poželjno ukoliko se radi o tome da jedan inženjer mora kontrolirati više uređaja koji se ne nalaze u istom skladištu. Postoje i senzori koji su postavljeni na određene dijelove skladišta kako bi pratili uvjete zraka, kako ne bi npr. došlo do curenja plinova. Odnosno ako je već došlo do curenja, kako bi se isto moglo zaustaviti na vrijeme[9].

2.3.6 Transport i logistika

Korištenje IoT-a u transportu, uvelike poboljšava proces slanja proizvoda od vlastitih skladišta do dućana pa i do krajnjih korisnika. Logistička industrija je koristila povezane ekosustave i prije dolaska pojma IoT. Razlog iza toga je taj što je omogućavao praćenje dostavnih vozila i nadzor procesa dostave, osiguravajući dostavu na vrijeme na određene lokacije [10]. IoT senzori mogu pomoći u otkrivanju problema s vozilom, poput pregrijavanja motora ili nenormalnog tlaka u gumama te na taj način omogućiti preventivno održavanje i smanjujući rizik od kvarova na cesti.

IoT u transportu omogućuje poslodavcima nadzor nad cijelom flotom vozila za dostavu u stvarnom vremenu, te dobivanje upozorenja o dolazećim nevremenima ili nesrećama na prometnicama kako bi se mogli zaobići. Također se IoT koristi i u skladištima kako bi se izbjegao gubitak dobara, te poboljšala sigurnost skladištenja istih. Korištenje IoT-a u pametnim skladištima omogućuje radnicima lakši pregled robe, te njihov brži pronalazak. Roba je označena sa senzorima koji dojavljuju radnicima trenutnu lokaciju i njihovo stanje ukoliko predmet mora biti čuvan u određenim uvjetima [10]. Pametna skladišta smanjuju greške u rukovanju s robom i poboljšavaju produktivnost zaposlenika. Isto tako se IoT može iskoristiti u javnom prijevozu za praćenje

autobusa, tramvaja i vozila u realnom vremenu. To dozvoljava putnicima da vide kada će doći sljedeće vozilo i planiraju svoje putovanje u skladu s time. Uređaji sa senzorima se mogu postaviti na parkirališta kako bi se moglo dojaviti korisnicima je li parkirno mjesto prazno ili zauzeto. Te informacije se mogu prikazati vozačima na pametnim telefonima, što im omogućava lakše pronalaženje parkirnog mjesta.

3 Pregled karakteristika komunikacijskih tehnologija

Komunikacijske tehnologije igraju veliku ulogu u izvedbi IoT-a, jer je ključ komunikacija dva ili više uređaja kako bi se iskoristio puni potencijal pametnih uređaja. IoT uređaji komuniciraju na različite načine koristeći stotine različitih protokola. Razlog tomu je što se način komunikacije mijenja ovisno o vrsti uređaja, njegovom položaju, s kojim drugim uređajima i sustavima se spaja te o sadržaju komunikacije [11]. Svaki uređaj u IoT okruženju mora biti sposoban komunicirati, bilo da samo šalje podatke ili da šalje i prima. Postoji žična i bežična komunikacija među uređajima.

Komunikacijske tehnologije se sastoje od više koraka:

1. kodiranje
2. modulacija
3. prijenos
4. demodulacija
5. dekodiranje

Kodiranje je prvi korak u procesu prijenosa informacije te se u njemu informacija transformira u tip podatka povoljan za prijenos (niz bitova). Modulacija je postupak „utiskivanja“ te iste informacije na elektromagnetski val. Prijenos, kao što i sam naziv govori je postupak odašiljanja informacije. Demodulacija je korak u kojemu demodulator na prijemnoj strani demodulira modulirani val te iz njega izdvaja digitalne podatke. Dekodiranje je zadnji dio procesa slanja i zaprimanja informacije u kojemu se digitalni podaci dekodiraju u svoj izvorni format (npr. zvuk, video, tekst).

Žična komunikacijska tehnologija se oslanja na fizičku povezanost dva ili više uređaja kako bi mogla biti uspostavljena komunikacija. Samim time je sigurnija, brža i pouzdanija od bežične komunikacije. S druge strane je manje fleksibilna od bežične, jer je glavni faktor ograničenosti duljina žice. Postoje analogna i digitalna žična komunikacija. U analognoj signal poruke se kontinuirano mijenja o vremenu. Ova metoda se koristi kada se prenosi kontinuirani signal, kao što su glasovni signali ili video signali. Analogna metoda je jednostavna za implementirati, dobra je za prijenos kontinuiranih signala. Široko je rasprostranjena i kompatibilna je s postojećom infrastrukturom. S druge strane ima i nedostatke poput:

- ograničena propusnost podataka,
- podložnost slabljenju signala na većim udaljenostima i
- osjetljivost na šum i interferencije.

Digitalna žična komunikacija funkcionira na principu gdje se signal poruke pretvara u niz bitova koji se onda prenose kroz žicu. Ova metoda je idealna kada je u pitanju prijenos digitalnih podataka kao što su računalni podaci ili promet koji se događa na internetu. Otporna na šum i različite interferencije, te omogućuje prijenos velikih količina digitalnih informacija. Nedostatci koje ima su:

- kompleksnija i skuplja implementacija u usporedbi s analognom,
- potrebna je konverzija signala iz analognog u digitalni signal i obrnuto i
- ograničena je dostupnost u usporedbi s analognom infrastrukturom.

Koriste se bakrena parica, koaksijalni kabel ili optičko vlakno. Bakrena parica se koristi za telefonske linije, internetske veze i kabelske televizije. Optičko vlakno se sastoji od tanke staklene niti koja koristi svjetlost za prijenos podataka, koristi se za internetske veze velike udaljenosti, podatkovne centre i medicinske slike. Žična komunikacijska tehnologija je osnova moderne komunikacije, nudi efikasan i pouzdan načina prijenosa podataka i signala. Napredak digitalnih tehnologija i optičkih vlakana doveo je do značajnog poboljšanja propusnosti i dometa, što ovu tehnologiju čini ključnom za današnju digitalnu infrastrukturu.

Bežična komunikacijska tehnologija omogućava izmjenu informacija dva ili više uređaja bez korištenja žice. To je moguće radi toga što se koriste elektromagnetski valovi za prijenos informacija. Ova metoda omogućava korištenje uređaja i komunikaciju u pokretu. Bežična tehnologija može pružiti komunikaciju u područjima gdje je postavljanje kablova nepraktično ili nemoguće. Lagano se mreža može širiti dodavanjem novih uređaja, što je odlično rješenje za rastuće potrebe mreže. Bežična komunikacija je osjetljiva na prisluškivanje i neovlašteno korištenje u usporedbi sa žičnim vezama. Također mogu biti ometane drugim elektronskim uređajima ili prirodnim fenomenima, te zbog toga može dovesti do smanjenja performansi ili gubitka veze. Domet bežičnih signala ovisi o tehnologiji i snazi odašiljača. Glavna razlika između žične i bežične komunikacije je medij prijenosa. Postoje tri tipa elektromagnetskih valova:

- radio valovi (najčešći tip, mobilni telefoni, Wi-Fi, Bluetooth),
- mikrovalovi (bežične veze velike udaljenosti, satelitske veze) i
- infracrveni valovi (kratko dometne bežične veze poput TV daljinskog upravljača).

Najčešća izvedba spajanja pametnog uređaja na internet je putem Wi-Fi. Wi-Fi je bežična tehnologija koja se koristi za spajanje računala, pametnih telefona i drugih takvih uređaja na Internet [12]. To je ustvari radio signal poslan od strane bežičnog usmjerivača do uređaja u blizini, te on prevodi taj signal u podatke koji se mogu vidjeti i koristiti. Pametni uređaj šalje radio signal nazad usmjerivaču, koji je povezan na internet putem kabela ili bežično. Ključan faktor kod Wi-Fi izvedba je to što funkcioniraju na određenom području ovisno o specifikacijama vlastite bežične točke.

Druga izvedba spajanja pametnih uređaja je putem mobilne mreže. Ukoliko uređaj nije spojen na Wi-Fi, a ima dogovorenu tarifnu opciju spajanja na internet prebacuje se na vlastitu mobilnu mrežu koja mu je dostupna putem njegovog mobilnog operatera. Wi-Fi i mobilna mreža funkcioniraju na način da se spajaju bežično na internet. U ovom slučaju gdje korisnik koristi vlastitu mobilnu mrežu mobilni uređaj se povezuje s mobilnom baznom stanicom koja je dio mreže koja pokriva veliko geografsko područje. Funkcionira na način da bazna stanica odašilje signal putem radio frekvencija uređaju. Trenutno aktivna mobilna mreža se naziva 5G (peta generacija celularne tehnologije), ona se temelji na 4G LTE (eng. *Long Term Evolution*), ali koriste sustav malih stanica umjesto velikih mobilnih tornjeva. Iz razloga kako bi podržale porast povezanih

uređaja te proširile pokrivenost i brzinu. Druge prednosti 5G-a uključuju niska kašnjenja i mogućnost komunikacije u stvarnom vremenu [13].

3.1. RFID

Radio Frekvencijska Identifikacija je bežična i beskontaktna tehnologija koja koristi radio frekvenciju kako bi se razmjenjivale informacije između prijenosnih uređaja i glavnog računala [14]. RFID tehnologija je komercijalno postala dostupna 1970-tih, te se danas može pronaći u ključevima od automobila, identifikacijskim iskaznicama zaposlenika, ENC-u i mnogim drugima.

RFID se sastoji od sljedećih elementa:

- RFID oznaka ili pametna naljepnica,
- RFID čitač i
- RFID antena.

Oznake uključuju antenu i integrirani krug koji omogućuju slanje podataka prema RFID čitaču. Taj čitač zatim radio valove transformira u upotrebljiva oblik podataka. Prikupljeni podaci s oznake se potom šalju glavnom računalnom sustavu putem komunikacijskog sučelja, gdje se mogu spremiti za kasniju analizu u bazi podataka. RFID omogućava beskontaktno i automatsko čitanje podataka, što je brže i preciznije od ručnog skeniranja barkodova. Oznaka koju koristi RFID je otporna na nečistoću, prašinu i oštećenja, dok s druge strane barkodovi se mogu oštetiti. Implementacija RFID sistema može biti dosta skuplja od tradicionalnog rješenja kao što je barkod, te domet varira ovisno i tehnologiji i može biti ograničen [14].

3.2. Bluetooth

Bluetooth je standardizirana tehnologija za bežičnu komunikaciju glasa i podataka na bliskim udaljenostima. To je tehnologija WPAN (eng. *Wireless Personal Area Network*) i primarni zadatak joj je prijenos informacija na kraćim udaljenostima. Djeluje u nelicenciranom frekvencijskom pojasu od 2,4 GHz do 2,485 GHz [15]. Domet mu je do 10 metara, te pruža brzine do 1 Mbps ili 3 Mbps, ovisno o verziji. Bluetooth koristi načelo prenošenja i primanja podataka pomoću radio valova. Također se može upariti samo s drugim uređajima koji imaju Bluetooth, ali mora biti unutar određenog komunikacijskog dometa kako bi se mogao povezati. Da bi se moglo izvesti povezivanje putem Bluetooth-a uređaj koji inicira komunikaciju treba aktivirati Bluetooth, čime signalizira susjednim uređajima da je spreman za povezivanje. Ostali uređaji, koji žele uspostaviti vezu, moraju također aktivirati Bluetooth i zatim skenirati okolinu kako bi detektirali i povezali se s željenim uređajem. Prednosti Bluetooth tehnologije su:

- bežična tehnologija,
- niska potrošnja energije i
- široka kompatibilnost.

3.3. Zigbee

Zigbee je isto poput Bluetooth-a tehnologija WPAN-a. On je tehnološki standard stvoren za kontrolu i detekciju mreže. Zigbee je otvoreni, globalni protokol temeljen na paketima dizajniran da pruži jednostavnu arhitekturu za sigurne, pouzdane, mreže s niskom potrošnjom energije[16]. To je standard koji se bavi potrebom za nisko troškovnom implementacijom uređaja s niskom potrošnjom energije, niskim brzinama prijenosa podataka za bežične komunikacije kratkog dometa.

Specifikacije koje Zigbee posjeduje su:

- niska potrošnja energije,
- male brzine prijenosa (20-250 kbps),
- male udaljenosti (<100 metara),
- lagana implementacija i
- mesh sustav.

Za razliku od Bluetooth-a Zigbee posjeduje niže brzine prijenosa, ali omogućuje veći domet po nižoj potrošnji energije. Iz tog razloga se često može naći u pametnim uređajima koji se koriste u IoT-u. Pametni uređaji manjih dimenzija često nemaju baterije velikih kapaciteta, te im iz tog razloga više odgovara implementacija Zigbee tehnologije za komunikaciju, kako bi produljili životni vijek baterija. Zigbee koristi Mesh sustav umrežavanja koji omogućuje uređajima međusobnu komunikaciju bez potrebe za centralnim Hub-om ili usmjerivačem. To je idealno za kućne uređaje koji moraju komunicirati međusobno, ali isto tako sa središnjim Hub-om[16].

3.4. Z-Wave

Bežična komunikacijska platforma, fokusirana na integraciju i upravljanje IoT uređajima unutar kućanstava. Glavna karakteristika ove tehnologije je njena P2P topologija, koja omogućuje daljinsko upravljanje uređajima poput svjetla, alarma, prozora i termostata. Pristup Z-Wave mreži omogućen je putem bežičnih ključeva, pametnih uređaja ili fiksnih tipkovnica. U uvjetima slobodnog prostora, udaljenost koju može pokriti je 30 metara. Specijalizira se za uređaje kojima je potrebno mali prijenos podataka. Z-Wave uređaji funkcioniraju tako da formiraju mrežu u obliku mreže, što bi značilo da svaki uređaj može djelovati kao repetitor signala te na taj način proširuje domet ukupne mreže i povećavajući njenu pouzdanost. Također je dizajnirana tehnologija za nisku potrošnju energije, što omogućava uređajima da rade duže na baterije. Ima visoku sigurnost iz razloga što koristi napredne metode šifriranja za zaštitu komunikacije i sprječavanja neovlaštenog pristupa [17].

3.5. LoRaWAN bežična tehnologija

Specifikacija LoRaWAN (eng. *Low Power Wide Area Network*) je protokol za umrežavanje s niskom potrošnjom energije i širokim područjem djelovanja osmišljen kako bi bežično povezivao uređaje napajane baterijama s internetom na regionalnim, nacionalnim ili globalnim mrežama[18]. Cilj joj je odraditi ključne zahtjeve IoT-a poput sigurnosti, dvosmjerne komunikacije i usluge

lokacije. LoRaWAN uređaji su smišljeni kako bi koristili što manje električne energije, te ih to čini odličnima za IoT koncept. To znači da jedan uređaj može godinama izdržati na jednoj bateriji. Također kako LoRaWAN može pokriti velike udaljenosti predstavlja odličan izbor za uređaje koji se koriste u pametnim gradovima, poljoprivredi ili čak praćenju divljih životinja. Sigurnost LoRaWAN-a uključuje *„end-to-end"* šifriranje, osiguravajući da podaci ostaju privatni i zaštićeni dok se prenose kroz mrežu[18].

3.6. Osnovne značajke 5G tehnologije

Bežična tehnologija 5G predstavlja petu generaciju mobilnih mreža i donosi značajne napretke. Tehnologija 5G omogućuje još veće brzine od prethodne 4G LTE tehnologije. Korištenjem manjih ćelija za povezivanje uređaja na Internet mrežu, umjesto klasičnih ćelijskih tornjeva. Tehnologija koja omogućuje veće brzine prijenosa u 5G je MIMO (eng. *Multiple input, multiple output*), ona dozvoljava primanje većeg broja podataka odjednom, te iz tog razloga uređaji istovremeno mogu dobivati potrebne podatke [19].

Prije 5G bežične tehnologije su postojale druge generacije:

- 1G (glasovni pozivi putem mobilnih telefoni),
- 2G (mogućnost slanja poruka putem mobilnog telefona (SMS)),
- 3G (mobilni telefoni se mogu povezati na Internet mrežu) i
- 4G (omogućuje veće brzine od prethodne).

Danas se testiraju autonomna vozila, koja funkcioniraju na 5G bežičnoj tehnologiji. Njegova niska latencija, brzina i pouzdanost mogu omogućiti nove razine efikasnosti, sigurnosti i udobnosti za vozače i putnike. Tehnologija 5G omogućuje autonomnim vozilima da primaju ažuriranje softvera i karte u realnom vremenu, te brzina ima veliki faktor jer omogućuje vozilu donošene brzih odluka ovisno u situaciji u vožnji [20]. Može povezati puno više uređaja po jedinici površine nego 4G, što je ključno za razvoj IoT-a i aplikacija s velikim brojem korisnika. Odlična tehnologija za razvoj pametnih gradova, industrijske automatizacije i drugih IoT aplikacija.

Izazovi koji se pojavljuju kod 5G tehnologije su:

- pokrivenost,
- sigurnost i
- trošak.

Pokrivenost je trenutno ograničena, naročito u ruralnim područjima, milimetarski valovi koji omogućuju velike brzine imaju ograničen doseg te prodiru loše kroz zgrade i druge objekte. Sigurnost je također jedan od glavnih izazova radi toga što su 5G mreže još uvijek nove i postoje potencijalne sigurnosne ranjivosti. Razvoj i implementacija 5G mreže je skupa. Zahtjeva nove infrastrukture poput baznih stanica kao i troškove razvoja i implementacije nove tehnologije. Visoki troškovi za telekom operatere znači da ih oni mogu prebaciti na korisnike kroz više cijene tarifnih paketa.

3.7. MiWi

Bežični protokol MiWi je razvijen od strane Microchip Technology, on dozvoljava komunikaciju uređaja u IoT okruženju s niskom potrošnjom energije. Koristi standard IEEE 802.15.4 za fizički sloj [21]. Razvijen je za uređaje s baterijskim napajanjem i optimizira prijenos podataka kako bi se produljio životni vijek baterije. Pruža doseg komunikacije od 20 do 100 metara, ovisno o okruženju i uređaju. Podržava *„peer-to-peer“* i zvjezdaste mrežne topologije, što dozvoljava fleksibilnu implementaciju za različite IoT aplikacije [21].

Prednosti koje donosi MiWi protokol su:

- niska cijena,
- jednostavnost i
- niska potrošnja energije.

MiWi protokoli se najčešće koriste u pametnim domovima, industrijskoj automatizaciji i nadzoru, bežičnim senzorima i također u aplikacijama za daljinsko upravljanje.

4 Analiza postojećih sustava nadzora i upravljanje u IoT mreži

Sustavi za nadzor i upravljanje IoT mrežom se odnose na skup alata, tehnika i procesa kojima se omogućuje efikasno vođenje, kontrola i održavanje uređaja unutar IoT ekosustava. Upravljanje uređajima u IoT okruženju uključuje daljinsko registriranje, konfiguriranje, pružanje, održavanje i nadzor povezanih uređaja s centralizirane platforme kojoj IT administratori mogu pristupiti putem internetske veze s bilo kojeg mjesta na bilo kojem uređaju[21]. Alati za upravljanje dozvoljavaju organizacijama bolji nadzor i kontrolu nad svojim mobilnim uređajima. Svaki veći pružatelj usluga u oblaku, npr. „*Amazon Web Services*“, „*Google Cloud*“ i „*Microsoft Azure*“, uključuje upravljanje IoT uređajima u svoju ponudu[22].

Sustavi za upravljanje i nadzor uređaja u IoT okruženju uključuju sljedeće procese:

- registriranje uređaja,
- autentifikaciju,
- konfiguraciju,
- održavanje,
- dijagnostiku i
- kraj životnog vijeka.

Registriranje uređaja se odnosi na povezivanje pametnog uređaja s platformom zaduženom za upravljanje i nadzor, prije nego što se omogući razmjena podataka.

Autentifikacija sporazumijeva potvrđivanje identiteta uređaja prije nego što se može dodati u sustav nadzora. To omogućuje korisniku da samo autorizirani uređaji se mogu naći u mreži i razmjenjivati osjetljive podatke međusobno, te na taj način smanjiti rizik od krađe podataka [22].

Konfiguracija uređaja je proces personalizacije funkcionalnosti koje pruža IoT uređaj. Na primjer korisnici mogu optimizirati značajke svojih uređaja s dodatnim kodom, revidirati postavke svojih uređaja za nove zahtjeve ili dodati dodatnu inteligenciju svojim uređajima [22].

Održavanje označava funkciju u sustava upravljanja povezanu za time da održava uređaje na najnovijim opcijama dostupnih, poput ažuriranja softvera kada je moguće.

Kraj životnog vijeka je proces koji se odnosi na to da kada pojedinačni uređaji zastare ili IoT projekti budu gotovi, da sigurno i isplativo stavi te iste uređaje izvan pogona. Organizacije mogu zadržati podatke o uređajima ako namjeravaju zamijeniti povučene fizičke uređaje ili arhivirati podatke ako trajno povlače uređaje i upotrebe [22].

4.1. Prednosti sustava za upravljanje i nadzor IoT

Sustavi za upravljanje i nadzor IoT-a postaju sve neophodnije za nadzor i kontrolu rastućem broju IoT uređaja u raznim industrijama. Ključne prednosti koje sustavi za upravljanje i nadzor omogućuju su:

- jednostavni proces ažuriranje uređaja,
- strogo osiguranje,
- brza registracija uređaja i
- lakši nadzor udaljenih uređaja.

Sustavi za upravljanje i nadzor dozvoljavaju IT administratorima efektivno ažuriranje većeg broja uređaja odjednom. Također ne samo što uštedi puno vremena, nego i osigurava brzo, efektivno i precizno slanje i primanje ključnih informacija od drugih uređaja [22].

Strogo osiguranje dozvoljava organizacijama osigurati svoje podatke implementacijom enkripcijom podataka i segmentacijom. Softver omogućuje administratorima upravljanje, nadogradnju i ažuriranje pristupa određenim uređajima ili grupama uređaja, osiguravajući da su uređaji i podaci uvijek sigurni [22].

Upravljanje IoT uređajima putem sustava za upravljanje i nadzor nudi alate koje tvrtkama omogućuju brži razvoj, konfiguraciju i implementaciju povezanih uređaja, omogućujući im da odmah stave cijele mreže u rad [22].

Također omogućuje lakši nadzor uređaja na terenu. Dozvoljava administratorima daljinsko ažuriranje, kao i ponovno pokretanje, sigurnosne zakrpe i vraćanje na tvorničke postavke na čitavoj floti IoT uređaja. Nadalje, upravljanje IoT uređajima daje administratorima mogućnost daljinske intervencije, dijagnostike i rješavanje izazova s kojima se određeni uređaji mogu suočiti [22].

4.2. Izazovi u sustavima za upravljanje i nadzor IoT

Sustavi za upravljanje i nadzor IoT-a donose niz prednosti, ali s druge strane suočavaju se s brojnim izazovima koji otežavaju njihovo korištenje i implementaciju. Glavni izazovi sustava za upravljanje i nadzor su:

- kontrola pristupa,
- proliferacija uređaja i
- fragmentirani podaci.

Problem kod kontrole pristupa je to što često IoT uređaji nisu osigurani i nisu zaštićeni lozinkom, što ih čini lakim metama kibernetičkih kriminalaca. Kako bi osigurali zaštitu uređaja, kao i osjetljivih korporativnih i korisničkih podataka, tvrtke moraju kontrolirati tko pristupa njihovim uređajima i podacima [22].

Osim izazova upravljanja velikim brojem IoT uređaja, nagli porast tih uređaja može opteretiti mrežu zbog povećanja potražnje za propusnošću, što može dovesti do zagušena mreže i

prekida u radu. Softver za upravljanje IoT uređajima obično sadrži funkcionalnosti koje omogućavaju tvrtkama da automatiziraju i centraliziraju operacije uređaja [22].

Kako sve više IoT uređaja dolazi na mrežu, tvrtkama može biti izazovno upravljati količinom i raznolikošću podataka koje generiraju budući da je većina njih nestrukturirana i nije ih lako koristiti [22]. Alati za upravljanje IoT uređajima mogu prikupljati, organizirati i analizirati te podatke

4.3. Primjeri sustava za nadzor i upravljanje IoT mrežom

Tvrtka Amazon ima nudi vlastiti sustav za nadzor, upravljanje i organizaciju IoT okruženja pod nazivom AWS Iot Device Management. Omogućuje korisniku praćenje i povezivanje uređaja u oblaku s AWS IoT Device Defender-om za provjeru i praćenje sigurnosne pozicije uređaja. Idealan je za tvrtke sa velikim broj IoT uređaja koje traže efikasan i centraliziran način za njihovo upravljanje. Dozvoljava korisnicima upravljanje svim svojim uređajima iz jednog centralnog uređaja. Dozvoljava administratoru indeksiranje uređaja za brzo pretraživanje i organiziranje. Svaki uređaj ima svoj digitalni prikaz koji omogućava interakciju i praćenje stanja uređaja čak i kada nije povezan, a to se naziva *„Device Shadow“*. Također sustav ima opciju pokretanja operacija na grupama uređaja poput ažuriranja sustava, resetiranje ili promjene konfiguracija. Ima funkciju *„Dynamic Thing Groups“* koja automatski grupira uređaje na temelju određenih upita te na taj način dozvoljava jednostavno upravljanje uređajima sličnih karakteristika. AWS IoT Device Management ima siguran sustav i sveobuhvatan sustav za upravljanje i nadzor IoT uređajima, te ga zbog toga čini idealnim za širok spektar primjene u različitim industrijama [23].

Azure IoT Hub je softver koji nudi Microsoft a omogućava sigurnu i pouzdanu dvosmjernu komunikaciju između milijun IoT uređaja i aplikacije na Cloud-u [24]. Ima mogućnost slanja poruka svim svojim uređajima iz aplikacije u cloud-u što može olakšati poslodavcima prijenos informacija. Ima široku primjenu od pametnih domova do pametnih gradova. Isto kao i AWS IoT Device Management omogućuje korisniku upravljanje i kontrolu flote putem jednog uređaja. Sigurnosne značajke koje ima su autentifikacija uređaja i kontrola pristupa. Autentifikacija uređaja znači da svaki uređaj mora obaviti proces provjere kako bi se povezao s IoT Hub-om, kontrola pristupa omogućuje primjenu pravila koja definiraju tko i kada može pristupiti podacima i funkcionalnostima. Prednosti Azure IoT Hub-a [24]:

- sigurnost,
- skalabilnost,
- upravljanje i
- fleksibilnost.

Cisco IoT Central je komercijalna platforma za upravljanje i nadzor IoT mrežom koju nudi Cisco Systems. Omogućuje praćenje stanja i performansi uređaja u realnom vremenu i konfiguraciju uređaja na daljinu. Ima robusne sigurnosne značajke poput šifriranja podataka u mirovanju i slanju, autentifikaciju korisnika i kontrolu pristupa. Dozvoljava administratoru jednostavno povezivanje različitih vrsta IoT uređaja putem raznih komunikacijskih protokola kao

što su MQTT, HTTP i CoAP. Koristi isto kao i AWS IoT Device Management sustav zvan *„Device Shadowing“* za praćenje i upravljanje uređaja, čak i kada nisu povezani. Za sigurnost koristi *„End-to-End“* enkripciju, te tako omogućava sigurnu komunikaciju između uređaja i oblaka. Također dolazi s funkcijom praćenja statusa i performansi uređaja u stvarnom vremenu [25].

5 Komparativna analiza Cambium Networks i Aruba Networks pristupnih točaka

Pristupna točka (eng. *Access point* (AP)) je mrežni uređaj koji omogućuje drugim Wi-Fi uređajima spajanje na mrežu. Postoji izvedba u kojoj AP nije povezan žično s usmjerivačem, a postoji i izvedba u kojoj je povezan žično. Također ima i izvedba u kojoj je AP ukomponiran u postojeći usmjerivač. Pristupna točka u slučaju kada je povezana žično s usmjerivačem, često koristi Ethernet kabel za povezivanje, te onda koristeći bežičnu LAN tehnologiju, najčešće Wi-Fi omogućuje drugim uređajima povezivanje na tu mrežu.

Postoje različiti Wi-Fi standardi koji omogućuju različite brzine, udaljenosti i frekvencije [26]:

- 802.11b (Wi-Fi 1),
- 802.11a (Wi-Fi 2),
- 802.11g (Wi-Fi 3),
- 802.11n (Wi-Fi 4),
- 802.11ac (Wi-Fi 5) i
- 802.11ax (Wi-Fi 6).

Prvi standard IEEE (eng. *Institute of Electrical and Electronics Engineers*) 802.11b također poznat kao i Wi-Fi 1, radi na 2.4 GHz frekvenciji i koristi DSSS/CKK modulacijsku shemu za podatke [26]. Podržava različite brzine varirajući od 1, 2, 5.5 i 11 Mbps. Prostor koji može pokriti je u prosjeku 38 metara u zatvorenom, te 140 metara u otvorenom prostoru.

Drugi standard IEEE 802.11a koristi OFDM modulacijsku shemu kako bi mogao prenijeti veći broj podataka u kraćem vremenu. Ovaj standard Wi-Fi 2 funkcionira na 5 GHz frekvencijskom području, te podržava brzine od 6, 9, 12, 18, 24, 36, 48 i 54 Mbps zahvaljujući korištenju 20 MHz pojasne širine [26]. Podržava slanje signala do 35 metara u zatvorenom, te 120 metara na vanjskom terenu.

Treći standard IEEE 802.11g koristi frekvencijski pojas od 2,4 GHz i 5 GHz. Isti je poput Wi-Fi 2 standarda, osim što koristi i 2,4 GHz frekvencijski pojas. Također koristi OFDM modulacijsku shemu, te ima iste brzine prijenosa.

Četvrti standard IEEE 802.11n je nasljednik Wi-Fi 3, u njemu je uveden MIMO (eng. *Multiple Input, Multiple Output*) koji omogućuje još veće brzine prijenosa. Podržava 20MHz i 40MHz pojasne širine. Zahvaljujući MIMO i korištenju veće pojasne širine, može postići brzine od 150 Mbps. Površinu koju pokriva je 70 metara u unutarnjem prostoru, te 250 u vanjskom. Koristi modulacijske sheme poput BPSK, QPSK, 16QAM i 64QAM [26].

Peti standard IEEE 802.11ac, podržava veće brzine prijenosa podataka zbog korištenja veće pojasne širine (do 160 MHz), višekorisničkog MIMO-a, većeg broja prostornih tokova i većeg broja modulacijskih shema (256QAM). Funkcionira na 5 GHz frekvencijskom području. Podržane su različite širine pojasnog kanala koje uključuju 20 MHz, 40 MHz, 80 MHz i 160 MHz.

Omogućuje maksimalnu brzinu prijenosa od 6,93 Gbps i raspon pokrivenosti približno 80 metara [26].

Zadnji standard koji je trenutno u funkciji je 802.11ax, odnosno Wi-Fi 6. On nudi veće brzine i veći raspon pokrivenosti u usporedbi s prethodnim standardima. Radi na frekvencijskom pojasu od 2,4 GHz i 5 GHz. Koncept OFDMA (eng. *orthogonal frequency-division multiple access*) uveden je u smjeru uzlazne i silazne veze, uključuje MU-MIMO (eng. *Multi-user, multiple-input, multiple-output*) koji omogućuje pristupnoj točki komuniciranje s više uređaja istovremeno. Tehnika multipleksiranja i kodiranja podataka OFDMA dijeli kanal na manje frekvencijske nosioce, svaki nosioc se može podijeliti pojedinom korisniku, te omogućuje slanje i primanje podataka od više klijenata istovremeno. Zbog svoje visoke učinkovitosti Wi-Fi 6 poznat je i kao HEW (eng. *High Efficiency* WLAN). On nudi bolju učinkovitost, mrežni kapacitet, performanse i korisničko iskustvo uz smanjenu latenciju [26].

5.1. Cambium Networks

Tvrtka Cambium Networks osnovana je 2011. godine u SAD-u, nudi širok spektar proizvoda i usluga za pružatelje širokopojasnih usluga, tvrtke, vlade i javne agencije. Njihova rješenja su pouzdana, inovativna i skalabilna. Cambium Network tvrtka je vodeća u području OFDMA tehnologije, te su dobili brojne nagrade za svoje proizvode i usluge [27]. Proizvodi su dizajnirani za rad u zahtjevnim okruženjima i mogu se skalirati kako bi zadovoljili potrebe rastućeg poslovanja. Konstantno se fokusiraju na razvoj i implementaciju najnovijih bežičnih tehnologija i brzom prihvaćanju novih standarda.

Pristupna točka XV3-8 je proizvod iz serije *„cnPilot Xirrus“*. Idealno je za organizacije koje traže visokoučinkovitu Wi-Fi mrežu za podršku velikog broja korisnika i aplikacija s velikom propusnošću. Omogućuje dediciranoj mreži kontinuirano skeniranje kako bi se poboljšali sigurnosni protokoli. Tri podatkovna radija mogu se konfigurirati kao dva 5GHz 4x4 plus jedan 2,4 GHz 4x4, ili se dva 5 GHz radija mogu kombinirati u jedan 5 GHz 8x8 radio s maksimalnom snagom i performansama Wi-Fi 6 standarda [27]. Moguće je simultano imati čak 16 drugačijih Wi-Fi SSID-ova, te je također moguće povezivanje do 1024 uređaja istovremeno. Pristupna točka omogućuje odličnu i detaljnu konfiguraciju lokalno ili korištenjem „*Cambium XMS management*“ ili kroz *„cnMaestroTM Cloud“*. Dostupne su maksimalne brzine do 6 Gbps. Koristi OFDMA tehnologiju za efikasnije korištenje spektra velikog broja korisnika, te to značajno smanjuje kašnjenja i poboljšava iskustvo korisnika, čak i u mrežama velikog opterećenja. Također XV3-8 koristi Mesh tehnologiju koja koristi više bežičnih pristupnih točaka za povezivanje i distribuciju Wi-Fi signala, te je iz tog razloga odličan izbor za tvrtke koje imaju velike prostore za pokriti signalom [27].

5.2. Aruba Networks

Aruba Networks je tvrtka koja se specijalizira za rješenja podatkovne mreže posebno u djelu bežičnih mreža (Wi-Fi) i mrežne sigurnosti. Osnovana je 2002. godine u SAD-u te je dio Hewlett Packard Enterprise grupe. Dostupan je širok spektar proizvoda, uključujući mrežne preklopnike,

upravljačke sustave za mreže, softver za upravljanje mrežama, bežične pristupne točke i rješenja za mrežnu sigurnost. Njihovi proizvodi i rješenja su poznati po svojoj pouzdanosti, performansama, jednostavnosti korištenja i inovativnosti. Nudi napredne sigurnosne funkcije za bežične mreže, uključujući WPA3 enkripciju, prevenciju ubacivanja i segmentaciju mreže. Njihovi proizvodi se koriste u raznim industrijama poput zdravstva, maloprodaje, obrazovanja i financijskih sektora. Poznati su po svojoj jednostavnosti i prilagođenosti za korisnika, kako bi mu pružili što bolju kontrolu i konfiguraciju mreže[28].

Pristupna točka Aruba AP12(RW) dizajnirana za male i srednje velike tvrtke. Nudi visoku pouzdanost, jednostavnu instalaciju i velike propusnost. Bazirana je na Wi-Fi 6 standardu, te može podržati 75 uređaja istovremeno. Koristi OFDMA tehnologiju za poboljšanje performansi u okruženjima s velikim brojem korisnika. Predviđena je za unutarnje korištenje, te koristi MU-MIMO izvedbu i zbog toga može postići brzine od 1.6 Gbps. Koristi ugrađeni sustav osiguranja koji sadrži vlastiti vatro zid (*eng. Firewall*) kako bi podijelio poslovni i javni promet. Osmišljen je za mobitele, IoT i sigurnosne potrebe. Dizajniran je kako bi služio kao glavni Wi-Fi usmjerivač za mrežu. Aruba Networks svojim korisnicima daje na uslugu njihovu aplikaciju za upravljanje mrežom „Aruba Instant on“ kako bi mogli putem svojeg mobilnog uređaja kontrolirati svoju postavljenu mrežu. Dolazi sa WPA3 enkripcijom kako bi se što kvalitetnije osigurala bežična mreža [28].

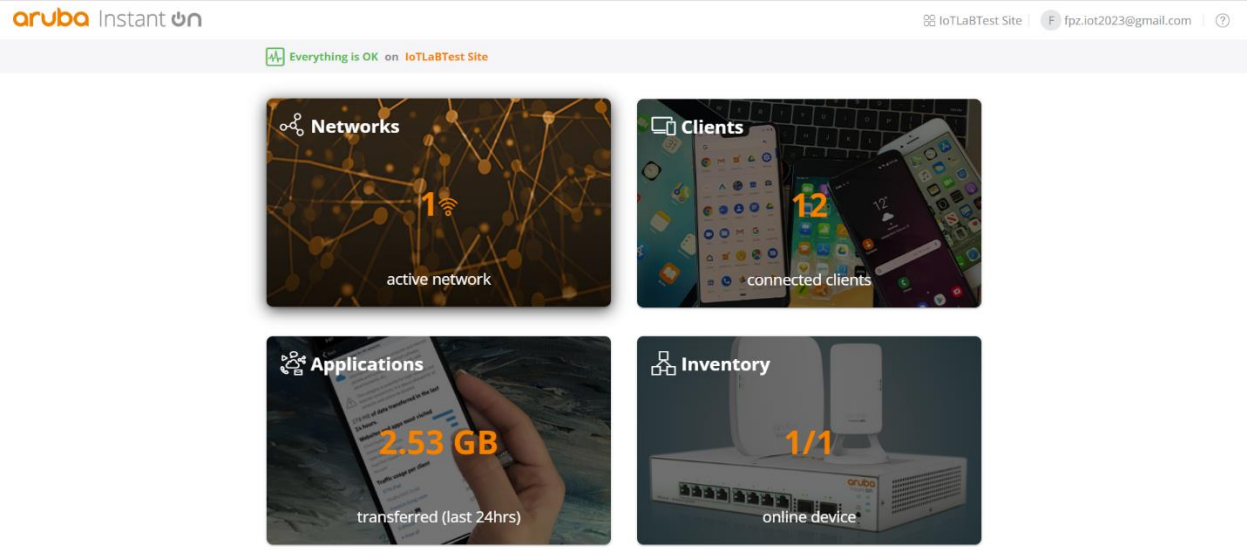
5.3.Konfiguracija pristupnih točaka

5.3.1 Aruba AP12 (RW)

Aruba Network pristupna točka je vrlo jednostavna za spajanje, potrebno je samo spojiti AP na prespojnik i u napajanje električne energije. Dolazi s aplikacijom za konfiguraciju i pregled mreže. Softver se može koristi putem web preglednika i putem pametnog mobitela. Zove se „Aruba Instant on“ te nudi razne mogućnosti koje su vrlo jednostavno prikazane i lagane za korištenje. Na slici broj 3 se može vidjeti početno korisničko sučelje te njene mogućnosti. Nudi četiri osnovna pregleda mreže:

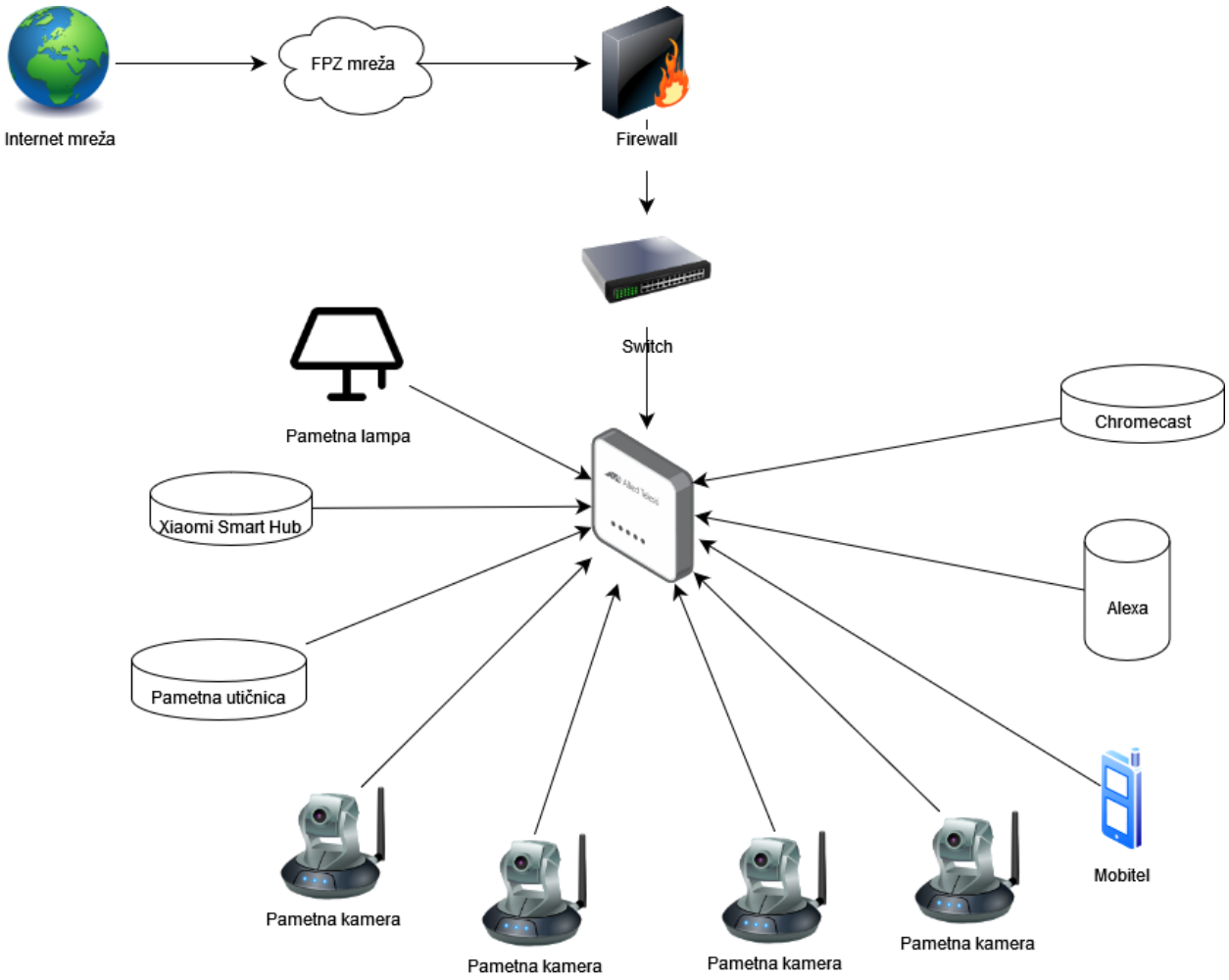
- aktivne mreže (engl. *Active Networks*),
- uređaji koji su spojeni na mrežu (engl. *Clients*),
- ostvareni promet (engl. *Applications*) i

- oprema (engl. *Inventory*).



Slika 3 Početno korisničko sučelje „Aruba Networks“ aplikacije

Aruba instant on softver dopušta pregled svih trenutno spojenih uređaja na postojeću mrežu. Sa slike 2 se može primijetiti da je trenutno spojeno 12 uređaja. Slika 4 prikazuje topologiju spojenih uređaja na mreži. Može se primijetiti kako su svi uređaji spojeni putem određenih bežičnih tehnologija na Aruba AP. Vidljivo je da su spojeni *„Xiaomi Smart hub“* i *„Alexa“* koji služe poput sustava za nadzor i upravljanje uređajima. Asistent *„Alexa“* ima ulogu slušanja govornih naredbi kako bi izvršila određene želje korisnika, te su također uređaji spojeni na *„Xiaomi Smart Hub“* radi lakše kontrole istih putem aplikacije na mobilnom uređaju. Sa slike je vidljivo da Aruba AP igra glavnu ulogu u izvedbi mreže, jer sav promet prolazi kroz njega prije slanja podataka korisniku. Također uređaji koji služe za izvršavanje naredbi od strane korisnika šalju te naredbe drugim uređajima putem AP.

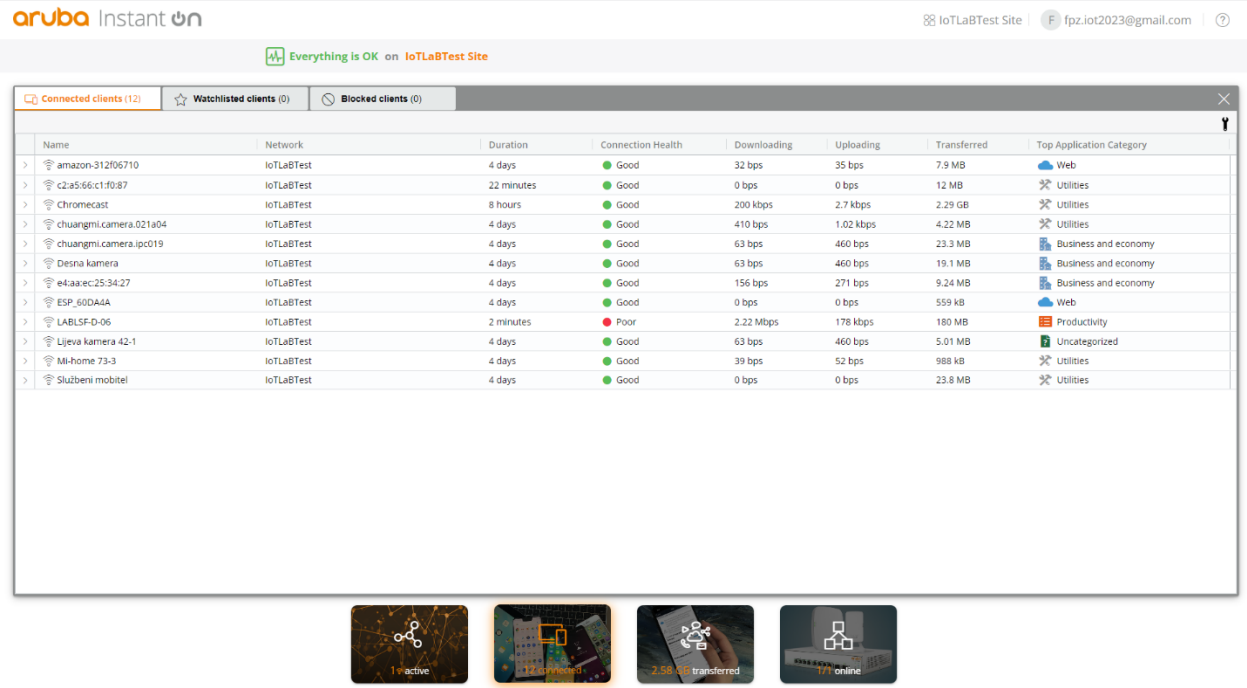


Slika 4 Topologija IoT mreže u laboratoriju

Softver koji Aruba Networks koristi također dozvoljava korisniku pregled trenutno spojenih uređaja na mrežu, te se na slici 5 može vidjeti njihov popis. Također se može vidjeti:

- razdoblje koliko je uređaj dugo spojen na mrežu,
- stanje konekcije,
- brzina preuzimanja,
- brzina slanja podataka i
- ostvareni promet.

Svi ti podaci su odlična komponenta koja omogućuje korisniku detaljan pregled svih uređaja, te također ima ključnu ulogu ukoliko dođe do nekakvog problema na mreži. Na način da se može pretpostaviti koji uređaj stvara probleme.

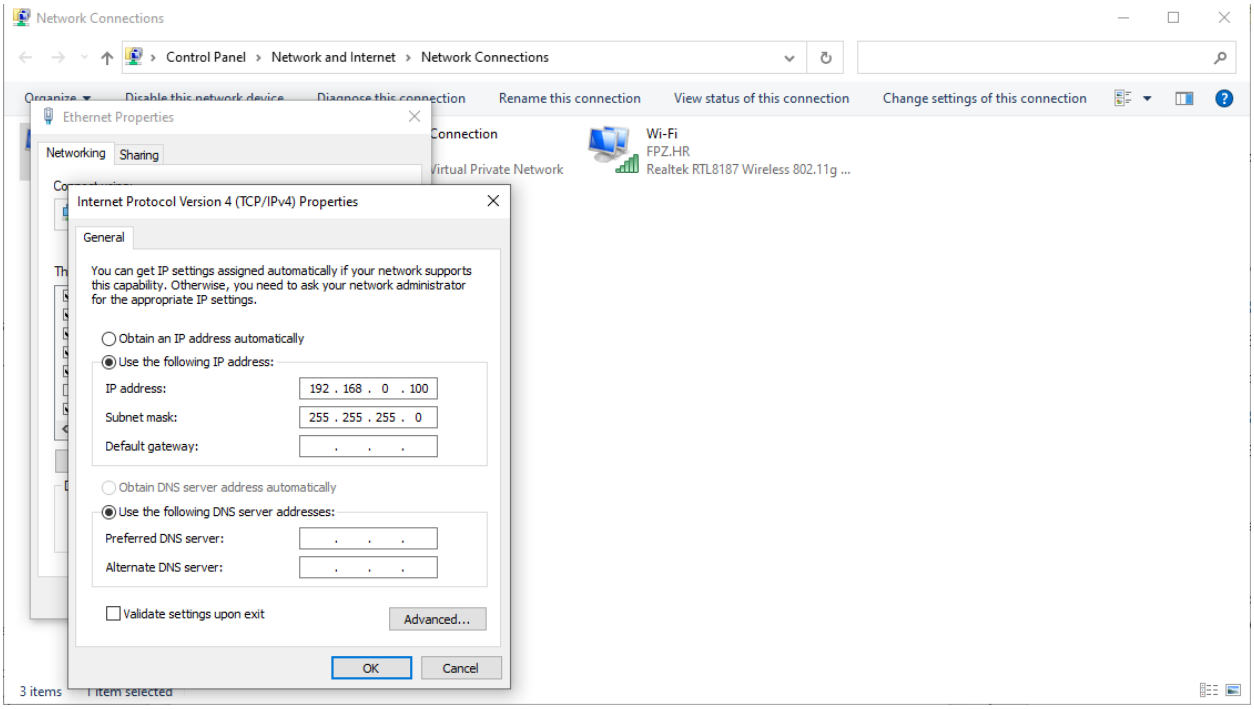


Slika 5 Pregled spojenih uređaja na "Aruba Networks" AP

Aruba dozvoljava korisniku jednostavno postavljanje AP, pristupačnu konfiguraciju, te isto tako i preglednu. Pristupna točka koja se koristila je bila AP 12 (RW), koja koristi Wi-Fi 6 standard.

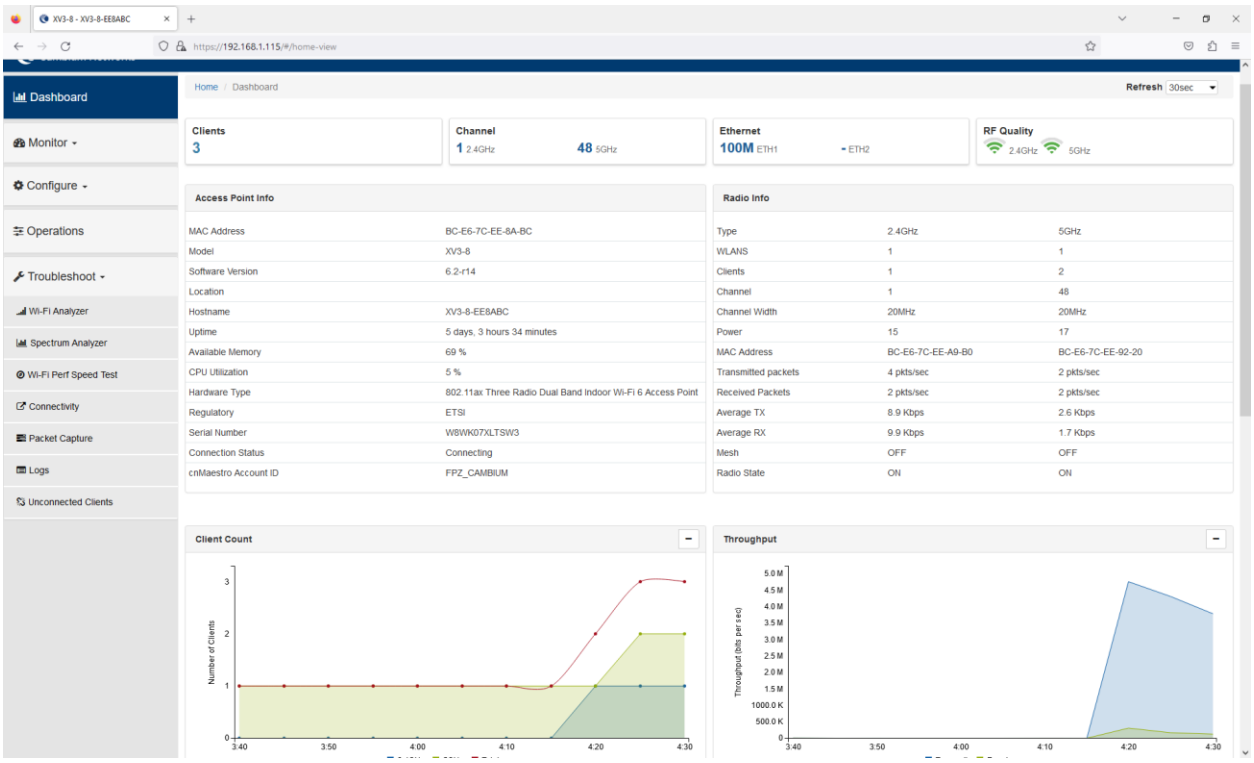
5.3.2 Cambium Networks

Pristupna točka XV3-8 je prijenosna jedinica koja se koristi za pružanje pristupa internetu i drugim bežičnim uslugama. Pouzdana je jedinica koja je dizajnirana za rad u zahtjevnim uvjetima. Koristi UHF i VHF radio valove za komunikaciju, ima domet i do 10 kilometara. Za razliku od pristupnih točaka Arube XV3-8 nije toliko jednostavna za postaviti, jer uključuje spajanje AP s računalom i prespojnikom. Na taj način se onda putem računala konfigurira lokalna IP adresa AP, što se može vidjeti na slici 6. Nakon što se AP postavi moguće je ući u njegove postavke putem njegove IP adrese.



Slika 6 Konfiguracija XV3-8 putem računala

Postavke za konfiguraciju su detaljne i kompleksne, ako se korisnik prvi puta susreće s tim pojmovima. Na slici 7 je vidljiva stranica za konfiguraciju „Cambium Networks“ AP-a, te se također mogu vidjeti brojne opcije i postavke koje se mogu nadgledati i mijenjati ovisno o željama. Može se vidjet kako uređaj radi na 2,4 GHz i 5 GHz pojasu i da je trenutno spojeno 3 klijenta na njega. Vidljiva su i dva grafa, prvi prikazuje koliko je klijenata spojeno na AP ovisno o vremenu spajanja, dok drugi prikazuje propusnost na mreži također ovisno o vremenu. Stranica za konfiguracija nudi opcije nadgledanja mreže, odnosno pregled svih klijenata koliko su dugo spojeni i koliki promet ostvaruju u stvarnome vremenu. Ukoliko dođe do problema s AP Cambium Networks nudi na svojoj stranici za konfiguraciju opciju za traženje i uklanjanje problema na mreži.



Slika 7 Mogućnosti konfiguracije "Cambium Networks" mreže

5.4. Usporedba Cambium Networks i Aruba Networks pristupnih točaka

Oba uređaja se baziraju na Wi-Fi 6 standardu bežične mreže te koriste 2,4 GHz ili 5 GHz frekvencijsko područje. Cambium Networks pristupna točka XV3-8 dozvoljava maksimalnu brzinu od 1,73 Gbps, dok Aruba AP12(RW) ima 1,2 Gbps. Cambium Networks je prilagođen za velike tvrtke, škole ili javna mjesta na kojima je veliki broj korisnika i potrebna je visoka propusnost. Za srednje velike i male tvrtke koje se više fokusiraju na jednostavnost upravljanja je Aruba Networks AP 12 (RW) bolja opcija. Pristupna točka XV3-8 zahtijeva bolje tehničko znanje korisnika.

Aruba Networks ima robusnije sigurnosne značajke, uključujući podršku za više standarda autentifikacije i šifriranja. Koristi WPA3 enkripciju koja je najnoviji standard Wi-Fi enkripcije te je značajno bolja od prethodne WPA2 [29]. Također Aruba Networks koristi višefaktornu autentifikaciju koja zahtijeva od korisnika da pruži više od jednog dokaza identiteta prilikom pristupa mreži. Funkcija sigurnosti koju Aruba Networks koristi je ta da se kreira odvojena mreža za goste, odvojeno od primarne mreže na kojoj se možda nalaze osjetljivi podaci. Segmentacija mreže je isto jedna od sigurnosnih opcija koja dozvoljava dijeljenje mreže na manje segmente, ograničavajući protok za poboljšanje sigurnosti i performansi. Cambium Networks nudi određene sigurnosne funkcije, ali one nisu toliko dobre kao kod Arube. Koristi WPA2/WPA3 enkripciju za zaštitu te dozvoljava korisniku da kreira više odvojenih Wi-Fi mreža sa različitim lozinkama. Cambium Networks pruža naprednu filtraciju paketa koja omogućava filtriranje prometa prema

određenim kriterijima za dodatnu kontrolu. Nudi korisniku dovoljno sigurnosnih funkcija za zaštitu većine Wi-Fi mreža, ali ako je potrebna napredna kontrola pristupa, višefaktorna autentifikacija ili druge sigurnosne mjere, Aruba Networks je bolji izbor. Opciju koju nudi Aruba je ta da može blokirati određene aplikacije i web sadržaje kako bi spriječila određene prijetnje za sigurnost mreže. Odlična opcija u slučaju gdje se pristupna točka koristi u tvrtkama sa velikim brojem korisnika kako bi se održao siguran rad za sve korisnike i njihove uređaje.

Cambium Networks sa svojom XV3-8 pristupnom točkom dozvoljava korisniku upravljanje mrežom na samom uređaju, no za napredno upravljanje i centraliziranu kontrolu korisniku će biti potreban zaseban kontroler *„Cambium Networks cnMaestro“*. Platforma cnMaestro je *„Cloud Management“* opcija na kojoj se pruža detaljan pregled svih uređaja na jednoj lokaciji. Korisnik može vidjeti:

- stanja uređaja u realnom vremenu,
- povezane klijente i njihovu aktivnost,
- detaljni pregled performansi mreže,
- analizu prometa za identifikaciju potencijalnih problema i
- povijest podataka za praćenje performansi mreže.

Stanje uređaja u realnom vremenu je odlična opcija za kontrolu mreže kako bi se moglo vidjeti koji uređaj dobiva koliko signala te ukoliko ima neki problem da se u što kraćem roku ukloni. Pregled povezanih klijenata i njihovu aktivnost omogućuje administratoru uvid u to koliko je korisnika trenutno spojenu na mrežu te čime se bave na mreži. Na taj način se mogu spriječiti potencijalni napadi na mrežu. Detaljni pregled performansi mreže omogućuju uklanjanje problema na mreži ukoliko ih ima, na način da se vidi koliko signala je poslano i koliko je primljeno. Povijest podataka za praćenje performansi mreže daje uvid administratoru u prethodne poteškoće na mreži te kako ih sljedeći puta ukloniti. Također se može vidjeti kako je mreža radila dok administrator nije nadgledao.

Aruba Instant On platforma dozvoljava jednostavno postavljanje i konfiguraciju, upravljanje mrežom preko cloud-a ili lokalnog uređaja. Također korisniku daje opciju za automatizaciju i analizu mreže. Aruba Networks pristupne točke dolaze sa svojom aplikacijom za kontrolu i postavljanje mreže te je iz tog razloga jednostavnija upotreba i instalacija nego kod XV3-8. Ova platforma je odlično rješenje za upravljanje manjim i srednjim mrežama koje koriste Aruba Instant On pristupne točke. Aplikacija je dizajnirana da bude laka za korištenje i ne zahtijeva puno IT iskustva, također Aruba nudi svoje funkcije za upravljanje putem vlastite web platforme koja omogućuje korisniku napredne kontrole i funkcije.

Što se tiče IoT-a Cambium Networks nudi tri radio-trake za komunikaciju, smanjujući zagušenja i poboljšavajući performanse, posebice u okruženjima sa velikim brojem uređaja. Koristi 2,4 GHz i 2x 5 GHz koji su idealni izbor u situacijama gdje se uređaji nalaze daleko od AP ili im je potrebna velika brzina. Pojas 2,4 GHz je odličan izbor za uređaje sa većim dometom i nižom propusnošću podataka, dok s druge strane 5 GHz može koristiti za uređaje kojima je potrebna veća brzina i manji domet. Pristupna točka XV3-8 podržava uobičajene IoT protokole poput LoRaWAN i Zigbee, te dozvoljava povezivanje veliki broj različitih pametnih uređaja. S

druge strane Aruba Networks nudi centralizirano upravljanje i pregled svih uređaja na mreži te to može biti korisno za veće implementacije IoT-a [30].

Pristupna točka Aruba AP 12 ima funkciju mesh kako bi se veći prostor mogao pokriti signalom. Vrlo jednostavan je proces povezivanja drugih pristupnih točaka s glavnom, te se na taj način mogu pratiti i osigurati rad pametnih uređaja u IoT okruženju. S druge strane Cambium XV3-8 ne podržava mesh sustav pokrivanja prostora. On nudi multi-hop funkciju koja omogućava bežično povezivanje Cambium uređaja na njega, ali ne pruža automatsko prebacivanje i pokrivanje cijelom površinom kao mesh sustav [30]. Svako bežično povezivanje može smanjiti propusnost i povećati kašnjenje. Mesh sustav omogućuje automatsko prebacivanje uređaja između pristupnih točaka, a multi-hop ručno povezivanje. U slučaju gdje se pametni uređaj miče kroz mrežu bolja opcija je Aruba radi svoje mesh funkcije. Iz tog razloga za dinamički IoT preporuča se Aruba AP 12 kako bi se osigurao kvalitetan rad pametnih uređaja bilo gdje na području pokrivenom pristupnim točkama. Centralizirano upravljanje mrežom je odlična funkcija za IoT izvedbu, jer dozvoljava jednostavno i brzo konfiguriranje uređaja. Omogućuje postavljanje različitih pravila i filtera za IoT uređaje te uvelike pojednostavljuje kontrolu i nadzor svih uređaja spojenih na mrežu. Ograničenja koja posjeduje AP 12 je limitirana podrška protokola iz razloga što je pristupna točka više fokusirana na Wi-Fi uređaje te iz tog razloga postoji mogućnost da neće podržavati standardne IoT protokole.

Tablica 1. Specifikacije pristupnih točaka

Aruba AP 12 (RW)	Cambium Newtorks XV3-8
Standardi i brzina • Wi-Fi 6 • 2,4 GHz i 5 GHz • 1,2 Gbps	**Standardi i brzina** • Wi-Fi 6 • 2,4 GHz i 2x5 GHz • 1,73 Gbps
Sigurnost • WPA 3 enkripcija • višefaktorna autentifikacija • segmentacija mreže	**Sigurnost** • WPA2/WPA3 enkripcija • napredna filtracija paketa
Upravljanje mrežom • Aruba Instant On • upravljanje mreže putem oblaka • automatizacija mreže putem oblaka	**Upravljanje mrežom** • cnMaestro • detaljni pregled performansi mreže • zahtjevnija konfiguracija
IoT • Mesh sustav • centralizirano upravljanje • manjak IoT protokola • 75 uređaja istovremeno	**IoT** • tri radio-trake za komunikaciju • LoRaWAN • Zigbee • 1024 uređaja istovremeno

U tablici 1. može se vidjeti pojednostavljeni i skraćeni prikaz specifikacija dviju pristupnih točaka. Može se primijetiti da je za IoT izvedbu ipak Cambium XV3-8 bolja opcija radi protokola koje posjeduje, ali je jedini problem pokrivenost mreže jer ne posjeduje Mesh sustav.

6 Zaključak

Razvojem digitalnog svijeta, povećava se količina postojećih pametnih uređaja koji se spajaju na Internet. Svaki od tih uređaja ima opciju spajanja s drugim pametnim uređajima na mreži, te oni međusobno komuniciraju kako bi se poboljšao i maksimizirao njihov rad.

Internet of Things (IoT) predstavlja mrežu fizičkih uređaja, vozila, kućnih uređaja, te ostalih uređaja koji su opremljeni sa senzorima, softverima i mogućnostima povezivanja na postojeće mreže.

Sigurnost u IoT izvedbi je od velike važnosti iz razloga što je sve veći broj uređaja povezanih na Internet. Neki od načina poboljšavanja sigurnosti su: autentifikacija ili autorizacija, segmentacija mreže, enkripcija, edukacija, procjena rizika.

IoT ima širok spektar primjene, te se koristi u različitim sektorima poput kućanstva, zdravstva, poljoprivrede, gradova, industrije i transporta.

Komunikacijske tehnologije igraju veliku ulogu u izvedbi IoT-a a sastoje od više koraka: kodiranje, modulacija, prijenos, demodulacija i dekodiranje.

Najčešća izvedba spajanja pametnog uređaja na internet je putem Wi-Fi, a vrlo često je i spajanje pametnih uređaja putem mobilne mreže. Najzastupljenije komunikacijske tehnologije u pametnim uređajima su: RFID, Bluetooth, Zigbee, Z-Wave, MiWi i LoRaWAN.

Upravljanje uređajima u IoT okruženju uključuje daljinsko registriranje uređaja, autentifikaciju, konfiguriranje, održavanje, dijagnostiku, tj. nadzor povezanih uređaja s centralizirane platforme kojoj IT administratori mogu pristupiti putem internetske veze s bilo kojeg mjesta na bilo kojem uređaju.

Sustavi za upravljanje i nadzor IoT-a donose niz prednosti, ali s druge strane suočavaju se s brojnim izazovima koji otežavaju njihovo korištenje i implementaciju. Glavni izazovi sustava za upravljanje i nadzor su: kontrola pristupa, proliferacija uređaja, fragmentirani podaci, ali i nagli porast broja tih uređaja što može opteretiti mrežu i dovesti do zagušena mreže te prekida u radu.

Usporedbom pristupnih točaka Cambium Networks i Aruba Networks dolazi se do zaključka. Oba uređaja se baziraju na Wi-Fi 6 standardu bežične mreže, te koriste 2,4 GHz ili 5 GHz frekvencijsko područje. Pristupna točka XV3-8 dozvoljava maksimalnu brzinu od 1,73 Gbps dok Aruba AP12(RW) ima 1,2 Gbps. Aruba AP12 (RW) koristi Mesh sustav umrežavanja, te je iz tog razloga pogodna za velike prostore. Cambium Networks prilagođen za velike tvrtke, škole ili javna mjesta na kojemu ima veliki broj korisnika i potrebna je visoka propusnost. Za srednje velike i male tvrtke koje se više fokusiraju na jednostavnost upravljanja je Aruba Networks AP 12 (RW) bolja opcija. Pristupna točka XV3-8 zahtijeva bolje tehničko znanje korisnika.

Popis literature

[1] IBM. *What is the internet of things?* Preuzeto s https://www.ibm.com/cloud/learn/internet-of-things. [Pristupljeno: Kolovoz, 2023.]

[2] GeeksforGeeks. *Architecture of Internet of Things (IoT).* Preuzeto s https://www.geeksforgeeks.org/architecture-of-internet-of-things-iot/. [Pristupljeno: Kolovoz, 2023.]

[3] Čavrak, I., & Sarić, M. *INTERNET of THINGS (IoT)- IZAZOVI I MOGUĆNOSTI CYBER SIGURNOSTI POVEZANE S IoT-om.* Preuzeto s https://hrcak.srce.hr/file/392472 [Pristupljeno: Kolovoz, 2023.]

[4] Google. *See smart home devices that work with Google Home.* Preuzeto s: https://home.google.com/explore-devices/ [Pristupljeno: Kolovoz, 2023.]

[5] Wipro. *What can IoT do for healthcare?* Preuzeto s https://www.wipro.com/business-process/what-can-iot-do-for-healthcare-/ [Pristupljeno: Kolovoz, 2023.]

[6] IoT Solutions World Congress. *IOT TRANSFORMING THE FUTURE OF AGRICULTURE.* Preuzeto s https://iotsworldcongress.com/ [Pristupljeno: Kolovoz, 2023.]

[7] Zagorje.com. *[VIDEO] POČELO JE: Na bregu u Zagorju 'špricali trsje' koristeći dron / Sv. Križ Začretje / Zagorje.com.* Preuzeto s: https://www.zagorje.com/clanak/sv-kriz-zacretje/video-pocelo-je-na-bregu-u-zagorju-spricali-trsje-koristeci-dron [Pristupljeno: Kolovoz, 2023.]

[8] Milanović Glavan, L. *Razvoj prometnih gradova u republici Hrvatskoj*. Ekonomski fakultet u Zagrebu. [Pristupljeno: Kolovoz, 2023.]

[9] SAP Insights. *What is industry 4.0? Definition, technologies, benefits.* Preuzeto s: https://www.sap.com/croatia/products/scm/industry-4-0/what-is-industry-4-0.html [Pristupljeno: Kolovoz, 2023.]

[10] Onomondo. *IoT in logistics and transportation.* Preuzeto s: https://onomondo.com/industries/logistics-and-transportation-iot/ [Pristupljeno: Kolovoz, 2023.]

[11] Digi International. *How Do IoT Devices Communicate?* Preuzeto s: https://www.digi.com/blog/post/how-do-iot-devices-communicate [Pristupljeno: Kolovoz, 2023.]

[12] Optimum. *What is WiFi?* Preuzeto s https://www.optimum.com/articles/internet/what-is-wifi [Pristupljeno: Kolovoz, 2023.]

[13] TechTarget. *What is mobile data?* Preuzeto s: https://www.techtarget.com/whatis/definition/mobile-data [Pristupljeno: Kolovoz, 2023.]

[14] Spica. *Što je zapravo RFID?* Preuzeto s https://www.spica.hr/blog/sto-je-zapravo-rfid [Pristupljeno: Kolovoz, 2023.]

[15] GeeksforGeeks. *Bluetooth.* Preuzeto s https://www.geeksforgeeks.org/bluetooth/. [Pristupljeno: Kolovoz, 2023.]

[16] GeeksforGeeks. *Introduction of ZigBee*. Preuzeto s https://www.geeksforgeeks.org/introduction-of-zigbee/. [Pristupljeno: Kolovoz, 2023.]

[17] PCMag. *Z-Wave Technology*. Preuzeto s: https://www.pcmag.com/encyclopedia/term/z-wave. [Pristupljeno: Kolovoz, 2023.]

[18] LoRa Alliance. *About LoRaWAN*. Preuzeto s https://lora-alliance.org/about-lorawan/. [Pristupljeno: Kolovoz, 2023.]

[19] Omega Software. *Utjecaj 5G tehnologije na Internet of Things.* Preuzeto s https://www.omega-software.eu/utjecaj-5g-tehnologije-na-internet-of-things/. [Pristupljeno: Kolovoz, 2023.]

[20] Aazam, M., Zeadally, S., & Baig, Z. *A survey on internet of things (IoT) security. Journal of Network and Computer Applications.* [Pristupljeno: Kolovoz, 2023.]

[21] MiWi protocol. Preuzeto s: https://www.microchip.com/en-us/products/wireless-connectivity/sub-ghz/miwi-protocol. [Pristupljeno: Lipanj, 2024.]

[22] Arapović I. *Simulacija rada IoT mreže primjenom programse podrške Cisco Packet Tracer.* [Pristupljeno: Lipanj, 2024.]

[23] Amazon. *AWS IoT Device Management.* Preuzeto s: https://aws.amazon.com/iot-device-management/. [Pristupljeno: Lipanj, 2024.]

[24] Azure. *Azure IoT Hub.* Preuzeto s: https://azure.microsoft.com/en-us/products/iot-hub. [Pristupljeno: Lipanj, 2024.]

[25] Cisco IoT Control Center. Preuzeto s: https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-control-center.html [Pristupljeno: Lipanj, 2024.]

[26] IEEE Standards Association. *The Evolution of Wi-fi Technology and Standards.* Preuzeto s: https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/. [Pristupljeno: Veljača, 2024.]

[27] Cambium Networks. *Cloud-managed Wi-Fi Access Points*. Preuzeto s: https://www.cambiumnetworks.com/products/wifi/ [Pristupljeno: Veljača, 2024.]

[28] Aruba Networks. *High-performance, secure, eneterprise wireless LAN with support for Wi-Fi 6 and Wi-Fi 6E.* Preuzeto s: https://www.arubanetworks.com/products/wireless/ [Pristupljeno: Veljača, 2024.]

[29] Firewalls. *Data sheet, indoor access point.* Preuzeto s: https://www.firewalls.com/pub/media/wysiwyg/datasheets/Aruba/DataSheet_ArubaIO_AP12.pdf [Pristupljeno: Svibanj, 2024.]

[30] Cambium Networks. *User guide, Enterprise Wi-Fi Access Points. System Release 6.2.* Preuzeto s: https://www.cambiumnetworks.com/wp-content/uploads/2021/08/Enterprise-Wi-Fi-6.3-Access-Point_User-Guide.pdf [Pristupljeno: Svibanj, 2024.]

Popis kratica i akronima

IoT (Internet of Things) Internet stvari

ENC (Elektronička naplata cestarina)

LTE (Long Term Evolution) bežični standard četvrte generacije (4G)

WPAN (Wireless Personal Area Network) bežična osobna mreža

IEEE (Institute of Electrical and Electronics Engineer) Institu inženjera elektrotehnike i elektronike

Wi-Fi (Wireless Fidelity)

OFDM (Orthogonal Frequency Division Multiplexing)

MIMO (Multiple Input Multiple Output) sustav sa više antena na odašiljačkoj i prijemnoj strani

BPSK (Binary Phase Shift Keying)

QPSK (Quadrature Phase Shift Keying)

QAM (Quadrature Amplitude Modulation)

WLAN (Wireless Local Area Network) Bežična lokalna mreža

PoE (Power over Ethernet) Napajanje električnom energijom putem Ethernet kabela

Popis grafičkih prikaza

Popis slika

Popis tablica

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni rad
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Komparativna analiza bežičnih pristupnih točaka u IoT okruženju, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, _____

Sven Bakrač,
(ime i prezime, *potpis*)