SVEUČILIŠTE U RIJECI

TEHNIČKI FAKULTET

Stručni studij elektrotehnike

Završni rad

PROBLEMATIKA IOT MREŽE

Rijeka, srpanj 2015.

Marino Draginić

0069051235

SVEUČILIŠTE U RIJECI

TEHNIČKI FAKULTET

Stručni studij elektrotehnike

Završni rad

PROBLEMATIKA IOT MREŽE

Mentor: Prof. v. š. mr. sc. Antun Sok

Rijeka, srpanj 2015.

Marino Draginić

0069051235

TEHNIČKI FAKULET
Povjerenstvo za završne ispite
preddiplomskog stručnog studija elektrotehnike
Br.: 602-04/15-14/36
Rijeka, 06.03.2015.

ZADATAK
za završni rad

Pristupnik: Marino Draginić

Matični broj: 0069051235
Lokalni matični broj: 10800007

Naziv zadatka: **PROBLEMATIKA IOT MREŽE**

Naziv zadatka na engleskom jeziku: **Internet of things network**

Sadržaj zadatka:

Funkcija i mogućnosti Internet of Things mreže, tehnologije koje se koriste i omogućavaju stalnu povezanost objekata. Problemi i moguća rješenja sigurnosti i privatnosti korisnika. Rješenja vezana uz problem potrošnje energije, perspektiva IoT tehnologije.

Zadano: 17.03.2015.

Mentor:
Prof. v. š. mr. sc. Antun Sok

Predsjednica Povjerenstva:
Izv. prof. dr. sc. Vera Gradišnik

Zadatak preuzeo dana: 17.03.2015.
(potpis pristupnika)

Dostaviti:
- Predsjednica Povjerenstva
- Mentor
- Djelovođa Povjerenstva
- Evidencija studija
- Pristupnik
- Arhiva Zavoda

IZJAVA

Sukladno s člankom 9. Pravilnika o završnom radu, završnom ispitu i završetku stručnih studija Tehničkog fakulteta Sveučilišta u Rijeci, od lipnja 2011., izjavljujem da sam samostalno izradio završni rad prema zadatku br. 602-04/15-14/36 od 06.03.2015.

Rijeka, srpanj 2015.

Draginić Marino

Marino Draginić

SADRŽAJ

1. UVOD

Sljedeći val u računalnom dobu nalaziti će se izvan područja tradicionalne radne površine (desktop). U Internet stvari (Internet of Things - IoT) paradigmi, mnogi predmeti koji nas okružuju će se nalaziti na mreži u jednom ili drugom obliku. Radio-frekvencijska identifikacija (Radio-frequency identification - RFID) i tehnologije mrežnih senzora omogućit će nam realizaciju ovog izazova, u kojemu su informacijski i komunikacijski sustavi neprimjetno ugrađeni u okolinu koja nas okružuje. To rezultira generacijom ogromnih količina podataka koje treba pohraniti, obraditi i prikazati u učinkovitom i lako shvatljivom obliku. Ovaj model će se sastojati od usluga koje su roba i dostavljene na način sličan tradicionalnim robama. Računarstvo u oblacima (Cloud computing) može pružiti virtualnu infrastrukturu za takvo korisno računalstvo koje integrira uređaje za praćenje, uređaje za pohranu, analitičke alate, vizualizacijske platforme i isporuku klijenata. Isplativi model koji nudi Cloud computing omogućit će uslugu rezerviranja s jednog kraja do drugog (end to end) za tvrtke i korisnike za pristup aplikacijama na zahtjev s bilo kojeg mjesta.

Pametno povezivanje s postojećim mrežama i programiranje svjesnog konteksta pomoću mrežnih resursa je neizostavni dio IoT-a. Uz rastuću prisutnost bežičnog pristupa internetu (WiFi i 4G LTE), evolucija prema sveprisutnim informacijskim i komunikacijskim mrežama je već vidljiva. Međutim, za uspješno stvaranje IoT-a, standard računalstva će morati ići iznad tradicionalnih mobilnih računalnih scenarija koje koriste pametni telefoni i prijenosna računala te se razvijati u povezivanju svakodnevnih postojećih objekata i ugrađivanju inteligencije u naše okruženje. Da tehnologija nestane iz svijesti korisnika, IoT zahtijeva:

1. zajedničko razumijevanje situacije svojih korisnika i njihovih aparata,

2. arhitekture softwera i komunikacijske mreže koje obrađuju i prenose kontekstualne informacije tamo gdje je relevantno,

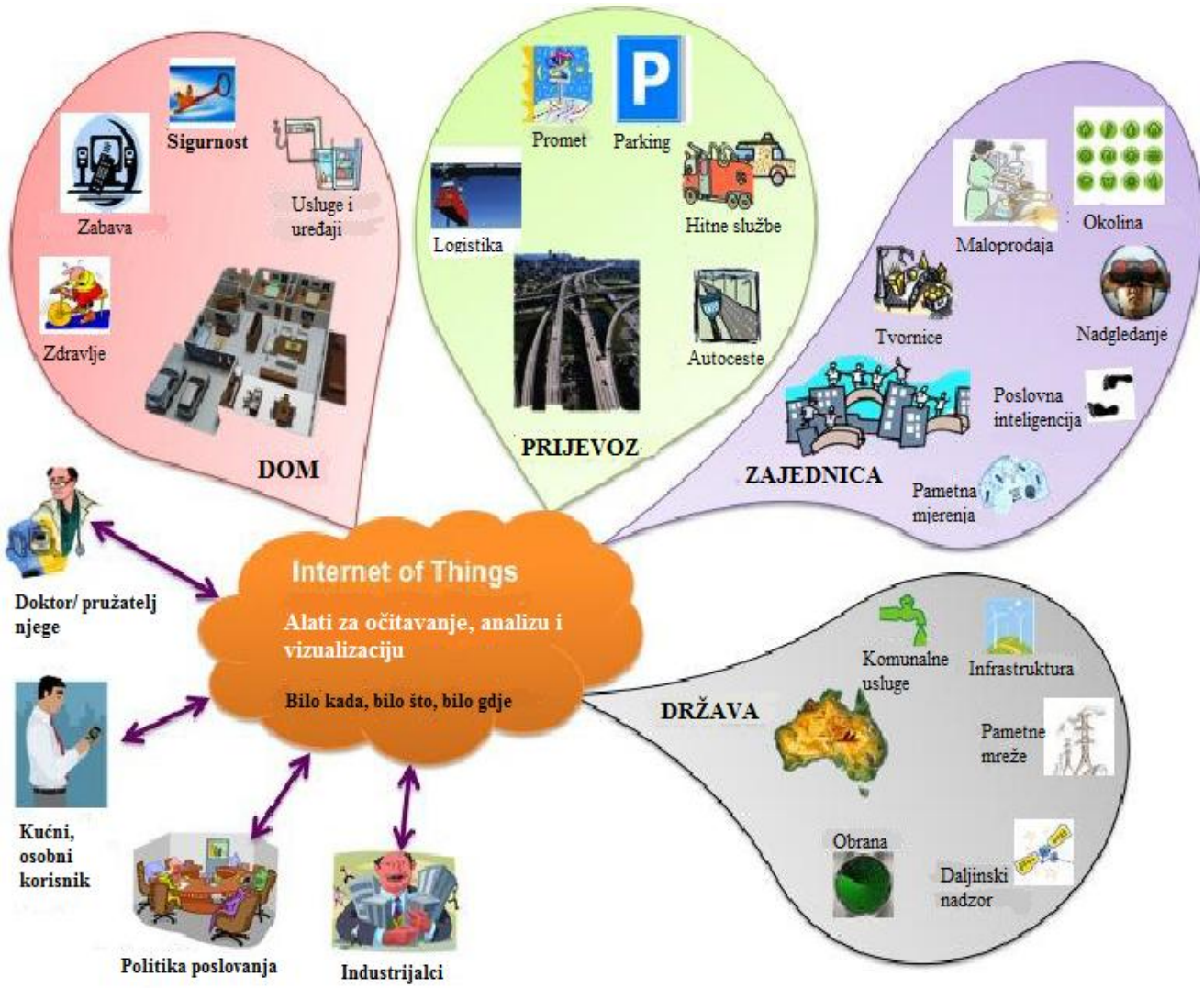
3. analitičke alate u IoT-u kojima je cilj samostalno i pametno ponašanje

Realizacijom ova tri temeljna zahtjeva, pametna povezanost i računalstvo svjesno konteksta se mogu ostvariti.

Radikalna evolucija trenutnog Interneta u mrežu međusobno povezanih objekata koji ne uzimaju samo informacije iz okoline (detekcijom) i vrše interakciju s fizičkim svijetom (aktivacija / naredbe / kontrola), ali i koristi postojeće internetske standarde za pružanje usluga za prijenos informacija, analizu, aplikacije i komunikacije. Potaknut rasprostranjenošću uređaja omogućenih otvorenimm bežičnim tehnologijama kao što su Bluetooth, radio–frekvencijska identifikacija,

Wi-Fi (Wireless Fidelity) i telefonske podatkovne usluge, kao i ugrađeni senzori i aktuatori čvorova, IoT je izašao iz svog „djetinjstva“ i nalazi se na rubu transformacije trenutnog statičkog Interneta u potpuno integrirani budući Internet. Revolucija interneta je dovela do međusobnog povezivanja ljudi do neviđenih razmjera i tempa. Sljedeća revolucija će biti povezanost između objekata za stvaranje pametnog okoliša. U 2011. godini, broj međusobno povezanih uređaja na planeti pretekao je stvarni broj ljudi. Trenutno je međusobno povezano 9 milijardi uređaja, a do 2020. godine se očekuje 24 milijarde uređaja. Prema udruzi za mobilne uređaje (Groupe Speciale Mobile Association - GSMA), to potencijalno omogućuje 1,3 trilijuna dolara prihoda operaterima mobilnih mreža te segmentima kao što su zdravlje, automobilska, komunalna i potrošačka elektronika.

Povezivanja objekata je prikazano na slici 1.1. u kojoj se aplikacijske domene odabiru na temelju skale utjecaja generiranih podataka. Raspon korisnika je od pojedinaca do nacionalnih organizacija koje se bave raznovrsnim pitanjima.



Slika 1.1. Prikaz krajnjih korisnika i područja aplikacija na temelju podataka [1]

Napor istraživača da stvore sučelje čovjek prema čovjeku pomoću tehnologije u kasnim 1980-im, rezultiralo je stvaranjem sveprisutne računalne discipline, čiji je cilj ugradnja tehnologije u pozadinu svakodnevnog života. Trenutno smo u eri poslije osobnih računala u kojoj pametni telefoni i drugi ručni uređaji mijenjaju naše okruženje, čineći ga više interaktivnim i informativnim. Mark Weiser, praotac sveprisutnog računarstva (ubicomp), definira pametni okoliš kao tjelesni svijet koji je bogato i neprimjetno isprepleten sa senzorima, pogonima, ekranima i računalnim elementima, neprimjetno ugrađenim u svakodnevne predmete naših života i povezane kroz kontinuiranu mrežu.

Stvaranje Interneta je označeno kao prekretnica prema ostvarenju vizije sveprisutnog računarstva koje omogućuje komunikaciju pojedinačnim uređajima s bilo kojim drugim uređajem na svijetu. Umrežavanje otkriva potencijal naizgled beskrajne količine distribuiranih računalnih resursa i memorija u rukama različitih vlasnika.

Napredak i konvergencija tehnologije mikro–električno-mehaničkih sustava (MEMS), bežične komunikacije i digitalne elektronike, rezultirala je razvojem minijaturnih uređaja koji imaju sposobnost osjeta, izračuna i bežične komunikacije na kratke udaljenosti. Te minijaturne uređaje nazivamo čvorovi te ih međusobno povezujemo da tvore mrežu bežičnih senzora (Wireless sensor network - WSN) i naći će široku primjenu u praćenju stanja okoliša, nadzoru infrastrukture, praćenju prometa, maloprodaji, itd.

Za realizaciju cijelovite IoT vizije, učinkovito, sigurno, skalabilno i tržišno orijentirano računalstvo i skladištenje izvora je bitno. Računarstvo u oblacima je najnovija paradigma u razvoju koja obećava pouzdane usluge koje se dostavljaju preko podatkovnih centara sljedećih generacija baziranih na tehnologijama virtualizirane pohrane. Ova platforma djeluje kao prijemnik podataka iz sveprisutnih senzora; kao računalo za analizu i interpretaciju podataka; također pruža korisniku lako razumljiv web–temeljen sadržaj. Sveprisutna očitavanja i obrada se odvija u pozadini, skriveno od korisnika.

Generirani podaci će se dijeliti preko različitih platformi i aplikacija, za razvoj zajedničke radne slike (Common operational picture - COP) okruženja, gdje je kontrola određenih neograničenih objekata moguća. Kao što smo prešli iz www (statičkih web stranica) na web2 (društveno umreženi web) ubuduće i web3 (web sveprisutnog računalstva), povećava se potreba za podacima na zahtjev pomoću sofisticiranih intuitivnih upita.

Da bismo u potpunosti iskoristili raspoloživu Internet tehnologiju, postoji potreba za implementacijom velike, platformno neovisne, infrastrukture mreža bežičnih senzora koja uključuje obradu i upravljanje podacima, aktivaciju i analitiku. Računarstvo u oblacima obećava visoku pouzdanost, skalabilnost i autonomiju za pružanje sveprisutnog pristupa, dinamičko

otkrivanje resursa i sposobnost potrebnu za sljedeću generaciju IoT aplikacija. Potrošači će moći odabrati razinu usluge promjenom parametara kvalitete usluge (Quality of service - QoS).

IoT se može realizirati u tri paradigme - Internet orijentiranoj (middleware), objektno orijentiranoj (senzori) i semantički orijentiranoj (znanje). Ova vrsta podjele je potrebna zbog interdisciplinarne naravi teme, korisnost IoT-a se može ostvariti samo u aplikacijskom domeni u kojoj se tri paradigme sijeku.

RFID skupina definira IoT kao svjetsku mrežu međusobno povezanih objekata jedinstveno adresiranih na temelju standardnih komunikacijskih protokola.

„Things“ se definiraju kao aktivni sudionici u poslovanju, informiranju i društvenim procesima u kojima mogu komunicirati među sobom i sa okolinom razmjenom podataka i informacija o okolišu, dok samostalno reagiraju na stvarna / tjelesna zbivanja u svijetu i utječu na njih vođenjem procesa koji pokreću akcije i stvaraju usluge sa ili bez izravne ljudske intervencije.

Pametni okoliš koristi informacijske i komunikacijske tehnologije kako bi ključne infrastrukturne komponente i usluge gradske uprave, obrazovanja, zdravstva, javne sigurnosti, prijevoza učinio interaktivnijim i učinkovitijim.

2. IOT ELEMENTI

Postoje tri temeljne IoT komponente:

1. Hardware - sastoji se od senzora, aktuatora i komunikacijskog hardware-a
2. Middleware - pohrana na zahtjev i računalni alati za podatkovnu analitiku
3. Prezentacija - lako razumljiva vizualizacija i interpretacija pomoću alata kojima se može naširoko pristupiti na različitim platformama i koji se dizajniraju za različite aplikacije

2.1. Radio–frekvencijska identifikacija (RFID)

RFID tehnologija je veliki napredak u ugrađenim komunikacijskim sustavima koja omogućuje dizajn mikročipova za bežičnu komunikaciju. Pomažu u automatskoj identifikaciji svega na što su stavljeni te djeluju kao elektronski barkod. RFID je bežična uporaba elektromagnetskih polja za prijenos podataka, potrebe automatske identifiikacije i praćenje oznaka priključenih na objekte. Oznake sadrže elektronski pohranjene podatke. Neke oznake se napajaju pomoću elektromagnetske indukcije magnetskih polja proizvedenih u blizini čitača. Druge vrste prikupljaju energiju iz ispitivačkih radio valova i djeluju kao pasivni transponder. Ostale vrste imaju lokalni izvor napajanja kao što je baterija te mogu raditi na stotine metara od čitača. Za razliku od barkoda, oznake ne moraju nužno biti u videokrugu čitača i mogu se ugraditi u objekt koji se prati. RFID oznake se koriste u raznim industrijama, kao naprimjer na automobilu tijekom proizvodnje za praćenje napretka kroz proizvodnu liniju; lijekovi u skladištima; RFID mikročipovi se ugrađuju u stoku i kućne ljubimce za identifikaciju. RFID oznake se mogu staviti na gotovinu, odjeću i ostale posjede ili ugraditi u životinje i ljude pa mogućnost čitanja osobno povjerljivih podataka bez pristanka postavlja pitanje privatnosti.
U 2012. godini, RFID tržište je vrijedilo 6.96 milijardi dolara, 7.77 milijardi dolara u 2013. i 8,89 milijardi dolara u 2014. To uključuje oznake, čitače i softver / usluge za RFID kartice, naljepnice i ostale oblike oznaka. Očekuje se da će tržišna vrijednost porasti na 27.31 milijardi dolara do 2024. godine.

Sustav za identifikaciju preko radio-frekvencije koristi oznake ili naljepnice stavljene na objekte koje treba identificirati. Dvosmjerni radio odašiljači–prijamnici koji se nazivaju ispitivači ili čitači šalju signal na oznaku i očitaju odgovor.

RFID oznake mogu biti pasivne, aktivne ili pasivne s baterijom. Aktivna oznaka je spojena s baterijom i periodički prenosi svoj identifikacijski signal. Pasivna oznaka s baterijom (Battery-assisted passive - BAP) ima malu bateriju i aktivira se kada je u prisutnosti RFID čitač. Pasivna oznaka je manja i jeftinija jer nema baterije; umjesto toga, oznaka koristi radio energiju čitača.

Međutim, da bi funkcionirala, pasivna oznaka mora biti osvijetljena s tisuću puta jačom razinom snage nego za prijenos signala. To mijenja razine smetnji i izloženosti radijaciji.

Oznake koje se mogu samo čitati (Read only), imaju tvornički dodijeljen serijski broj koji se koristi kao ključ u bazi podataka, a u oznakama s kojih se može čitati i pisati (Read / write), postoji mogućnost pisanja objektno specifičnih podataka u oznaku od strane korisnika sustava. RFID oznake se sastoje od najmanje dva dijela: integriranog kruga za pohranjivanje i obradu podataka, moduliranje i demoduliranje radiofrekvencijskog signala, prikupljanje istosmjernog napajanja iz incidentnog signala čitača; te antene za primanje i odašiljanje signala. Podaci oznake se pohranjuju u stalnu memoriju. RFID oznake uključuju ili fiksnu ili programabilnu logiku za obradu prenešenih i podataka sa senzora.
RFID čitač odašilje kodirani radio signal za ispitivanje oznake. RFID oznaka prima poruku, a zatim reagira s identifikacijskim i drugim informacijama. To može biti samo serijski broj jedinstvene oznake, informacije vezane uz proizvod kao što je kataloški broj, serija ili broj serije, datum proizvodnje, ili drugi posebni podaci.

RFID sustavi se mogu klasificirati prema vrsti oznake i čitača. Sustav pasivni čitač aktivna oznaka (Passive Reader Active Tag - PRAT) ima pasivni čitač koji prima samo radio signale iz aktivnih oznaka (sadrži bateriju, samo prijenos). Raspon PRAT sustava se može podesiti od 0-600 m, čime pronalazi upotrebu u aplikacijama kao što su zaštita imovine i nadzor.
Sustav aktivnog čitača pasivne oznake (Active Reader Passive Tag - ARPT) ima aktivni čitač koji prenosi ispitivački signal i prima autorizacijske odgovore pasivne oznake.
Sustav aktivnog čitača aktivne oznake (Active Reader Active Tag - ARAT) koristi aktivne oznake koje se aktiviraju s ispitivačkim signalom iz aktivnog čitača. Varijacija ovog sustava također može koristiti pasivnu oznaku s baterijom (BAP) koja djeluje kao pasivna oznaka, ali ima malu bateriju za napajanje povratnog signala oznake.
Fiksni čitači se postavljaju za stvaranje određene zone za ispitavanje koja se može kontrolirati. To omogućuje definiran prostor za čitanje te kada oznake ulaze i izlaze iz zone za ispitivanje. Mobilni čitači mogu biti ručni ili montirani na kolica ili vozila.

Tablica 2.1. RFID frekvencijski pojasevi [1]

Pojas	Domet	Brzina prijenosa	Primjedbe
120 – 150 kHz (LF)	10 cm	niska	identifikacija životinja, prikupljanje tvorničkih podataka

13.56 MHz (HF)	10 cm - 1 m	niska do umjerena	pametne kartice
433 MHz (UHF)	1 – 100 m	umjerena	obrambene aplikacije s aktivnim oznakama
865 - 868 MHz	1 – 12 m	umjerena do visoka	barkod, različiti standardi
2450 - 5800 MHz (mikrovalovi)	1 – 2 m	visoka	802.11 WLAN, Bluetooth standardi
3.1 – 10 GHz (mikrovalovi)	do 200 m	visoka	zahtijevaju polu - aktivne ili aktivne oznake

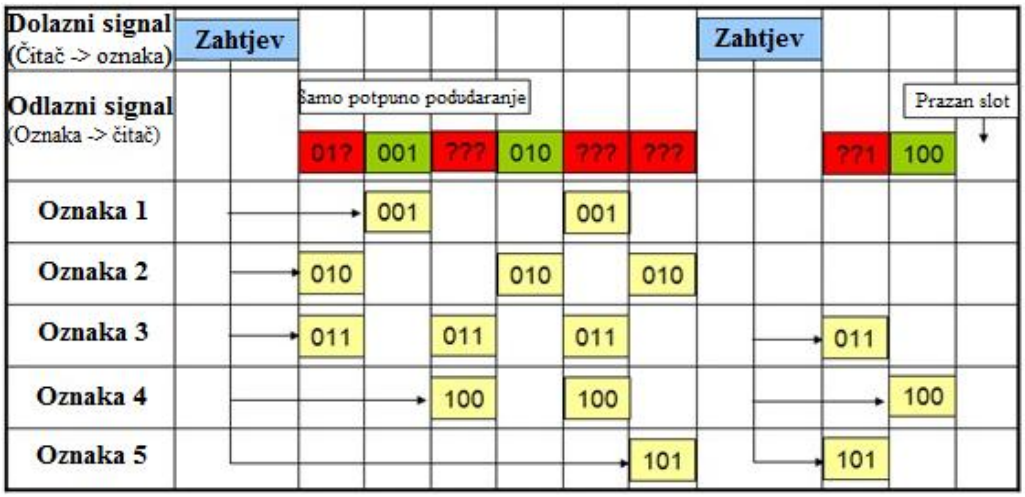
Elektronička šifra proizvoda (Electronic Product Code - EPC) je zajednička vrsta podataka koja se pohranjuje u oznake. Kada se zapiše pomoću RFID pisača, oznaka sadrži 96 - bitni niz podataka. Prvih osam bitova su zaglavlje koje definira verziju protokola. Sljedećih 28 bitova definira organizaciju koja upravlja podacima te oznake, a organizacijski broj dodijeljuje globalni EPC konzorcij. Sljedeća 24 bita su klasa objekta, definiraju vrstu proizvoda, a posljednjih 36 bitova su jedinstveni serijski broj za određenu oznaku. Posljednja dva polja su dodjeljena od strane organizacije koja je izdala oznaku. Poput usklađenog lokatora sadržaja (Uniform Resource Locator - URL), elektronička šifra proizvoda se može koristiti kao ključ u globalnoj bazi podataka za jedinstvenu identificikaciju određenog proizvoda.

Često više oznaka odgovori čitaču oznaka jer se mnogi pojedinačni proizvodi s oznakama mogu isporučiti u zajedničkom okviru ili paleti. Dvije vrste protokola se koriste za izoliranje određene oznake, čime se njezini podaci čitaju između mnogih sličnih oznaka. U slotted Aloha sustavu, čitač emitira pokretačku naredbu i parametre koje oznake pojedinačno koriste da pseudo - slučajno odgode svoje odgovore. Kada koristi protokol "prilagodljivo binarno stablo", čitač šalje pokretački simbol, a zatim prenosi jedan dio osobnih podataka istovremeno na koje samo oznake s odgovarajućim bitovima odgovore te na kraju samo jedna oznaka odgovara kompletnim identifikacijskim nizom.

RFID oznake se lako stavljaju ili ugrađuju u druge objekte. Na primjer, 2009. su istraživači na Sveučilištu u Bristolu uspješno zalijepili RFID mikro-transponder na žive mrave za praćenje njihovog ponašanja.

Najmanji RFID čip je Hitachiev, dimenzija 0.05 mm × 0.05 mm. Proizvodnja je omogućena pomoću procesa silicija na izolatoru (Silicon on insulator - SOI). Ovi čipovi veličine prašine

mogu pohraniti 38-znamenkasti broj pomoću 128 bitne memorije samo za čitanje (Read-only memory - ROM).



Slika 2.1.1. Slotted Aloha protokol [2]

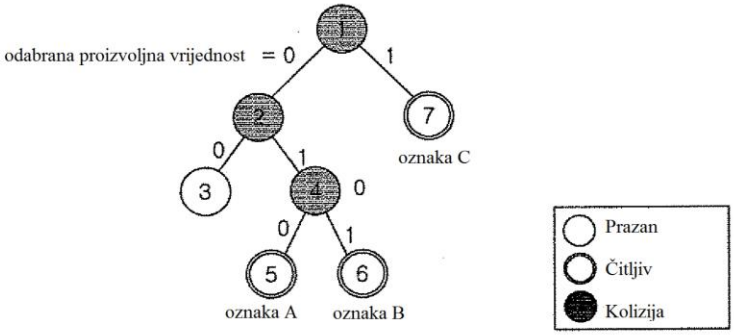


FIG. 2

period čitanja	brojač napretka utora	brojač dodijeljenog utora			brojač završetka utora	povratna informacija čitača	primjedba
		oznaka A	oznaka B	oznaka C	čitač		
1	0	0	0	0	1	Kolizija	
2	0	0	0	1	2	Kolizija	
3	0	1	1	2	3	Prazno	
4	0	0	0	1	2	Kolizija	
5	0	0	1	2	3	Čitljivo	Identificirana oznaka A
6	1	0	1	2	3	Čitljivo	Identificirana oznaka B
7	2	0	1	2	3	Čitljivo	Identificirana oznaka C
8	3	0	1	2	3	ništa	Završetak identifikacije

Slika 2.1.2. Protokol binarnog stabla [3]

2.2. Bežične senzorske mreže (WSN)

Nedavni tehnološki napredak u integriranim krugovima malih snaga i bežičnoj komunikaciji povećao je dostupnost učinkovitih, isplativih minijaturnih uređaja za primjenu u aplikacijama na daljinu. Ovi faktori su poboljšali održivost korištenja senzorskih mreža koja se sastoji od velikog broja inteligentnih senzora koji omogućuju prikupljanje, obradu i analizu vrijednih informacija koje se prikupljaju u različitim okruženjima.

Aktivni RFID ima sličnu upotrebu kao i WSN čvorovi donjeg kraja s ograničenim mogućnostima obrade i skladištenja. Znanstveni izazovi koji se moraju prevladati kako bi se ostvario ogroman potencijal WSN-a su značajni i multidisciplinarni u prirodi. Podaci sa senzora se dijele između čvorova senzora i šalju na distribuirani ili centralizirani sustav za analizu. Komponente koje čine WSN prateću mrežu uključuju:

1.WSN hardware : obično čvor (WSN jezgreni hardware) sadrži senzorska sučelja, procesne jedinice, primopredajne jedinice i napajanje. Najčešće se sastoji od više A/D pretvarača za senzorska sučelja i više modernih senzorskih čvorova koji mogu komunicirati koristeći jedan frekvencijski pojas.

2.WSN komunikacijski stog : Čvorovi su najčešće razmješteni na ad hoc način za većinu aplikacija. Izrada odgovarajuće topologije, usmjeravanje i MAC (Media Access Control) sloj su kritični za skalabilnost i dugovječnost razmještene mreže. Čvorovi u WSN-u moraju komunicirati među sobom za prijenos podataka u jednom ili više skokova prema baznoj stanici. Problemi poput ispadanja čvorova, posljedično degradiranih mreža su česti. Komunikacijski stog na vrhu čvorova trebao bi imati mogućnost komunikacije s vanjskim svijetom putem Interneta te djelovati kao prolaz prema WSN podmreži i Internetu.

3.Middleware : Mehanizam koji kombinira računalnu infrastrukturu sa uslužno orijentiranom arhitekturom (Service-oriented architecture - SOA) i senzorskim mrežama za pružanje pristupa prema heterogenim senzorskim resursima u svrhu implementacije neovisnog djelovanja. To se temelji na ideji izoliranja resursa koje može koristiti više aplikacija. Potreban je platformno neovisan middleware za razvoj senzorskih aplikacija, kao što je Open Sensor Web Architecture (OSWA). OSWA je izgrađena na jedinstvenom nizu operacija i standardnih podataka kao što je definirano od strane Open Geospatial Consortium (OGC).

4.Sigurno prikupljanje podataka : Učinkovit i siguran način prikupljanja podataka je potreban za produljenje vijeka trajanja mreže, kao i osiguranje prikupljanja pouzdanih podataka sa senzora. Ispad čvora je zajednička karakteristika WSN-a te topologija mreže treba imati sposobnost oporavka. Osiguravanje sigurnosti je izuzetno važno jer je sustav automatski povezan s pogonima i zaštita sustava od uljeza je kritična.

2.3. Adresne sheme

Sposobnost jedinstvene identificikacije „objekata“ je ključna za uspjeh IoT mreže. Osim jedinstvene identificikacije milijarde uređaja, omogućava nam i kontrolu udaljenih uređaja putem Interneta. Najkritičnije osobine jedinstvenih adresa su: jedinstvenost, pouzdanost i skalabilnost.

Svaki element koji je već povezan i oni koji će biti povezani, moraju se prepoznati po jedinstvenoj identifikaciji, lokaciji i funkcionalnosti. Trenutni IPv4 protokol može podržati geografsko prepoznavanje skupina senzorskih uređaja, ali ne i pojedinačno. Atributi internetske mobilnosti u IPv6 protokolu mogu ublažiti neke od problema identifikacijskih uređaja. Međutim, problem stvaraju heterogena priroda bežičnih čvorova, promjenjive vrste podataka, istodobne operacije i slijevanje podataka iz uređaja.

Dosljedno funkcioniranje mreže se postiže kanaliziranjem prometa podataka posvuda i bez prestanka. TCP (Transmission Control Protocol) / IP (Internet Protocol) protokol usmjerava podatke na pouzdan i učinkovit način od izvora do odredišta, IoT-u problem predstavlja usko grlo na sučelju između pristupnog računala i bežičnih senzorskih uređaja. Skalabilnost adrese uređaja postojeće mreže mora biti održiva. Dodavanje mreža i uređaja ne smije ugroziti performanse mreže, funkcioniranje uređaja, pouzdanost podataka preko mreže ili učinkovitu upotrebu uređaja sa korisničkog sučelja.

Za rješavanje tih pitanja temeljan je sustav Uniform Resource Name (URN). URN stvara replike resursa kojima se može pristupiti putem URL-a. Uz velike količine prostornih podataka, važno je iskoristiti prednosti metapodataka za prijenos informacija iz baze podataka prema korisniku putem Interneta. IPv6 protokol je vrlo dobar izbor za jedinstveni pristup resursima i na daljinu. Za jedinstveno adresiranje kućanskih aparata planira se razviti „lagani“ IPv6.

Bežične senzorske mreže (smatrajući ih kao građevni blokovi IoT-a), koje rade na različitom stogu u odnosu na Internet, ne mogu posjedovati IPv6 stog za pojedinačno adresiranje, te će trebati podmreže s pristupnikom koji posjeduje URN. S obzirom na to, potreban je sloj za adresiranje senzorskih uređaja od strane nadležnog pristupnika. Na razini podmreže, URN za senzorske uređaje mogu biti jedinstveni identifikacijski dokumenti (ID) umjesto ljudski prihvatljivih imena kao na webu i pregledna tablica na pristupniku za adresiranje ovog uređaja. Na razini čvora svaki senzor će imati URN (brojeve) za adresiranje senzora pomoću pristupnika. Cijela mreža sada tvori povezivačku mrežu od korisnika (na visokoj razini) prema senzorima (niska razina) koja je adresirana (kroz URN), dostupna (preko URL-a) i upravljiva (kroz URC).

2.4. Pohranjivanje i analiza podataka, vizualizacija

Jedan od najvažnijih rezultata ovog područja u nastajanju je stvaranje jedinstvene količine podataka. Kritična pitanja su skladištenje, vlasništvo i istek podataka. Internet troši do 5% ukupne energije proizvedene danas, a sa ovim zahtjevima će se sigurno povećati. Pouzdanost i učinkovitost bi osigurali podatkovni centri koji rade na obnovljivoj energiji i koji su centralizirani. Podaci moraju biti pohranjeni i inteligentno korišteni za pametno praćenje i pokretanje. Važno je razviti algoritme umjetne inteligencije koji mogu biti centralizirani ili distribuirani na temelju potreba. Za razumijevanje prikupljenih podataka potreban je razvoj fuzijskih algoritama. Za postizanje automatiziranog donošenja odluka potrebni su genetski algoritmi, neuronske mreže i druge tehnike umjetne inteligencije. Ovi sustavi pokazuju osobine kao što su interoperabilnost, integracija i adaptivna komunikacija. Također imaju modularnu arhitekturu, kako u pogledu hardverskog dizajna sustava, tako i u razvoju softvera i obično su vrlo dobro prilagođeni za IoT aplikacije.

Vizualizacija je kritična za primjenu IoT-a, jer omogućuje interakciju korisnika s okolinom. Sa najnovijim dostignućima u touch screen tehnologiji, upotreba pametnih tableta i telefona je postala vrlo intuitivna. Da običan čovjek u potpunosti iskoristi IoT tehnologiju, mora se stvoriti atraktivna i jednostavno razumljiva vizualizacija. Polaganim prelaskom sa 2D na 3D ekrane, može se osigurati više smislenih informacija za korisnika. Vađenje smislene informacije iz sirovih podataka je netrivijalno. To obuhvaća otkrivanje događaja i vizualizaciju pridruženih sirovih i modeliranih podataka, sa informacijom prikazanom u skladu s potrebama krajnjeg korisnika.

3. PRIMJENA IOT TEHNOLOGIJE

Postoji nekoliko aplikacijskih domena na koje će utjecati razvoj IoT-a. Primjena se može klasificirati na temelju vrste dostupnosti mreže, pokrivenosti, razmjera, heterogenosti, uključenosti korisnika i utjecaju. Aplikacije se najčešće kategoriziraju u četiri područja primjene: Osobna i dom, poduzeće, komunalne usluge i mobilne. To je prikazano na slici 3.1. koja predstavlja osobnu i kućnu primjenu IoT-a na skali od pojedinca ili kuće, IoT poduzeća na skali zajednice, uslužni IoT na nacionalnoj ili regionalnoj razini i mobilni IoT koji se obično širi na druge domene, uglavnom zbog prirode povezanosti i razmjera. Postoji velika razlika u aplikacijama i upotrebi podataka između domena. Na primjer, osobni i kućni IoT iznosi podatke o korištenju električne energije u kući i čini ga dostupnim dobavljaču električne energije (komunalno poduzeće) koje može optimizirati ponudu i potražnju na IoT-u komunalnih usluga. Internet omogućuje razmjenu podataka između različitih pružatelja usluga što stvara višestruke poslovne mogućnosti.

3.1. Osobna, kućna i uredska primjena

Podatke prikupljene sa senzora koriste samo pojedinci koji izravno posjeduju mrežu. Obično se WiFi koristi kao okosnica koja omogućuje veću propusnost podataka (video prijenos), kao i veće stope uzorkovanja (zvuk).

Sveprisutno zdravstvo je želja u posljednja dva desetljeća, a IoT pruža savršenu platformu za ostvarenje te vizije pomoću senzora tjelesnih područja i IoT pozadine za postavljanje podataka na poslužitelje. Na primjer, pametni telefon se može koristiti za komunikaciju zajedno s nekoliko sučelja kao što je Bluetooth za povezivanje senzora za mjerenje fizioloških parametara. Do sada, postoji nekoliko aplikacija dostupnih za Apple iOS, Google Android i Windows Phone operativni sustav koji mjere razne parametre. Međutim, to se tek treba centralizirati u oblaku da bi liječnici opće prakse pristupili podacima.

Produljenje osobne tjelesne mreže je stvaranje sustava kućnog praćenja za skrb starijih osoba, koji omogućuje liječniku praćenje bolesnika i starijih osoba u njihovim domovima i time smanjivanje troškova hospitalizacije kroz rane intervencije i liječenja.

Kontrola kućne opreme kao što su klima uređaji, hladnjaci, perilice rublja, itd., omogućit će bolje upravljanje energijom. Socijalno umrežavanje će proći kroz još jednu transformaciju s milijardama međusobno povezanih objekata.

„Mreža objekata“ se odnosi na radno okruženje koje funkcionira kao poduzeće bazirano na aplikaciji. Podatke prikupljene od takvih mreža koriste samo vlasnici i podaci se mogu objaviti

selektivno. Praćenje stanja okoliša je prvi zajednički program koji se provodi za vođenje evidencije o broju putnika i upravljanju u zgradi (npr. grijanje, ventilacija, klima-heating, ventilation, and air conditioning - HVAC, rasvjeta).

Senzori su uvijek bili sastavni dio tvorničkih postavki za sigurnost, automatizaciju, kontrolu klime, itd. Taj sustav će se s vremenom zamijeniti sa bežičnim sustavom koji daje fleksibilnost u promjeni postavki kada je potrebno. To bi bila IoT podmreža posvećena održavanju tvornice.

Tablica 3.1. Aplikacijske domene pametnog okoliša [1]

	Pametni dom / ured	Pametna trgovina	Pametni grad	Pametna poljoprivreda / šuma	Pametna voda	Pametan prijevoz
Veličina mreže	mala	mala	srednja	srednja / velika	velika	velika
Broj korisnika	mali, članovi obitelji	mali, na razini zajednice	veliki, javnost	mali, zemljoposjednici	mali, vlada	veliki, javnost
Napajanje	punjiva baterija	punjiva baterija	punjiva baterija, obnovljivi izvori	obnovljivi izvori	obnovljivi izvori	punjiva baterija, obnovljivi izvori
Poveznaost s Internetom	Wifi, 3G, 4G LTE	Wifi, 3G, 4G LTE	Wifi, 3G, 4G LTE	Wifi, satelitska komunikacija	satelitska komunikacija	Wifi, satelitska komunikacija
Upravljanje podacima	lokalni server	lokalni server	dijeljeni server	lokalni, dijeljeni server	dijeljeni server	dijeljeni server
IoT uređaji	RFID, WSN	pametna trgovina	RFID, WSN	WSN	pojedinačni senzori	pojedinačni senzori, RFID, WSN
Zahtjevi propusnosti	mali	mali	veliki	srednji	srednji	srednji / veliki

Jedna od glavnih IoT aplikacija je pametan okoliš. Postoji nekoliko testnih projekata koji se provode, a mnogo toga se planira u narednim godinama. Pametan okoliš uključuje podsustave kao što je prikazano u tablici 3.1., a karakteristike iz tehnološkog stajališta su kratko navedene. Svaka od pod domena pokriva mnoge fokus grupe i podaci će se dijeliti. Aplikacije unutar urbane sredine koje mogu imati koristi od realizacije pametnih gradova prikazane su u tablici 3.2. Aplikacije su grupirane prema svojim utjecajnim mjestima. To uključuje učinak na građane s obzirom na zdravlje, prijevoz u svjetlu njegova utjecaja na mobilnost, produktivnost, zagađenja i kritične usluge u zajednici koje lokalne vlasti omogućuju gradskim stanovnicima.

Tablica 3.2. Potencijalne IoT aplikacije različitih fokus grupa [1]

Građani	
Zdravstvo	praćenje pacijenata, nadzor osoblja, sprječavanje proširivanja bolesti - zdravstveni status u realnom vremenu, prediktivne informacije za pomoć na terenu, političke odluke u pandemijskim scenarijima
Hitne službe, obrana	daljinski nadzor osoblja, upravljanje i distribucija resursa, planiranje odgovora; senzori ugrađeni u infrastrukturi zgrade za prve odgovore u hitnim slučajevima ili scenarijima katastrofe
Nadzor	praćenje tijeka gužva za upravljanje u kriznim situacijama; učinkovito korištenje javnih i maloprodajnih prostora; tijek rada u trgovačkim okruženjima
Prijevoz	
Upravljanje prometom	inteligentni prijevoz pomoću informacija u realnom vremenu i optimizacija putanje
Nadzor infrastrukture	senzori ugrađeni u infrastrukturu za praćenje strukturnog stanja i održavanje, nadzor nesreća za upravljanje incidentima i koordinaciju hitnog odgovora
Usluge	
Voda	kvaliteta vode, odvod, uporaba, distribucija, upravljanje otpadom
Upravljanje zgradama	temperatura, kontrola vlage, praćenje potrošnje energije grijanja, ventilacije i klimatizacije (HVAC)
Okoliš	onečišćenje zraka, praćenje buke, industrijski nadzor

3.2. Primjena u komunalnim i mobilnim uslugama

Podaci iz mreža u ovoj aplikacijskoj domeni su obično za optimizaciju usluga, a ne za usluge potrošača. Već se koriste od strane komunalnih poduzeća (pametna brojila u elektroprivredama) za upravljanje resursima kako bi se optimizirali troškovi u odnosu na dobit. To su vrlo opsežne mreže (najčešće propisane od strane velikih organizacija na regionalnoj i nacionalnoj razini) za praćenje kritičnih komunalnih usluga i učinkovito upravljanje resursima.

Pametna mreža i pametna mjerenja su potencijalni IoT programi koji se provode diljem svijeta. Učinkovita potrošnja energije može se postići kroz kontinuirano praćenje svake električne točke unutar kuće i korištenje ove informacije za promjenu načina upotrebe električne energije. Ova informacija na gradskoj skali se koristi za održavanje ravnoteže opterećenja unutar mreže za osiguravanje visoke kvalitete usluge.

Video bazirani IoT koji integrira obradu slike, računalnu viziju i umrežavanje razvojnih cjelina pomoći će u razvoju novog znanstveno-istraživačkog prostora na raskrižju video, infracrvenih, mikrofonskih i mrežnih tehnologija. Nadzor, najčešće korištena mrežna aplikacija kamera, pomaže pratiti mete, identifikaciju sumnjivih aktivnosti, otkrivanje prtljage i praćenje neovlaštenog pristupa. Automatska analiza ponašanja i otkrivanje događaja (kao dio sofisticirane video analize) je u povojima i otkrića se očekuju u sljedećim godinama.

Mreža za nadgledanje kvalitete vode i osiguranje pitke vode je još jedan kritični program koji bi se realizirao pomoću IoT-a. Senzori za mjerenje kritičnih parametara vode su instalirani na važnim mjestima kako bi se osigurala visoka kvaliteta opskrbe. Time se izbjegava slučajna kontaminacija između oborinske vode, pitke vode i otpadnih voda. Ista mreža se može koristiti za praćenje navodnjavanja u poljoprivrednim zemljištima. Mreža je također proširena za praćenje parametara tla što omogućava informirano donošenje odluka o poljoprivredi.

Pametni transport i pametna logistika se nalaze u zasebnoj domeni, zbog prirode dijeljenja podataka i potrebne provedbe glavne mreže. Urbani promet je glavni čimbenik u degradaciji kvalitete zraka i emisiji stakleničkih plinova. Prometna zagušenja izravno nameću značajne troškove gospodarskih i društvenih aktivnosti u većini gradova. Učinkovitost i produktivnost opskrbnog lanca ozbiljno ovisi o ovim zagušenjima koji uzrokuju kašnjenja tereta i nesupjehe planiranih isporuka. Dinamičke informacije prometa će utjecati na kretanje tereta, omogućiti bolje planiranje i poboljšano raspoređivanje. Transportni IoT će omogućiti korištenje velikih WSN-ova za trenutno praćenje trajanja putovanja, izbor rute od polazišta do odredišta, duljine redova, zagađenje zraka i emisije buke. IoT će vjerojatno zamijeniti informacije o stanju u prometu koje se nalaze u postojećim senzorskim mrežama induktivne petlje detektora vozila na raskrižjima postojećih sustava kontrole prometa. Također će poduprijeti razvoj modela baziranih

na scenarijima za planiranje i projektiranje ublažavanja planova, kao i poboljšane algoritme za kontrolu urbanog prometa, uključujući i više-objektivne sustave kontrole. U kombinaciji s podacima prikupljenim iz sustava kontrole prometa, važeće i relevantne informacije o stanju u prometu se mogu predstaviti putnicima.

Rasprostranjenost uređaja Bluetooth tehnologije (BT) odražava trenutno IoT prodiranje u niz digitalnih proizvoda, kao što su mobilni telefoni, automobilski uređaji slobodnih ruku (hands-free), navigacijski sustavi, itd. BT uređaji emitiraju signale s jedinstvenim identifikacijskim brojem pristupa mediju (MAC-ID) koji može očitati BT senzor unutar područja pokrivanja. Čitači postavljeni na različitim mjestima se mogu upotrijebiti za identifikaciju kretanja uređaja. Dopunjena drugim izvorima podataka, kao što su prometni signali ili autobusni Globalni pozicijski sustav (Global Positioning System – GPS), istraživački problemi koji se mogu riješiti uključuju vrijeme putovanja vozila na autocestama i arterijskim ulicama, dinamičke (vremenski ovisne) matrice na mreži. Postoji mnogo problema privatnosti i digitalno zaboravljanje je domena u nastajanju gdje se rješava pitanje privatnosti.

Druga važna primjena u mobilnoj IoT domeni je učinkovito upravljanje logistikom. To uključuje praćenje predmeta koji se prevoze i učinkovito planiranje prijevoza. Praćenje predmeta se provodi lokalno, npr., u kamionu se replicira domena poduzeća, ali prometno planiranje se provodi pomoću IoT mreže velikih razmjera.

4. MEĐUPROGRAM IOT-A

Međuprogram (middleware) je sučelje između hardverskog sloja i aplikacijskog sloja koje je odgovorno za interakciju s uređajima i upravljanje informacijama. Uloga međuprograma je predstavljati jedinstveni model programiranja za interakciju s uređajima. Međuprogram je zadužen za maskiranje heterogenosti i distribucijskih problema s kojima se susrećemo u interakciji s uređajima.

IoT ima slojevitu arhitekturu dizajniranu da odgovori zahtjevima industrije, poduzeća i društva. Slika 4.1.1. prikazuje generičku slojevitu arhitekturu IoT-a koja se sastoji od pet slojeva:

1. sloj Edge tehnologije

Hardverski sloj koji se sastoji od ugrađenih sustava, RFID oznaka, senzorskih mreža i svih ostalih senzora u različitim oblicima. Ovaj hardverski sloj može obavljati više funkcija, kao što su prikupljanje informacija iz sustava ili okoliša, obrada podataka i prateća komunikacija.

2. sloj pristupnog gatewaya

Ovaj sloj se bavi rukovanjem podacima, odgovoran je za usluge objavljivanja i pretplaćivanja koje pružaju stvari, usmjeravanje poruka i održavanje komunikacije između platformi.

3. sloj međuprograma

Ovaj sloj ima neke kritične funkcionalnosti, kao što su agregiranja i filtriranja primljenih podataka iz hardverskih uređaja, otkrivanje informacija i pružanje kontrole pristupa uređajima za aplikacije.

4. aplikacijski sloj

Ovaj sloj je odgovoran za pružanje raznih usluga aplikacija. Te usluge se pružaju putem sloja međuprograma različitim aplikacijama i korisnicima u IoT-baziranim sustavima. Aplikacijske usluge se mogu koristiti u različitim industrijama (logistika, maloprodaja, zdravstvo, itd.).

4.1. IoT bazirani međuprogram

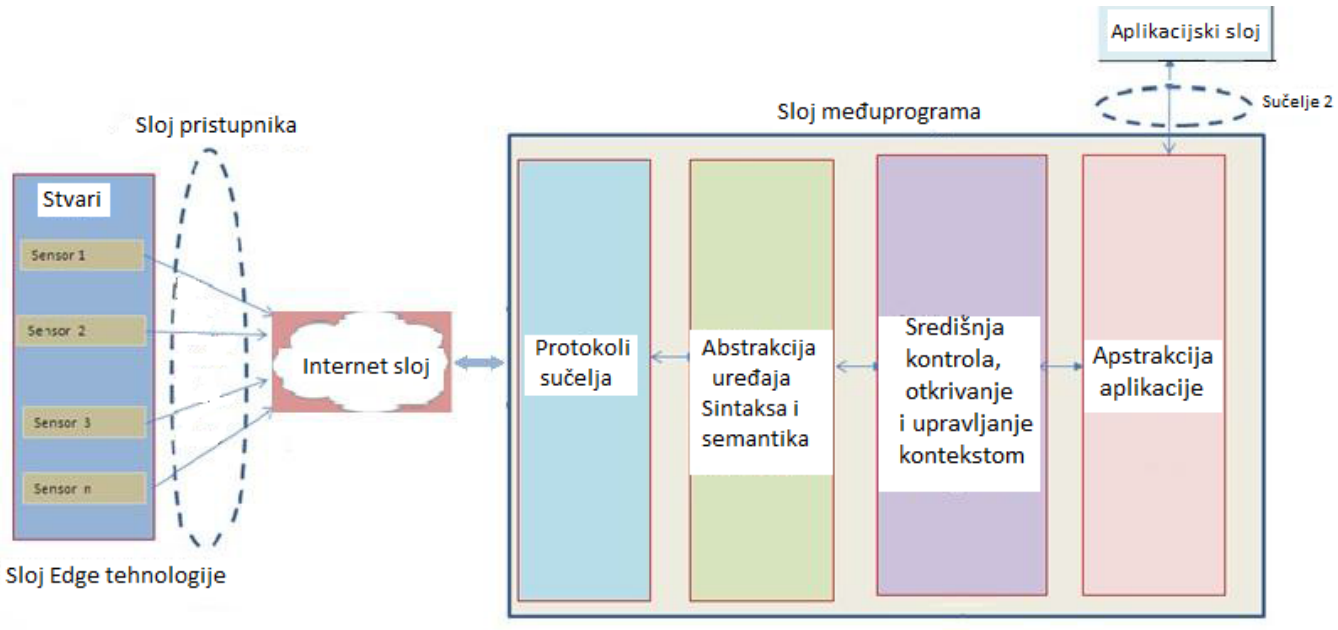
Potrebna funkcionalnost međuprograma za upravljanje interakcijom s različitim uređajima dijeli se na četiri funkcionalne komponente: protokole sučelja, apstrakciju uređaja, središnju kontrolu, otkrivanje i upravljanje kontekstom i apstrakciju zahtjeva.

Komponenta protokola sučelja definira protokole za razmjenu podataka između različitih mreža koje mogu raditi na temelju različitih komunikacijskih protokola, kako bi se omogućila tehnička interoperabilnost. Ova komponenta je odgovorna za rukovanje osnovnim povezivanjima u fizičkim i podatkovnim vezama, mreže, transport, a ponekad i aplikacijski sloj TCP / IP stoga.

Da bi se nosili sa heterogenosti uređaja, možemo koristiti modul za svaki uređaj kako bi preveli protokol koji podržava uređaj na zajednički protokol. Ovaj modul može biti postavljen ili na strani uređaja ili na strani međuprograma. Ako želimo imati izravnu interakciju s uređajima, treba staviti modul na stranu međuprograma, također, uređaji obično imaju ograničenu sposobnost računalnih procesa. U slučaju neizravne interakcije s uređajima možemo razviti posrednički modul između međuprograma i uređaja. Komponenta protokola sučelja je odgovorna da međuprogram podržava izravne i neizravne interakcije.

Apstrakcija uređaja je komponenta odgovorna za pružanje apstraktnog oblika koji olakšava interakciju aplikacijskih komponenti s uređajima.
Sintaktička interoperabilnost je povezana s formatima podataka. Poruke koje se prenose komunikacijskim protokolima moraju imati dobro definiranu sintaksu i format kodiranja, a to se može predstaviti pomoću visoko razinskih prijenosnih sintaksi, kao što su HTML (HyperText Markup Language) i XML (EXtensible Markup Language).
Semantička interoperabilnost je obično povezana sa značenjem sadržaja poruke koja je razumljiva čovjeku. Interoperabilnost na ovoj razini znači da postoji zajedničko razumijevanje među ljudima o značenju sadržaja (podataka) koji se razmjenjuje među njima. Budući da komponenta apstrakcije uređaja ne komunicira izravno s ljudima, semantička interoperabilnost u kontekstu apstrakcije uređaja je zadužena za pružanje zajedničkog razumijevanja za aplikacije. Komponenta apstrakcije uređaja (Device Abstraction – DA) osigurava dvije opće funkcionalnosti: naređuje uređajima obavljanje neke funkcije te definira i konfigurira profile uređaja za web usluge (Devices Profile for Web Services - DPWS).
Kontekst karakterizira stanje subjekta, što može biti mjesto, osoba ili stvar koja je bitna za korisnika, aplikaciju i njihove interakcije. Funkcionalna komponenta središnje kontrole, otkrivanja i upravljanja kontekstom (Central control, Context detection & Management - CCM) je odgovorna za podršku kontekstno svjesnog računalstva što je računalni stil koji uzima u obzir kontekst entiteta koji su u interakciji sa sustavom. Međuprogram IoT sustava mora biti kontekstno svjestan da bi radio u pametnim sredinama.
Svijest o kontekstu uključuje dvije funkcionalnosti: otkrivanje konteksta, koje se sastoji od prikupljanja podataka iz izvora i odabira informacije koja može imati utjecaj na proračun; obrada konteksta, upotreba prikupljenih podataka za obavljanje zadatka ili donošenje odluke.

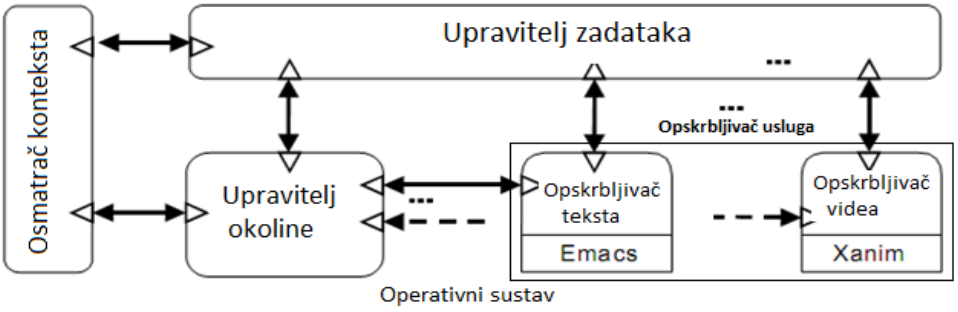
Apstrakcija aplikacije je funkcionalna komponenta koja pruža sučelje za aplikacije visoke razine i krajnjim korisnicima interakciju s uređajima.



Slika 4.1.1. Funkcionalne komponente međuprograma za IoT sustave [4]

Sada slijedi kratki opis međuprograma, AURA-e jer ima naglasak na izradu i manipulaciju prikupljenih podataka iz uređaja, a cilj je pružanje jednostavne konfiguracije i implementacije za krajnjeg korisnika i razvojne programere. Da se ostvari taj cilj, potrebno je olakšano okupljanje manipulacije podataka, a AURA je jedan od međuprograma koji razmatra manipulaciju podacima. Hydra je jedan od najpopularnijih i najbolje dokumentiranh međuprograma. TinyDB je usredotočen na prikupljanje podataka iz uređaja, a u IoT sustavu moramo prikupiti podatke iz okoline kroz različite uređaje. WiseMID je jedini međuprogram među opisanim koji je specifičan po uštedi energije.

AURA je međuprogram koji podržava interakcije s kompleksnim uređajima (npr. digitalni fotoaparati, dlanovnici, itd), kao i njihovu integraciju. AURA definira proxy, nazvan osobna aura koja omogućuje korisnicima da koriste uređaj neovisno o njihovim fizičkim lokacijama. Slika 4.1.2. prikazuje glavne komponente AURA okvirne arhitekture i njihove interakcije.



Slika 4.1.2. Komponente AURA okvirne arhitekture [4]

4 glavne komponente AURA-e su:

1. upravitelj zadacima

Ova komponenta ima za cilj pružiti minimalnu distrakciju za krajnje korisnike u slučaju bilo kakve promjene u okruženju sustava, kao što su promjena položaja ili operativnog sustava krajnjeg korisnika. Ova komponenta pruža platformno neovisan opis zadataka krajnjim korisnicima, kao što su produciranje videa i uređivanje teksta, što su apstraktne usluge. Apstrakcija usluge omogućuje krajnjem korisniku da zahtjeva izvršenje zadatka na isti način na različitim platformama. Na primjer, kako bi se omogućilo uređivanje teksta krajnjem korisniku u UNIX okruženju, AURA koristi Emacs, dok u Windows okruženju AURA koristi Microsoft Word.

2. opskrbljivač usluga (Service supplier - SS)

Kako bi odgovorila na zahtjeve krajnjeg korisnika, ova komponenta implementira usluge sređivajući zadatke. Uređivač teksta može mapirati korisnički zahtjev za uređivanje u Notepad , Emacs ili Microsoft Word.

3. osmatrač konteksta (Context Observer - CO)

Ova komponenta prikuplja informacije o fizičkom smislu i sukladno aktivira događaj za upravitelja okoline i zadataka. Informacija je o lokaciji, djelatnosti, autentifikaciji krajnjih korisnika. Promatrač konteksta može podržati različite stupnjeve složenosti ovisno o različitim uređajima raspoređenim u različitim okruženjima. Ako uređaj ima više mogućnosti, CO komponenta može postati složenija.

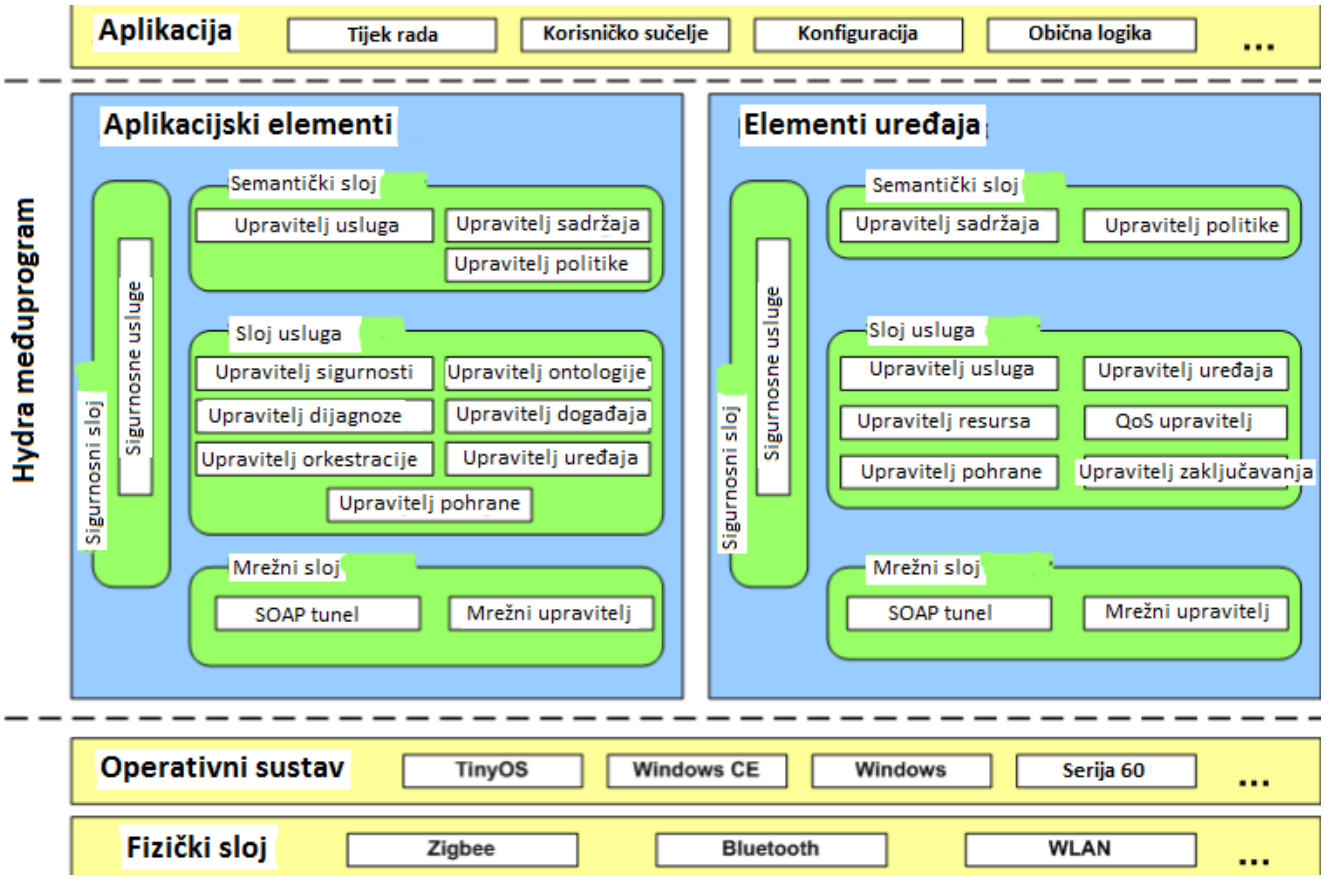
4. upravitelj okoline (Environment Manager - EM)

Ova komponenta je pristupnik prema okolini. Ona zna koje usluge dobavljači na raspolaganju pružaju i gdje usluge mogu biti razmještene. Ako krajnji korisnik traži datoteku, EM komponenta podržava različite načine pristupa datoteci, na primjer pomoću FTP-a (File Transfer Protocol). Kako bi se korisnicima olakšao pristup datotekama, ova komponenta oblaže detaljne informacije o pristupu datotekama u distribuiranom okruženju.

Promjenom položaja krajnjeg korisnika od strane Upravitelja zadataka, može se promjeniti raspoređivanje dobavljača na novoj lokaciji. Ako korisnik prestane raditi na datoteci sa uređivačem teksta na stolnom računalu i želi raditi na datoteci putem iPad-a, sustav je odgovoran za obradu ove promjene. AURA koristi četiri konektora da sakrije detalje distribucije i heterogenost usluga dobavljača: između prizme i proizvoljnog dobavljača, između osmatrača konteksta i upravitelja okoline, između prizme i upravitelja okoline, između osmatrača konteksta

i prizme. Svaki od tih priključaka koristi poseban protokol ovisno o vrstama komponenti na koje se povezuju. Mogu imati mnoge implementacije da podrže određene mehanizme interakcije niske razine.

Hydra je poznati međuprogramski okvir za IoT baziran sustav. Ovaj međuprogram pokriva gotovo sve funkcionalne komponente. Kako je Hydra SOA-bazirani međuprogram, podržava mnoge potrebne funkcionalnosti za podršku IoT sustava. Hydra međuprogram je inteligentan software koji se nalazi između aplikacije i operativnog sustava za obradu različitih zadataka na troškovno učinkovit način. Ovaj međuprogram pruža web uslugu sučelja za interakciju s fizičkim uređajima, pogonima, senzorima ili podsustavsima, bez obzira na njihove tehnologije mrežnih sučelja, npr. Bluetooth, RF, RFID, WiFi.
Ovaj međuprogram je dizajniran kako bi olakšao interakciju s uređajima apstrahiranjem iz detaljnih informacija o tim uređajima i njihovim mrežama. Hydra smatra svaki uređaj uslugom. Ona pruža inteligentni sloj usluga koji omogućuje krajnjim korisnicima interakciju s tim uređajima, bez suočavanja s komunikacijskim tehnologijama koje su podržane od strane uređaja.



Slika 4.1.3. Komponente izvan i unutar Hydra međuprograma [4]

TinyDB međuprogram je prvi projekt koji predlaže ideju sažimanja uređaja. TinyDB omogućuje krajnjim korisnicima interakciju s uređajima bez uvida u detalje specifikacije uređaja, kao što su komunikacijski protokoli koje podržavaju ti uređaji.
TinyDB pruža jezik specifične domene (Domain Specific Language - DSL) krajnjim korisnicima za interakciju s uređajima. Njegov DSL je upitni jezik koji podržava izbor, pridruživanje, projekcije i agregacije za rad s ugrađenim senzorskim okruženjem. DSL omogućuje krajnjem korisniku informacije o vremenu, mjestu, vrsti i načinu uzimanja uzoraka u ugrađenom senzorskom okruženju. TinyDB podržava sljedeće vrste upita:

Prateći upiti koji traže vrijednost jednog ili više atributa periodično i kontinuirano, kao što je izvještaj o temperaturi skladišta svakih sat vremena.
Upiti o stanju mreže pružaju informacije o samoj mreži. Odabir susjednih čvorova, trajanje baterije veće od praga.
Istraživački upit pokazuje status određenog čvora ili skupa čvorova u određenom trenutku, kao na primjer odabir temperature senzora sa istom specifičnom identifikacijom.
Pokretački upit se može koristiti za zahtijevanje fizičkog djelovanja. Na primjer, krajnji korisnik sustava želi isključiti ventilator u sobi kada je temperatura u prostoriji niža od praga.

WISeMid je energetski svjesni međuprogram za integriranje bežičnih senzorskih mreža i Interneta. U IoT baziranom sustavu je ušteda energije u interakciji među uređajima izuzetno važna jer oni obično imaju ograničene dobavljače energije. IoT sustav se također temelji na IP komunikaciji. WISeMid je usredotočen na integriranje Interneta i WSN-a na aplikacijskoj razini. Taj međuprogram predlaže nekoliko mehanizama uštede energije, kao što su:

1. Usluga sakupljanja
Cilj usluge sakupljanja podataka je prikupljanje korelacijskih ili redundantnih podataka, te smanjenje ukupnog broja prenesenih podataka u mreži. Na taj način se može smanjiti mrežni promet i uštedjeti energija manjim brojem interakcija s uređajima. U ovoj usluzi korisnik šalje jedan zahtjev i dobiva odgovor temeljen na prikupljanju posljednjih vrijednosti traženih uređaja. Na taj način se smanjuje broj transakcija i uštedi energija.

2. Prekid skladištenja odgovora
Ova usluga prestane slati iste poruke s istim parametrima. Na primjer, ako su senzorski podaci uređaja fiksni za određeni vremenski period, može se poslati samo jedan zahtjev razmatranom uređaju, a zatim upotrijebiti poruku odgovora za odgovor na sve istovrsne upite koji stignu u tom razdoblju. Dakle, WISeMid sprječava sustavu dobivanje informacija sa senzora, sve dok su podaci još uvijek aktualni.

3. Pretvorbe veličina poruka

Ova usluga smanjuje veličinu poruka u IoT sustavu. Na primjer, ako smo odredili vrstu podataka cijeli broj (Integer) za područje koje dobiva brojčanu vrijednost 1, mnogi bajtovi se nepotrebno koriste. Za sačuvanje bajtova, format se može pretvoriti iz Integer u Short. WISeMid uklanja nepotrebne bajtove s poruka.

4. Prizivanje asinhronih obrazaca

Ova usluga nudi četiri uzorka za obradu zahtjeva krajnjeg korisnika na asinkroni način. Ovi obrasci spriječavaju traćenje vremena sustava s blokiranjem, kada zahtjevi mogu biti obrađeni na asinkroni način. To su sljedeći obrasci: Fire and forget: Ovaj uzorak podržava jednosmjerne operacije, koje nemaju povratne vrijednosti i iznimke pogreške. Ovaj obrazac ne može prijaviti bilo kakve pogreške krajnjem korisniku, kada dođe do pogreške prilikom slanja ili prizivanja udaljene usluge.

Sinkronizacija s poslužitelja: Ovaj obrazac se koristi kada želimo biti sigurni da je zahtjev zaprimljen od strane poslužitelja, čak i ako zahtjev nema iznimki ili povratne vrijednosti. U tom slučaju, usluga poziva davatelja usluga, a zatim čeka potvrdnu poruku davatelja usluga. Ovaj obrazac se koristi u slučaju kada se usluga treba pozvati prije drugih usluga.

Anketa: Ovaj obrazac se temelji na upitu i operacijama odgovora. Provjerava je li stigao asinkroni odgovor, a ako je tako, dobiva povratnu vrijednost.

Rezultat povratnog poziva: Ovaj obrazac može izazvati događaj na strani krajnjeg korisnika kada traženi rezultat postane dostupan.

WISeMid koristi jezik definicije sučelja (Interface Definition Language - IDL) kako bi opisao usluge u ovom međuprogramu. IDL je jedinstveni jezik za opisivanje usluga bez obzira gdje se (Internet ili WSN) ili koji se provedbeni jezik koristi. IDL sadrži modul (paket) koji je kontejner za određivanje usluga sučelja. Svaka usluga sučelja uključuje ime i operaciju koju može podržati. Svaka operacija sadrži vrste ulazno / izlaznih parametara. Na slici 4.1.4. se nalazi WISeMid arhitektura koja je podijeljena na sljedeći način:

Sloj uobičajenih usluga

Ovaj sloj sadrži opće usluge, koje nisu za određene aplikacijske domene. To uključuje sljedeće usluge: Agregacija senzora podataka, definiranje grupa u WSN-u, imenovanje za pohranu potrebnih podataka za pristup usluzi.

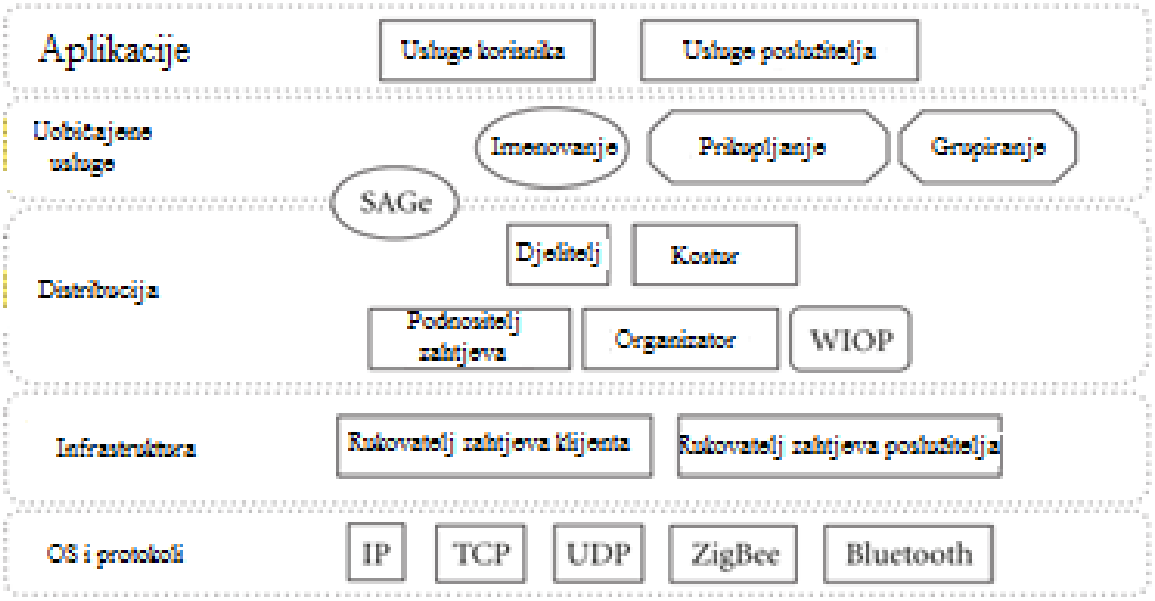
Distribucijski sloj

Ovaj sloj definira potrebne komponente za korištenje usluge. Na primjer, Podnositelj zahtjeva (Requestor) je komponenta koja omogućuje daljinsko pozivanje s parametrima, kao što su, npr.

daljinska usluga lociranja, naziv usluge i argumenti na strani klijenta. WISeMid koristi WISeMid Inter-ORB Protocol (WIOP) za obavljanje interakcija između zahtjeva i odgovora.

Sloj infrastrukture

Ovaj sloj se sastoji od Rukovatelja zahtjeva poslužitelja i Rukovatelja zahtjeva klijenta. Ovi rukovatelji omogućuju mrežnu komunikaciju za interakciju s uređajima.



Slika 4.1.4. WISeMid arhitektura [4]

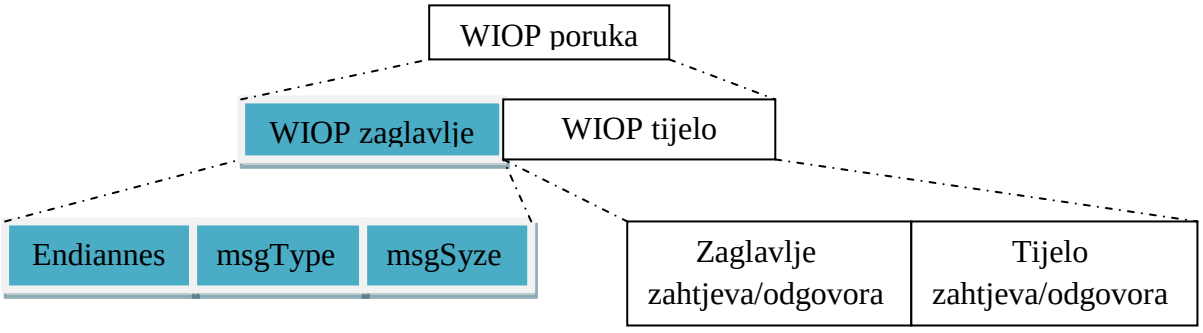
4.2. WIOP protokol i usporedba međuprograma

WIOP protokol definira format poruke zahtjeva ili odgovora između klijenta i poslužitelja. Svaka poruka se sastoji od zaglavlja i tijela. Postoje dvije verzije WIOP-a:

1) WIOPi podržava komunikaciju putem Interneta

2) WIOPs podržava komunikaciju u Bežičnoj senzorskoj mreži (WSN)

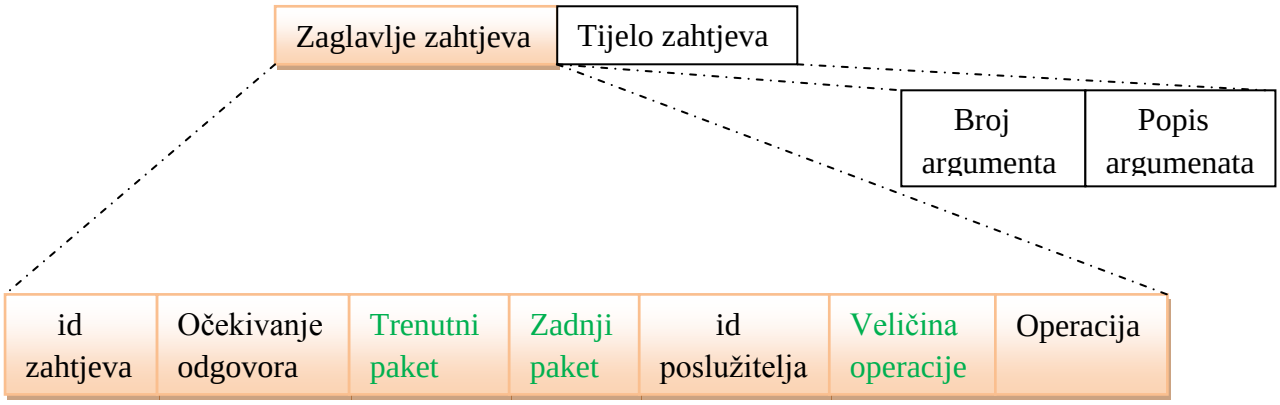
Slika 4.2.1. prikazuje WIOP zaglavlje koje ima tri polja. Polje msgType pokazuje je li poruka zahtjev ili odgovor.



Slika 4.2.1. WIOP poruka [4]

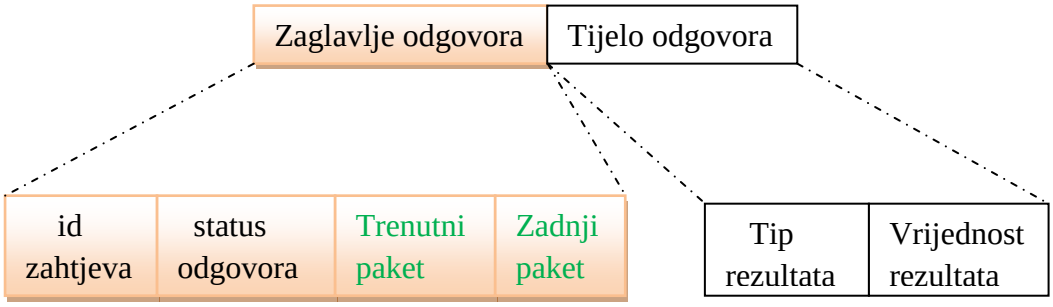
WIOP tijelo se može sastojati od poruke zahtjeva ili odgovora s vlastitim tijelom i zaglavljem.

Slika 4.2.2. prikazuje WIOP poruku zahtjeva. Polja sa zelenim slovima se koriste samo u WIOPs verziji, a ostala polja su uobičajena u obje WIOP verzije.
Polje Odg pokazuje očekuje li zahtjev odgovor ili ne. Definiranjem pet operacija, možemo imati pristup ili koristiti uslugu i registrirati usluge u WISeMID uslugu imenovanja. Operacije definirane u opr. području su: Bind za registriranje usluga po nazivu i povezivanje ih s imenom, Lookup za vraćanje oznaka povezanih s nazivom usluge, Rebind za zamjenu oznake koja je povezana s uslugom, Unbind za odjavljivanje naziva usluge, List daje popis svih registriranih usluga.



Slika 4.2.2. WIOP poruka zahtjeva [4]

Slika 4.2.3. prikazuje poruku odgovora, u kojem su polja sa zelenim slovima za WIOPs verzije, a ostatak za obje verzije. Za označavanje na koji se zahtjev odnosi adresa odgovora, može se koristiti id zahtjeva. Status odgovora ukazuje je li došlo do iznimke.



Slika 4.2.3. WIOP poruka odgovora [4]

AURA može promijeniti svoju konfiguraciju automatski kada se promjene korisnički zadaci ili okoliš. AURA je osmišljena kako bi pružila platformno-neovisan opis korisničkih zadataka što

omogućava korisniku upotrebu različitih aplikacija na različitim mjestima bez promjene konfiguracije. Tehnički detalji za interakciju sa fizičkim uređajima su izvan opsega AURA projekta.

Hydra omogućuje apstrakciju nad uređajima tako da krajnji korisnik ne treba znati detaljne informacije za konfiguriranje uređaja. Štoviše, Hydra olakšava proces implementacije pružajući sučelje za interakciju s uređajima koji se smatraju kao davatelji usluga u vrijeme njihova djelovanja. Za uređaje koji nemaju dovoljno računalne snage da bi bili davatelji usluga, Hydra koristi proxy koji omogućava uređajima interakciju s Hydra međuprogramom preko IP protokola.

TinyDB je definiran za upotrebu zajedno s TinyOS-om, što je softverski paket. To je osmišljeno kako bi se olakšao pristup najnižoj razini hardvera na energetski učinkovit način. TinyDB podržava samo TinyOS-bazirane uređaje. Krajnji korisnik mora znati specifikacije uređaja prije rada s uređajima u TinyDB-u.

WISeMid se fokusira na integriranje Interneta i bežičnih mreža senzora na razini usluga pružanjem transparentnosti pristupa, lokacije i tehnologije. Davanjem ovih mogućnosti, međuprogram može pružiti jednostavnost implementacije jer nam ne trebaju detaljne informacije kao što je adresa senzora za implementaciju usluge.

Tablica 4.2.1. Funkcionalne komponente pojedinih međuprograma [4]

Funkcionalne komponente	Aura	Hydra	TinyDB	WISeMid
Apstrakcija aplikacije	✓	✓	×	✓
Središnja kontrola, upravljanje i detekcija sadržaja	✓	✓	×	✓
Apstrakcija uređaja	×	✓	✓	×
Protokol sučelja	×	✓	✓	✓

5. IOT BAZIRAN NA „OBLACIMA“

IoT vizija se može promatrati iz dvije perspektive – internetski bazirane i objektno bazirane. Internetski bazirana arhitektura uključuje internetske usluge kao glavni fokus dok se podaci prikupljaju sa objekata. U objektno baziranoj arhitekturi, pametni objekti su u središtu pozornosti. U ovom poglavlju analizirat će se internetski bazirani pristup. Konceptualna razvojna cjelina koja integrira sveprisutne senzorske uređaja i aplikacije prikazana je na slici 5.1. Za ostvarenje punog potencijala računarstva u oblacima, kao i sveprisutnih očitavanja, najboljom se čini kombinacija razvojne cjeline s oblakom u središtu. To ne daje samo fleksibilnost dijeljenja povezanih troškova na najlogičniji način, već je također vrlo prilagodljivo. Pružatelji usluga očitavanja mogu pridružiti mrežu i ponuditi svoje podatke pomoću oblaka za pohranu; programeri analitičkih alata mogu pružiti svoje softverske alate; stručnjaci umjetne inteligencije mogu dati svoje podatke i alate strojnog učenja korisnih za pretvorbu podataka u znanje, a računalni grafički dizajneri mogu ponuditi razne vizualizacijske alate. Računarstvo u oblacima može ponuditi te usluge kao infrastrukture, platforme ili softver, gdje se puni potencijal ljudske kreativnosti može iskoristiti upotrebom navedenih usluga. Generirani podaci, korišteni alati i stvorena vizualizacija nestaju u pozadini, čime se ostvaruje puni potencijal IoT-a u raznim područjima primjene. Kao što se može vidjeti na slici 5.1., oblak integrira sve krajeve sveprisutnog računarstva pružajući skalabilnu pohranu, računanja vremena i druge alate za izgradnju novih poduzeća. U ovom poglavlju pisat će se o oblak platformi pomoću Manjrasoft Aneka i Microsoft Azure platforme za prikaz cloud integracije paradigmi pohrane, računanja i vizualizacije. Uvodi se važno područje interakcije između oblaka koje je korisno za kombiniranje javnog i privatnog oblaka pomoću Aneke. Ova interakcija je kritična programerima aplikacija kako bi donijeli informacije koje se očitavaju, algoritme za analizu i vizualizaciju u jednoj razvojnoj cjelini.

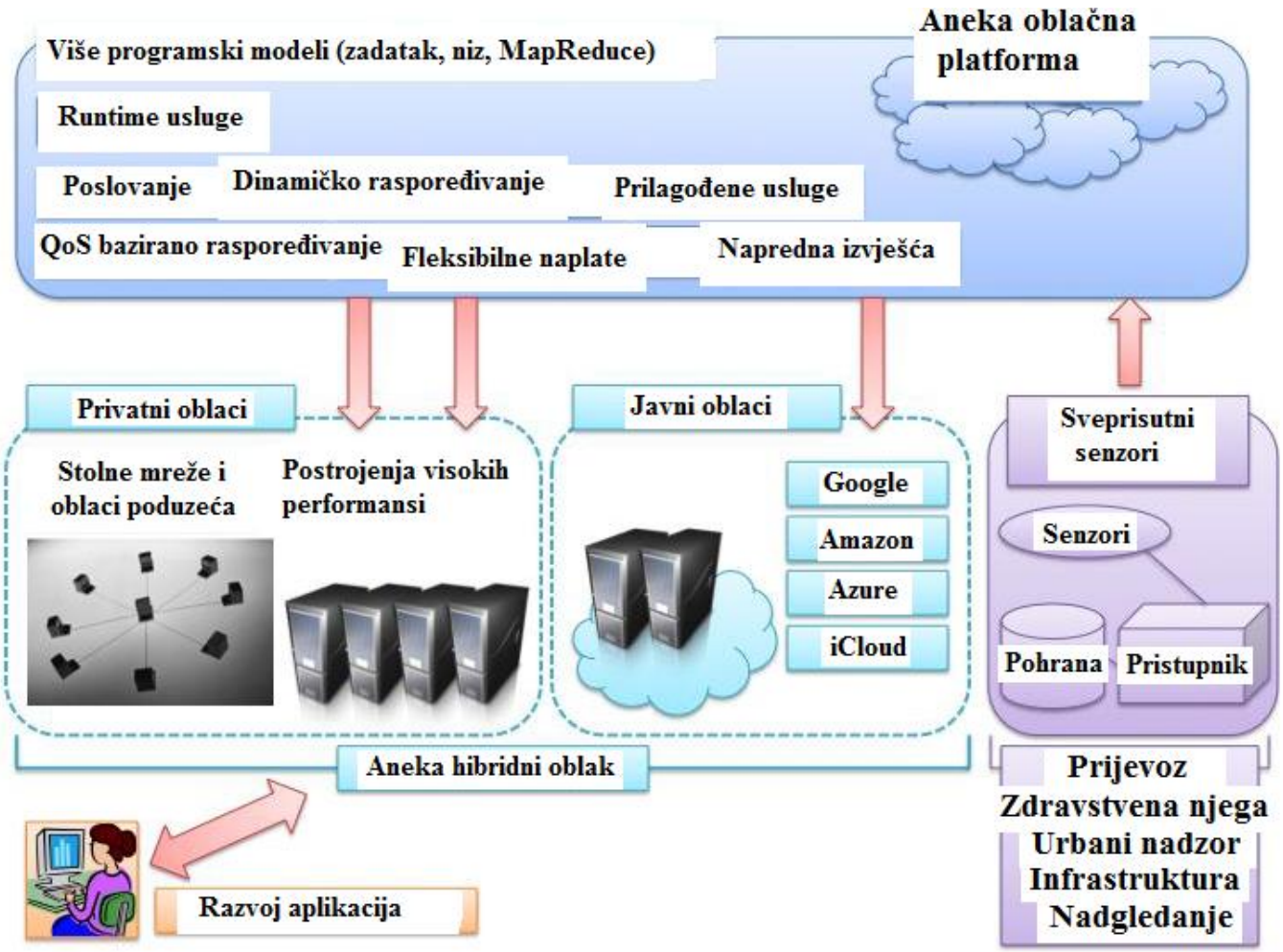
Slika 5.1. Konceptualna IoT razvojna cjelina s Računarstvom u oblacima u središtu [1]

5.1. Aneka platforma računarstva u oblacima

Aneka je .NET bazirana platforma kao usluga (Platform as a service - PaaS), tj. razvojna aplikacija, koja može iskoristiti resurse za pohranu i izračun javnih i privatnih oblaka. Nudi okruženje određenog trajanja i skup aplikacijskih programskih sučelja (Application programming interface - API) koji omogućavaju programerima da izgrade prilagođene aplikacije pomoću višestrukih programskih modela kao što su programiranje zadataka, programiranje nizova i MapReduce programiranje. Aneka pruža niz usluga koje omogućuju korisnicima kontrolu, auto skaliranje, rezerviranje, nadzor i račun korisnika za resurse koje koriste njihove aplikacije. U kontekstu aplikacije pametnog okoliša, Aneka PaaS ima još jednu važnu karakteristiku: podržava dodjele sredstava na javnim oblacima kao što su Microsoft Azure, Amazon EC2 i GoGrid te također iskorištavanje sredstava privatnih oblaka u rasponu od stolnih računala do virtualnih podatkovnih centara. Pregled Anek PaaS-a je prikazan na slici 5.1.1. Za programere aplikacija, oblak usluga, kao i podaci sveprisutnih senzora su skriveni i oni se pružaju kao usluge po cijeni od strane Aneka alata za rezervaciju.

Automatsko upravljanje oblacima za pružanje i isporuku IoT usluge kao Software kao usluga (Software as a service – SaaS) aplikacije će biti integrirajuća platforma budućeg Interneta. Postoji potreba za stvaranjem infrastrukture za dijeljenje podataka i usluga koja se može koristiti za rješavanje više različitih aplikacijskih scenarija. Na primjer, otkrivanje anomalija u očitanim podacima koje se provodi u aplikacijskom sloju je usluga koja se može dijeliti između više aplikacija. Postojeće / nove aplikacije razmještene kao hosted usluge i kojima se pristupa preko Interneta se nazivaju SaaS. Za upravljanje SaaS aplikacijama u velikim razmjerima, PaaS sloj treba koordinirati oblak (rezerviranje izvora i raspoređivanje aplikacija) bez utjecaja na zahtjeve kvalitete usluge (QoS) bilo koje aplikacije. Autonomne komponente upravljanja treba staviti na mjesto za raspored i rezerviranje sredstava sa višom razinom točnosti za podršku IoT aplikacija. Ova koordinacija zahtijeva PaaS sloj da podržava autonomne mogućnosti upravljanja potrebne za rukovanje raspoređivanjem aplikacija i rezervacijom resursa uz zadovoljene QoS zahtjeve korisnika. Autonomni sustav za upravljanje će čvrsto integrirati sljedeće usluge s Aneka razvojne cjeline: računanje, praćenje i profiliranje, raspoređivanje i dinamičko rezerviranje. Računanje, praćenje i profiliranje će hraniti senzore autonomnog upravitelja, a menadžeri djelovatelji će kontrolirati raspoređivanje i dinamičko rezerviranje. S logičke točke gledišta dvije komponente koje će iskoristiti uvođenje autonomnih značajki u Aneka-u su aplikacije rasporeda i rezervacija dinamičkih resursa.

Aneka planer je odgovoran za dodjeljivanje pojedinih resursa zadacima u aplikacijama za izvršenje na temelju korisničkih QoS parametara i ukupnog troška za davatelja usluga. Ovisno o zahtjevima proračuna i podacima pojedine senzorske aplikacije, usmjerava komponentu dinamičkog rezerviranja resursa da pokrene ili ukine određeni broj računalnih, mrežnih i resursa za pohranu održavajući red zadataka prema rasporedu. Ova logika je ugrađena kao više-objektivna aplikacija raspoređivačkih algoritama. Planer je u mogućnosti upravljati padovima resursa premještanjem zadataka na druge pogodne Cloud resurse.
Komponenta dinamičkog dodjeljivanja resursa implementira logiku za osiguravanje i upravljanje virtualiziranim resursima u privatnim i javnim okruženjima računarstva u oblacima temeljenim na zahtjevima za resursima prema aplikacijskom planeru. To se postiže dinamičkim pregovaranjem s Cloud poslužiteljem infrastrukture kao usluge (Infrastructure as a service – IaaS) za pravu vrstu resursa za određeno vrijeme i trošak uzimajući u obzir prošlost izvršavanja aplikacija i raspoloživost proračuna. Ova odluka je donesena u hodu, dok SaaS aplikacije stalno šalju zahtjeve prema Aneka cloud platformi.



Slika 5.1.1. Pregled Aneka-e unutar IoT arhitekture [1]

5.2. IoT analiza senzorskih podataka pomoću Aneka-e i Microsoft Azure-a

Microsoft Azure je oblak platforma koju nudi Microsoft, a uključuje četiri komponente. Postoji nekoliko razloga za integriranje Azure-a i Aneka-e. Aneka možete pokrenuti neograničen broj instanci na Azure oblaku za pokretanje svojih aplikacija. U osnovi ona pruža opremačku infrastrukturu. Aneka također pruža napredne PaaS značajke kao što je prikazano na slici 5.1.1. Ona pruža više programske modele (zadatak, niz, MapReduce), izvršenja usluge, usluge upravljanja opterećenja, dinamičke dodjele, QoS na temelju raspoređivanja i fleksibilne naplate.
Alati i podaci se trebaju dijeliti između programera aplikacija za stvaranje novih aplikacija. Postoje dvije glavne prepreke u takvoj provedbi. Interakcija između oblaka postaje kritična što se rješava Aneka InterCloud modelom. Aneka podrška za InterCloud model omogućuje stvaranje hibridnog Cloud računalnog okruženja koje kombinira resurse privatnih i javnih oblaka. Kada privatni oblak nije u stanju ispuniti aplikacijske QoS zahtjeve, Aneka unajmljuje dodatne mogućnosti iz javnog oblaka kako bi se osiguralo da se aplikacija izvrši u određenom roku. Alati

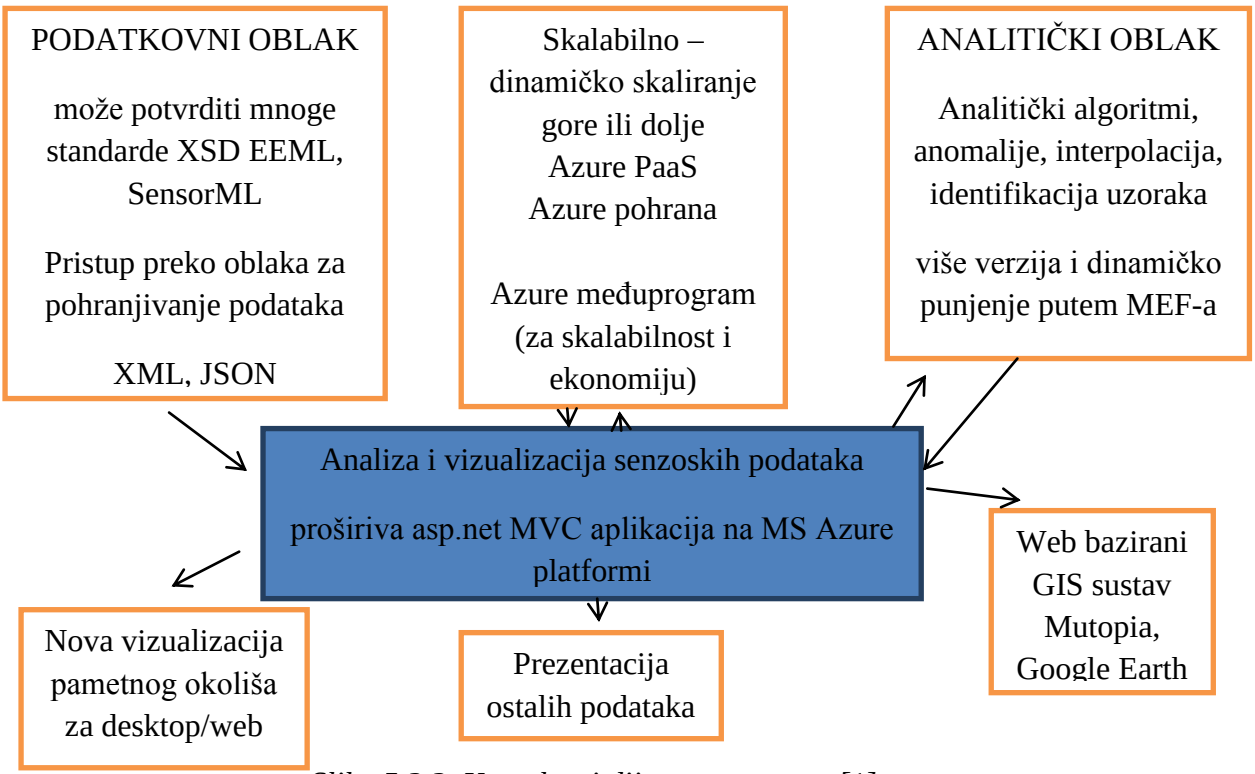
podatakovne analize i umjetne inteligencije su računarski zahtjevniji što zahtijeva velike resurse. Za alate podatakovne analize i umjetne inteligencije, Aneka programski model zadataka pruža mogućnost izražavanja aplikacija kao skup nezavisnih zadataka. Svaki zadatak može obavljati različite operacije, ili istu operaciju na različitim podacima, a može se izvršiti u bilo kojem redoslijedu od strane runtime okruženja. Shematski prikaz interakcija između Aneka-e i Azure-a je na slici 5.2.1., gdje su Aneka radni kontejneri razmješteni kao instance Azure radne uloge. Aneka glavni kontejner će biti raspoređen u lokalnom privatnom oblaku, dok će se Aneka radni kontejneri izvoditi kao instance sustava Microsoft Azure radne uloge. Kad Aneka radnici izvrše Aneka radne jedinice, šalju rezultate natrag Aneka glavnoj jedinici, a ona šalje rezultate natrag korisničkoj aplikaciji.

Tablica 5.2. Komponente Microsoft Azure-a [1]

Microsoft Azure	računalne usluge na zahtjev, usluge skladištenja
SQL Azure	podržava SQL prebacivanja i sinkronizaciju relacijskih podataka preko SQL Azure-a te na prostorima SQL Servera
AppFabric	međupovezivanje oblaka, aplikacije na zahtjev
Azure tržište	online servis za izradu transakcija na Apps i Data platformama

Slika 5.2.1. Shematski prikaz interakcije između Aneka-e i Azure-a za aplikacije analize podataka [1]

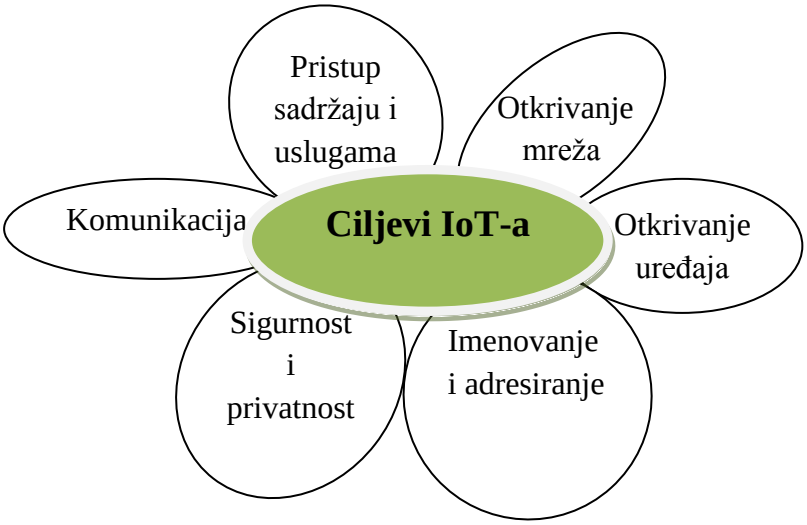
Još jedna važna značajka nezavisne IoT radne arhitekture je dinamičko ažuriranje SaaS-a od strane aplikacijskih programera. Alate za analizu (najčešće u Dynamic-link library - DLL obliku) treba koristiti više klijenata i moraju se ažurirati. Zbog administrativnih povlastica Azure-a, to je ne-trivijalan zadatak. Razvojna cjelina upravljanja proširljivosti (Managed Extensibility Framework - MEF) pruža jednostavno rješenje. MEF je sastavni sloj .NET-a koji poboljšava fleksibilnost, održavanje i ispitljivost velikih aplikacija. MEF se može koristiti za uključivanje preko treće strane ili može donijeti prednosti lagano vezanih plugin arhitektura za uobičajene aplikacije. To je knjižnica za stvaranje laganih, proširivih aplikacija. To omogućuje programerima aplikacija otkrivanje i korištenje proširenja bez konfiguracije. Ona također omogućuje programerima aplikacija lako zatvaranje koda i izbjegavanje ovisnosti. MEF dopušta ponovno korištenje proširenja u aplikacijama, ali i između aplikacija. MEF pruža standardni način host aplikaciji za razotkrivanje i korištenje vanjskih ekstenzija. Proširenja se, po svojoj prirodi, mogu ponovno upotrijebiti među različitim aplikacijama. Međutim, proširenja i dalje mogu biti provedena na način da su za pojedine programe. Proširenja mogu ovisiti jedna o drugima i MEF se brine da su spojena zajedno u ispravnom redoslijedu. Jedan od ključnih dizajnerskih ciljeva IoT web aplikacije je nadogradivost i MEF pruža ovo rješenje. Uz MEF možemo koristiti različite algoritme (kada postanu dostupni) za IoT analizu podataka: npr. ispuštanje analitičkog sklopa u mapu koja odmah postaje dostupna na primjenu. Dijagram konteksta sustava razvijene podatkovne analize je prikazan na slici 5.2.2.



Slika 5.2.2. Kontekstni dijagram sustava [1]

6. SIGURNOSNI MODEL

IoT scenariji, poput pojedinačnog bežičnog uređaja povezanog s internetom, rasporeda bežičnih uređaja, mreže senzora su povezani s novim zahtjevima mrežnih usluga koja motiviraju preispitivanje internetske arhitekture. Nekoliko mobilnih / bežičnih značajki mogu zahtijevati mehanizme koji se ne mogu provoditi putem konvencionalnog IP okvira za internet ili ako se mogu, pate od degradacije performansi zbog dodatnog viška povezanog s mrežnim protokolima koji su izvorno dizajnirani za statičku infrastrukturu računalstva.



Slika 6.1. Ciljevi IoT tehnologije [5]

1. Imenovanje i adresiranje

Današnja internetska adresna shema je vrlo kruta što je dobro prilagođeno za statičku, hijerarhijsku strukturu topologije. Ona pruža vrlo učinkovit način za označavanje i pronalaženje svakog sučelja uređaja u ovoj hijerarhiji. Za potporu mobilnosti i usmjeravanja sljedeća generacija Interneta mora pružiti načine za imenovanje i usmjeravanje puno većeg skupa mrežnih elemenata nego što su točke povezivanja. Ključan uvjet je čisto arhitektonsko razdvajanje adresa za imenovanja i usmjeravanja.

2. Otkrivanje uređaja i mreža

Trenutni Internet je tekstualno dominantan sa relativno učinkovitim tražilicama za otkrivanje tekstualnih resursa sa ručnim podešavanjem. Internet ispunjen nestrukturiranim informacijama dobivenim od velikog broja senzorskih uređaja mora podržavati učinkovite mehanizme za otkrivanje dostupnih senzorskih resursa. Nova arhitektura mora podržavati metode za upis novog senzorskog sustava u širu mrežu.

3. Pristup sadržaju i uslugama

Nova arhitektura treba osigurati mehanizme čišćenja podataka koji sprječavaju propagaciju korumpiranih podataka kroz mrežu senzora. Konkretno, usluge koje održavaju kalibraciju uređaja i nadzor / otkrivanje manipulacija senzorskih uređaja trebaju biti integrirane u senzorske mreže. To se može realizirati kroz stjecanje konteksta informacije i uporabom statističke tehnike za lokalno otkrivanje neispravnih ulaza.

4. Komunikacija

Bežični uređaji trebaju neovisno djelovati na širem Internetu jer postoje trenuci tijekom kojih povezivanje bežičnog uređaja ili mreža na Internet nije dostupno. Tijekom tih vremena, bežični uređaji trebaju raditi stabilno isključeni iz ostatka infrastrukture, kao i biti u stanju uspostaviti "lokalne" ad-hoc mreže korištenjem vlastitih izvornih protokola. Time bi se pitanja autorizacije i ažuriranja uređaja rješavala nevidljivo, uz minimalnu latenciju.

5. Sigurnost i privatnost

Očekuje se da će bežične mreže biti platforma novog Interneta na koju će se izvršiti niz napada. Na najosnovnijoj razini, bežični uređaji će vjerojatno imati razvijene sheme imenovanja i adresiranja te će biti potrebna provjera i autentifikacija imena i adresa koji se koriste. Parametar jedinstveno povezan s bežičnim mrežama je pojam o lokaciji. Lokacijska informacija koju mreža osigurava treba biti pouzdana.

Postoji nekoliko ključnih svojstava IoT-a koja postavljaju dodatne zahtjeve za sigurnost.

Mobilnost: IoT uređaji su mobilni i često se spajaju na Internet putem velikog skupa providera

Bežičnost: ovi sustavi se obično spajaju na ostatak Interneta preko širokog raspona bežičnih veza, uključujući Bluetooth, 802.11, WiMAX, ZigBee i GSM / UMTS. Uz bežične komunikacije, promatrač u blizini može presresti jedinstvene identifikatore niske razine koji se šalju u jasne adrese uređaja kao što su. Bluetooth i 802.11.

Ugrađena uporaba: glavni IoT uređaji imaju jednu uporabu (krvni tlak ili praćenje rada srca, kućanski aparati). Rezultat toga je mogućnost profiliranja korisnika pomoću obrazaca za detekciju komunikacije jedinstvenih za specijalizirane uređaje.

Raznolikost: ovi uređaji imaju raspon računalnih sposobnosti od punopravnog računala do RFID oznaka. Privatnost dizajna se mora prilagoditi i najjednostavnijim uređajima.

Skala: uređaji su praktičniji, broj im raste dnevno što otežava korisnicima praćenje pitanja privatnosti.

Sigurnosni zahtjevi su sljedeći:

Otpornost na napade: Sustav mora izbjeći pojedine točke neuspjeha i treba prilagoditi sebe ispadima čvorova.
Provjera podataka: U načelu, prihvatne adrese i informacije objekata moraju biti ovjerene.
Kontrola pristupa: Ponuditelji informacija moraju biti u stanju provesti kontrolu pristupa na ponuđenim podacima.
Privatnost klijenta: Treba poduzeti mjere da samo ponuditelji informacija mogu promatrati korištenje sustava određenog kupca.
Identifikacija korisnika: Odnosi se na proces potvrđivanja korisnika prije nego što mu se dopušta upotreba sustava.
Sigurno spremanje: Uključuje povjerljivost i integritet osjetljivih informacija pohranjenih u sustavu.
Upravljanje identitetom: To je široko upravno područje koje se bavi identificiranjem osoba / objekata u sustavu i kontrolom njihovog pristupa resursima pridruživanjem korisničkih prava i ograničenja s utvrđenim identitetom.
Siguran prijenos podataka: Osiguranje povjerljivosti i integriteta prenešenih podataka, sprečavanje odbacivanja komunikacijske transakcije i zaštita identiteta subjekata komunikacije.
Dostupnost: Osiguravanje da neovlaštene osobe ili sustavi ne mogu uskratiti pristup ili korištenje odobrenim korisnicima.
Siguran pristup mreži: Omogućuje mrežnu vezu ili pristup servisu samo ako je uređaj ovlašten.
Siguran sadržaj: Sigurnost sadržaja ili upravljanje digitalnim pravima (Digital rights management - DRM) štite prava digitalnog sadržaja koji se koristi u sustavu.
Okolina sigurnog izvršenja: Sigurno, runtime okruženje osmišljeno radi zaštite protiv devijantnih aplikacija.
Otpornost na manipulaciju: Odnosi se na želju da se održe prijašnji sigurnosni zahtjevi čak i kada uređaj padne u ruke zlonamjernih osoba, a može biti fizički ili logički ispitano.

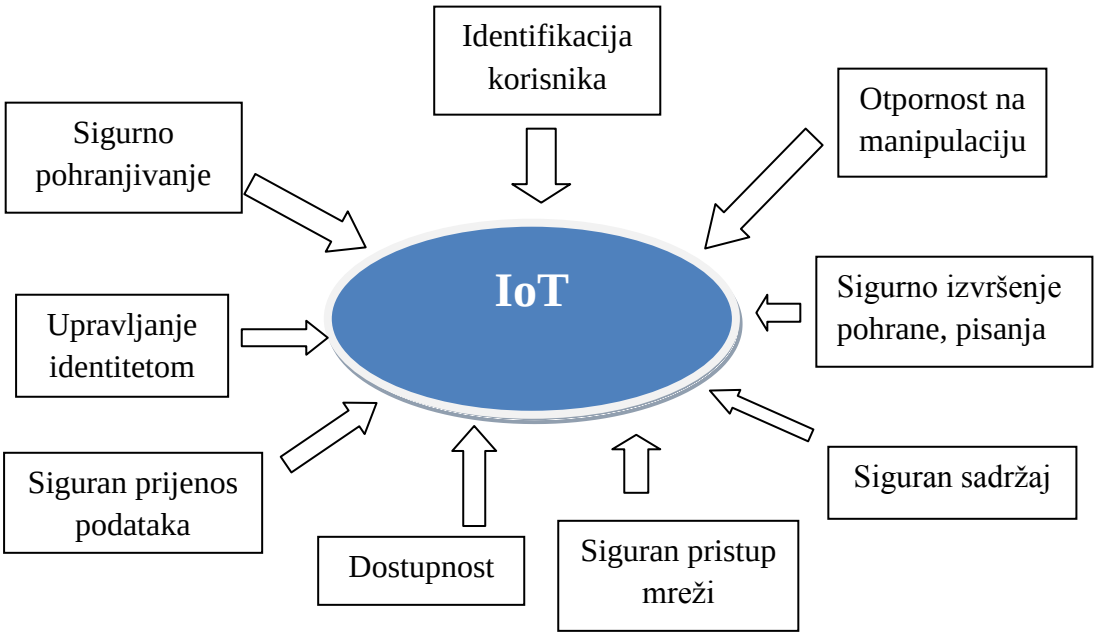
IoT zajedno s novim sigurnosnim prijetnjama mijenja ukupni profil sigurnosnog rizika. Iako implementacija tehnoloških rješenja može odgovoriti na IoT prijetnje i ranjivosti, IoT sigurnost je prvenstveno pitanje upravljanja. Djelotvorno upravljanje prijetnjama povezanim s IoT-em zahtijeva zvučnu i temeljitu procjenu rizika s obzirom na okoliš i razvoj plana za ublažavanje identificiranih prijetnji. Sika 6.3. predstavlja taksonomiju prijetnji za razumijevanje i procijenu različitih prijetnji povezanih s korištenjem IoT-a.
Identifikacija obuhvaća određivanje jedinstvenog uređaja / korisnika / sesije s autentifikacijom, ovlaštenjima, računovodstvom i rezerviranjima.

Komunikacijske prijetnje pokrivaju napade uskraćivanja usluge (Denial of service - DoS) koji se događaju kada napadač neprestano bombardira ciljanu pristupnu točku (Access Point) ili mrežu s lažnim zahtjevima, uranjenim porukama uspješne veze, lažnim porukama o padovima te druge naredbe.

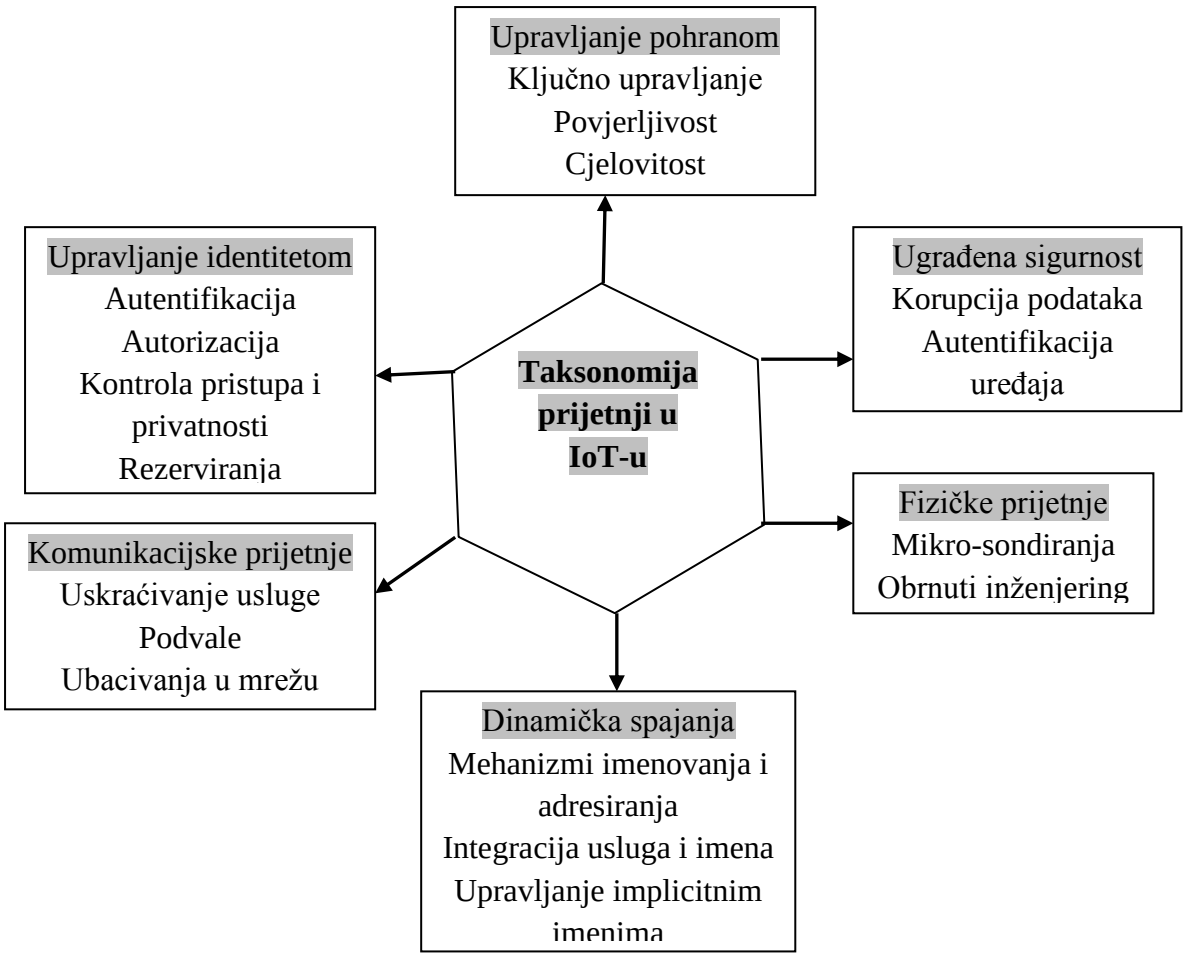
Fizička prijetnja uključuje mikro sondiranja i obrnuti inženjering što dovodi do teških sigurnosnih problema izravnim petljanjem po hardverskim komponentama. Neke vrste fizikalnih napada zahtijevaju skupe materijale zbog čega su relativno teško izvedivi. Primjeri su repakiranje čipova, rekonstrukcija rasporeda, mikro-sondiranje.

Ugrađeni sigurnosni model prijetnji će obuhvatiti sve prijetnje na fizičkom i MAC sloju. Sigurnosne prijetnje poput manipulacija uređajima i podacima, analize susjednih kanala, praćenje sabirnica će biti problemi na razini uređaja.

Upravljanje pohranom ima presudan utjecaj na ključno poslovodstvo kako bi se postigla povjerljivost i integritet. Također moramo biti oprezni u izboru koje kriptografske komponente koristiti kao građevne blokove jer na primjer, tekstovi šifri za enkripcije javnog ključa mogu otkriti podatke o identifikaciji namijenjenog primatelja.



Slika 6.2. Visoki sigurnosni zahtjevi IoT-a [5]



Slika 6.3. Taksonomija prijetnji u IoT-u [5]

Sigurnosni okvir za IoT uglavnom uključuje arhitekture za pružanje i upravljanje kontrole pristupa, autentifikaciju i autorizaciju. To će osigurati metode za kontrolu identifikacija i autentifikacija korisnika te za administriranje kojim autoriziranim korisnicima se odobrava pristup zaštićenim resursima. Neki od opisanih okvira se mogu koristiti za dobivanje više funkcija, kao što je prikazano u tablici 6.1.

Okviri dopuštaju korisnicima digitalno potpisivanje i šifriranje poruka bez prethodnog kontakta za međusobnu autentifikaciju. Baziraju se na potvrdi identiteta, potvrde vežu javni ključ na identitet. Primjeri okvira potvrde identiteta su infrastruktura javnog ključa (Public key infrastructure - PKI) i dobra privatnost (Pretty Good Privacy - PGP).

Jednostruko prijavljivanje (Single sign-on - SSO) omogućava korisnicima da se u sustavu ovjere samo jednom. Korisnici tada mogu pristupiti svim resursima za koje imaju dozvolu pristupa bez unošenja više lozinki. SSO okviri obuhvaćaju: Kerberos distribuirana usluga autentičnosti, koji pruža SSO u jednoj administrativnoj domeni.

Windows Live ID: internetski bazirani SSO okvir kojeg koriste Microsoftovi programi i web usluge kao što je MSN Messenger.

OpenID: autentifikacijski okvir koji omogućava korisnicima prijavu na različite web stranice koristeći jedan digitalni identitet, eliminirajući potrebu za različitim korisničkim imenima i lozinkama za svaku stranicu.

Liberty Alliance: konzorcija koja ima za cilj uspostaviti otvorene standarde, smjernice i najbolju praksu za udruženo upravljanje identitetom.

WS - savez: federalni standardni identitet razvijen od strane Microsofta, IBM-a, VeriSign-a, BEA-e i RSA Sigurnosti, koji je sastavni dio sigurnosnog okvira Web usluga.

Savezni identitet omogućuje korisnicima jedne sigurnosne domene siguran pristup resursima na drugoj sigurnosnoj domeni, bez potrebe za drugim korisničkim računom. Korisnici se registriraju na autentifikacijskom poslužitelju u njihovoj domeni, a druge domene vjeruju tvrdnjama.

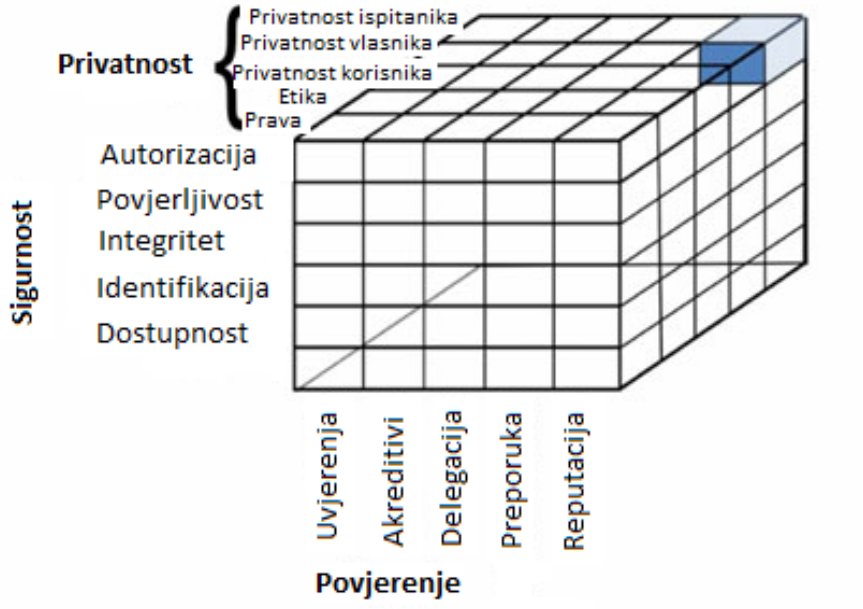
Korisnički bazirano upravljanje identitetom je dizajn koji se fokusira na upotrebljivost i isplativost sa korisničkog gledišta. Postoje tri glavna pristupa prema korisnički baziranom upravljanju identitetom koji upravljalju sa više identiteta kao što su informacijske kartice.

Okvir sigurnosti uređaja uključuje sigurnosni softver i sigurnosne mogućnosti isporučene preko mreže. Softver je ugrađen u uređaje za vrijeme proizvodnje.

Tablica 6.1. SSO okviri [5]

	Okvir	Upravljanje identifikacijskim certifikatima	Jednostruka prijava	Federalni identitet	Korisnički centriran
1.	PKI	✓			
2.	PGP	✓			
3.	Kerberos		✓		
4.	Windows Live ID		✓		✓
5.	OpenID		✓		✓-
6.	Liberty Alliance		✓	✓	✓
7.	WS-Federation		✓	✓	

Integrirana i povezana perspektiva sigurnosti, povjerenja i privatnosti može potencijalno isporučiti ulaz za rješavanje pitanja zaštite u IoT-u. Struktura kocke je dobar modelirajući mehanizam za sigurnost, povjerenje i privatnost u IoT-u. Kocka ima tri dimenzije s mogućnošću jasnog prikaza njihovih križanja. Stoga je kocka idealna modelirajuća konstrukcija za oslikavanje konvergencija sigurnosti, povjerenja i privatnosti. IoT pristupni podaci potrebni za odobrenje / odbijanje zahtjeva za pristup su složeni po prirodi. To je izravna posljedica visoke razine međusobne povezanosti stvari, usluga i ljudi. Jasno je da su vrsta i struktura podataka potrebnih za odobrenje / odbijanje zahtjeva pristupa složeni i treba obratiti pozornost na sljedeća IoT pitanja: sigurnost (odobrenje), povjerenje (ugled), privatnost (ispitanik). Ovo je opisano na slici 6.4.



Slika 6.4. Sigurnosni model IoT-a [5]

Pojedinačni razvoj tehnologija IoT-a treba ostvariti ono što je Internet propustio učiniti: od samog početka osigurati odgovarajuće mehanizme sigurnosti i privatnosti. Moramo biti sigurni da su odgovarajuća sigurnost i privatnost na raspolaganju prije nego što se tehnologija uvede i postane dio našeg svakodnevnog života. Sigurnosni zahtjev i taksonomija prijetnji inzistiraju na Modulu pouzdane platforme koji nudi bazu za sigurnu generaciju kriptografskih ključeva i ograničavanje njihove uporabe, kao dodatak hardverskom pseudo-slučajnom generatoru brojeva. Također uključuje mogućnosti kao što su daljinsko potvrđivanje i zapečaćena pohrana. "Udaljena potvrda" stvara ključni sažetak konfiguracije hardvera i softvera. Opseg sažetka softvera određuje program za šifriranje podataka. To omogućuje trećoj strani provjeru da nije došlo do promjene programa. "Vezanje" šifrira podatke pomoću TPM odobravajućeg ključa, jedinstvenog RSA ključa spaljenog u čip tijekom proizvodnje.

7. IZAZOVI I SMJERNICE ZA BUDUĆNOST

Predložena vizija sa oblakom u središtu se sastoji od fleksibilne i otvorene arhitekture koja je korisnički centrirana i omogućuje različitim stranama interakciju unutar IoT razvojne cjeline. To omogućuje interakciju na način pogodan za vlastite potrebe, tj. IoT ne vrši potisak na njih. Na taj način, razvojna cjelina uključuje odredbe za zadovoljavanje različitih zahtjeva za vlasništvo podataka, sigurnost, privatnost i dijeljenje informacija.

IoT specifični izazovi su na područjima kao što su privatnost, djelomično istraživanje, analiza podataka, vizualizacija temeljena na Geografskom informacijskom sustavu (Geographic information system – GIS) i računarstvo u oblacima osim standardnih WSN izazova uključujući arhitekturu, energetsku učinkovitost, sigurnost, protokole i kvalitetu usluge. Krajnji cilj je postojanje Uključi i koristi (Plug n' Play) pametnih predmeta koji se mogu implementirati u bilo koje okruženje s interoperabilnom okosnicom dopuštajući im da se uklope s drugim pametnim objektima oko njih. Standardizacija frekvencijskih pojaseva i protokola igra ključnu ulogu u ostvarenju tog cilja.

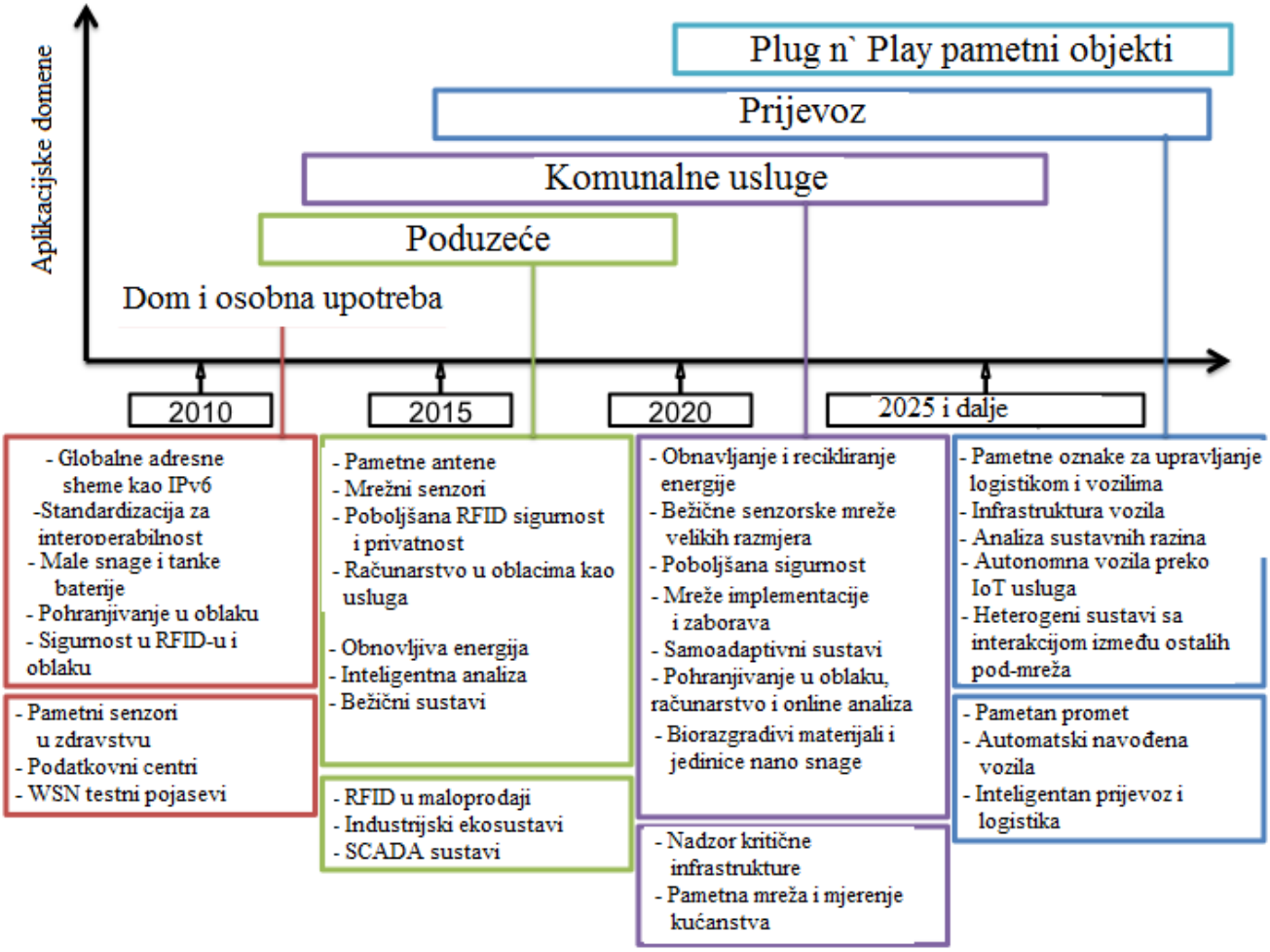
Putokaz ključnih zbivanja u IoT istraživanju u kontekstu aplikacija je prikazan na slici 7.1., koji uključuje tehnološke programe i ključne aplikacijske ishode očekivane u sljedećem desetljeću.

Sveukupna arhitektura u početnim fazama IoT istraživanja će imati ozbiljan utjecaj na samom terenu i trebat će ju dodatno istražiti. Najveći dio posla koji se odnosi na IoT arhitekturu je od strane bežičnih senzorskih mreža. Arhitektura koja se temelji na računarstvu u oblacima u središtu je predložena u odjeljku 5. Međutim, to ne može biti najbolja opcija za svaku aplikacijsku domenu, posebno za obranu u kojoj se oslanjamo na ljudsku inteligenciju. Iako je arhitektura sa oblakom u središtu najbolja kada se traže usluge temeljene na troškovima, treba istražiti ostale arhitekture za različita područja primjene.

Učinkovito heterogeno očitavanje urbanog okoliša treba istovremeno zadovoljiti zahtjeve više senzorskih modaliteta. To ima utjecaja na mrežni promet, pohranu podataka i korištenje energije. Važno je da to obuhvaća i fiksnu i mobilnu senzorsku infrastrukturu kao i kontinuirano i slučajno uzorkovanje. Generalizirana razvojna cjelina je potrebna za prikupljanje podataka i modeliranje koja učinkovito iskorištava prostorna i vremenska svojstva podataka, kako u osjetnom području, tako i u povezanim prijenosnim domenama. Na primjer, urbano mapiranje buke treba stalno prikupljanje razina buke uz korištenje baterijski napajanih čvorova koristeći fiksnu infrastrukturu i djelomično očitavanje kao ključne komponente za zdravlje i kvalitetu životnih usluga za stanovnike.

Tlačna očitavanja omogućuju mjerenja reduciranih signala bez utjecaja na točnu rekonstrukciju signala. Signal u jednoj bazi se može očitati od malog broja projekcija na drugu bazu koja je

nepovezana s prvom. Problem se svodi na pronalaženje rješenja kroz najmanje koeficijente vektora koji se slaže s mjerenjima. U sveprisutnom osjetnom kontekstu, to ima implikacije za kompresiju podataka, mrežni promet i distribuciju senzora. Tlačna bežična očitavanja (Compressive wireless sensing - CWS) koriste sinkronu komunikaciju za smanjivanje snage odašiljanja svakog senzora; emitira bučne projekcije podatkovnih uzoraka na središnje mjesto za agregaciju.



Slika 7.1. Plan ključnih tehnoloških razvoja u kontekstu IoT aplikacijskih domena [1]

Sigurnost će biti glavna briga gdje god su mreže raspoređene u velikim razmjerima. Sustav može biti napadnut na više načina - onesposobljavanje dostupnosti mreže; slanje pogrešnih podataka u mrežu; pristup osobnim podacima; itd. Tri fizičke komponente IoT-a - RFID, WSN i oblak su osjetljive na takve napade. Sigurnost je ključna za bilo koju mrežu i prvu liniju obrane protiv korupcije podataka čini kriptografija. Od komponenti, RFID (osobito pasivni) se čini najranjivijim jer omogućuje praćenje osoba, kao i objekata, a visoki stupanj inteligencije se ne može omogućiti na tim uređajima. Ovi kompleksni problemi se mogu riješiti primjenom kriptografske metode koja zaslužuje više istraživanja prije nego što je široko prihvaćena. Protiv

napadača izvana, enkripcija osigurava povjerljivost podataka, dok kodovi autentičnosti poruka osiguravaju cjelovitost i autentičnost podataka. Enkripcija, međutim, ne štiti od unutarnjih zlonamjernih napada, potrebna su ne-kriptografska sredstva, osobito u WSN-u. Također, povremeno se trebaju instalirati nove senzorske aplikacije ili postojeće ažurirati. To se radi daljinskim bežičnim reprogramiranjem svih čvorova u mreži. Tradicionalno mrežno reprogramiranje se sastoji isključivo od protokola slanja podataka koji distribuira kod svim čvorovima u mreži bez autorizacije, što je prijetnja sigurnosti. Sigurni reprogramibilni protokol omogućuje čvorovima provjeru autentičnosti svakog ažuriranja koda i spriječava zlonamjernu instalaciju. Većina takvih protokola se temelji na referentnom protokolu Deluge. Kriptografski dodaci su potrebni da postave temelje za razvoj viših sofisticiranih algoritama.
Sigurnost u oblaku je još jedno važno područje istraživanja koje zahtijeva pozornost. Uz prisustvo podataka i alata, oblak obrađuje i ekonomiju IoT-a kojoj će napadi biti još veća prijetnja. Sigurnost i zaštita identiteta postaju kritični u hibridnim oblacima, gdje privatne i javne oblake koriste tvrtke.
Pamćenje podataka zauvijek u kontekstu IoT-a postavlja mnoga pitanja privatnosti jer se prikupljeni podaci mogu koristiti u pozitivne (oglašavanje) i negativne svrhe (za klevetu). Digitalno zaboravljanje je jedno od ključnih područja istraživanja kako bi se riješili problemi i razvio odgovarajući okvir za zaštitu osobnih podataka.

Heterogene mreže su (po defaultu) višeuslužne; pružaju više od jednog posebnog programa ili uslugu. To podrazumijeva više vrsta prometa unutar mreže, ali i sposobnost jedne mreže da podržava sve aplikacije bez kompromisa QoS-a. Postoje dvije aplikacijske klase: propusnost i tolerancija kašnjenja elastičnog prometa (npr. praćenje vremenskih parametara na niskim stopama uzorkovanja), propusnost i kašnjenje osjetljivog neelastičnog (u realnom vremenu) prometa (npr. buka ili praćenje prometa), koji se mogu dodatno diskriminirati sa podatkovno povezanim aplikacijama (npr. visoka i niska rezolucija videa) s različitim QoS zahtjevima. Dakle, potreban je kontrolirani, optimalni pristup za pružanje različitog mrežnog prometa, svakog sa svojom vlastitom aplikacijskom QoS. Nije lako dati QoS jamstva u bežičnim mrežama, jer segmenti često čine „razmake“ u jamstvu resursa zbog raspodjele resursa i ograničene sposobnosti upravljanja u dijeljenom bežičnom mediju. Kvaliteta usluge u računarstvu u oblacima je još jedan veliki istraživački prostor koji će zahtijevati sve više i više pozornosti kako podaci i alati postanu dostupni na oblacima. Aplikacije velikih kapaciteta i rast IoT-a mogu dovesti do uskog grla.

Protokoli na senzorskom kraju IoT-a će igrati ključnu ulogu u potpunoj realizaciji. Oni čine okosnicu tunela podataka između senzora i vanjskog svijeta. Za energetski učinkovit rad, kritični

su MAC protokol i primjereni protokol usmjeravanja. Nekoliko MAC protokola je predloženo za različite domene sa Time division multiple access - TDMA (bez kolizija), Carrier sense multiple access - CSMA (niska učinkovitost u prometu) i Frequency Division Multiple Access - FDMA (bez kolizija, ali zahtijeva dodatni krug u čvorovima). Nijedan od njih nije prihvaćen kao standard i sa više dostupnih „objekata“ ovaj će scenarij postati pretrpan što zahtijeva daljnja istraživanja.

Pojedini senzor može ispasti iz brojnih razloga, stoga mreža mora biti samo-prilagođavajuća i omogućiti višesmjerno usmjeravanje. Višeskočni protokoli usmjeravanja se koriste u mobilnim ad hoc mrežama i zemaljskim WSN-ovima. Oni su uglavnom podijeljeni u tri kategorije - podaci u središtu, lokacijski bazirani i hijerarhijski, na temelju različitih područja primjene. Energija je glavna tema razmatranja za postojeće protokole usmjeravanja. U slučaju IoT-a, treba napomenuti da će okosnica biti dostupna i broj skokova u multi-hop scenariju će biti ograničen. U takvom scenariju, postojeći protokoli usmjeravanja će biti dovoljni za praktičnu primjenu s manjim izmjenama.

Brojni projekti su se počeli baviti razvojem ljudski baziranih (ili djelomičnih) seenzorskih platformi. Očitavanje sa ljudima u središtu nudi mogućnost jeftinog očitavanja okoliša lokaliziranog korisniku. Dakle, može dati najbliži pokazatelj okolišnih parametara koje je doživio korisnik. Podaci okoliša prikupljeni od strane korisnika oblikuju socijalnu valutu. To rezultira u više pravovremenim podacima koji se generiraju u usporedbi s podacima dostupnim putem infrastrukture fiksne mreže senzora. Najvažnija je, prilika korisniku za pružanje povratne informacije o njihovim iskustvima određenog parametra okoliša koji pruža vrijedne informacije u kontekstu povezanog s određenim događajem.

Ograničenja ljudski baziranih senzorskih mreža tvore novo značenje na ulogu referentnih podataka koje pruža fiksna infrastruktura IoT-a kao okosnica. Problem nestalih uzoraka je temeljno ograničenje ljudski baziranih očitavanja. Oslanjajući se na volontiranje korisničkih podataka i na nedosljedno prikupljanje uzoraka dobivenih preko različitih vremena i različitih mjesta (na temelju korisnikova željenog sudjelovanja i dane lokacije ili puta prolaska), ograničava sposobnost proizvodnje smislenih podataka za bilo koje aplikacije i političke odluke. Takva platforma može postići istinski angažman krajnjeg korisnika samo u rješavanju problema i implikaciji vlasništva podataka, privatnosti i odgovarajućim poticajima za sudjelovanje. Senzorski modaliteti se mogu dobiti dodavanjem senzorskih modula vezanih uz telefon za očitavanja posebnih aplikacija, poput senzora kvalitete zraka ili biometrijskih senzora. U takvim scenarijima, pametni telefoni postaju kritični IoT čvorovi koji su na jednom kraju spojeni na oblak i na nekoliko senzora na drugom kraju.

Izdvajanje korisne informacije iz složenog senzorskog okoliša na različitim prostornim i vremenskim rezolucijama je izazovan problem istraživanja u umjetnoj inteligenciji. Trenutne state-of-the-art metode koriste plitke metoda učenja u kojima se unaprijed definirani događaji i anomalije podataka izlučuju korištenjem učenja sa nadzorom i bez nadzora. Sljedeća razina učenja uključuje zaključne lokalne aktivnosti pomoću vremenskih informacija o događajima izvađenih iz plitkog učenja. Krajnja vizija je otkrivanje složenih događaja na temelju većih prostornih i dužih vremenskih skala. Temeljni istraživački problem koji se javlja u složenim osjetnim okruženjima ove prirode je kako istodobno naučiti prikaze događaja i aktivnosti na više razina složenosti (tj, događaji, lokalne aktivnosti i složene aktivnosti). Fokus u istraživanjima strojnih učenja je područje dubokih učenja, koje teži naučiti više slojeva apstrakcije koja se mogu koristiti za tumačenje navedenih podataka. Ograničenja resursa u senzorskim mrežama stvaraju nove izazove za učenje s razumijevanjem u smislu potrebe za prilagodljivim, distribuiranim tehnikama učenja.

Pojavom novih tehnologija prikaza, omogućiti će se kreativna vizualizacija. Razvoj od CRT (Cathode ray tube) do plazme, LCD (Liquid crystal display), LED (Light-emitting diode) i AMOLED (Active-matrix organic light-emitting diode) zaslona uvjetovao je vrlo učinkovitu prezentaciju podataka (pomoću touch sučelja), a korisniku navigaciju podacima bolje nego ikad prije. S novim 3D zaslonima, ovo područje sigurno ima više mogućnosti za istraživanje i razvoj. Podaci koji dolaze iz sveprisutnog računalstva nisu uvijek spremni za izravnu uporabu pomoću vizualizacijske platforme i zahtijevaju daljnju obradu. Trebaju se razviti nove vizualizacijske sheme za predstavljanje heterogenih senzora u 3D krajoliku koji varira vremenski. Još jedan izazov vizualizacijskih podataka prikupljenih unutar IoT-a je da su oni zemljopisno vezani i rijetko raspoređeni. Zbog toga je potreban okvir na temelju Internet GIS-a.

Integrirani IoT i aplikacije računarstva u oblacima koji omogućuju stvaranje pametnih okruženja, kao što su Pametni gradovi trebaju biti u mogućnosti: kombinirati usluge više sudionika i skalu da podrže veliki broj korisnika na pouzdan i decentraliziran način. Oni moraju biti u mogućnosti djelovati u žičnim i bežičnim mrežnim okruženjima, nositi se s ograničenjima, kao što su pristup uređajima ili izvori podataka s ograničenom moći i nepouzdanim povezivanjem. Oblačne aplikacijske platforme moraju biti poboljšana podrška brzom stvaranju aplikacija pružajući domene specifičnih programskih alata i okruženja i nevidljivom izvršenju aplikacija iskorištavanjem mogućnosti više-dinamičnih i heterogenih izvora u svrhu zadovoljavanja zahtjeva kvalitete usluga različitih korisnika.

Oblačno upravljanje resursima i sustav raspoređivanja trebaju biti u mogućnosti dinamički prioritizirati zahtjeve i pružateljske resurse tako da se kritični zahtjevi služe u realnom vremenu. Za dostavu rezultata na pouzdan način, raspored treba biti dopunjen algoritmima umnožavanja zadataka za upravljanje neuspjehom. Raspoređivački algoritmi Cloud aplikacija trebaju sljedeće mogućnosti:

1. Više-ciljna optimizacija: raspoređivački algoritmi trebaju biti u stanju nositi se s QoS parametrima poput vremena odziva, troškova korištenja usluge, maksimalni broj raspoloživih sredstava po jedinčnoj cijeni i kazne za degradaciju usluga.

2. Tolerancija greške na temelju umnožavanja zadataka: Kritični zadaci aplikacije će biti transparentno replicirani i izvršeni na različitim resursima, tako da ako jedan resurs ne završi zadatak, može se koristiti replicirana verzija. Ova logika je presudna u zadacima u realnom vremenu koje treba obraditi za pravodobno pružanje usluga.

8. ZAKLJUČAK

Brzi porast broja uređaja sa sposobnostima komunikacije i aktivacije približava viziju Interneta stvari gdje su funkcije osjeta i djelovanja neprimjetno uklopljene u pozadinu i nove mogućnosti su ostvarene kroz pristup novim bogatim izvorima informacije. Evolucija mobilnog sustava nove generacije ovisit će o kreativnosti korisnika u projektiranju novih aplikacija. IoT je idealna tehnologija u nastajanju koja može utjecati na ovo područje pružajući nove rastuće podatke i potrebne računalne resurse za stvaranje revolucionarnih aplikacija.

U ovom radu je predstavljen oblak sa korisnikom u središtu za približavanje ovog cilja kroz interakciju privatnih i javnih oblaka čime se potrebe krajnjeg korisnika iznose na vidjelo. Dopuštajući potrebnu fleksibilnost kako bi se zadovoljile različite, a ponekad i suprotstavljene potrebe različitih sektora, predložen je okvir omogućen od strane skalabilnog oblaka da se osigura kapacitet za iskorištavanje IoT-a. Okvir omogućuje odvajanje umrežavanja, obračuna, skladištenja i vizualizacijskih tema čime svaki sektor može samostalno rasti, ali nadopunjuju jedni druge u zajedničkom okruženju. Na standardizaciju koja je u tijeku u svakoj od tih tema, oblak u središtu neće negativno utjecati. U predlaganju novog okvira, istaknuti su povezani izazovi u rasponu od odgovarajuće interpretacije i vizualizacije ogromne količine podataka, do privatnosti, sigurnosti i pitanja upravljanja podacima koja moraju podupirati takvu platformu kako bi to bilo istinski održivo. Konsolidacija međunarodne inicijative posve jasno ubrzava napredak prema IoT-u, pružajući sveobuhvatni pogled za integraciju i funkcionalne elemente koji mogu dostaviti operativni IoT.

Internet stvari nekome može djelovati zastrašujuće ili prijeteće jer nas približava automatiziranom, robotskom svijetu. No, realnost je da smo već počeli automatizirati što više aspekata radnog mjesta, a dom je sljedeći korak. To ne znači da će stvari razmišljati za nas ili donositi odluke umjesto nas. Internet stvari nam jednostavno omogućuje da se usredotočimo na veće projekte od paljenja svjetla ili provjeravanja temperature hladnjaka.

LITERATURA

[1] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswamia: „Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions,“ 2011.

[2] Zornitza Prodanoff, Seungnam Kang: “ RFID Model for Simulating Framed Slotted ALOHA Based Anti-Collision Protocol for Muti-Tag Identification,“ 2011.

[3] Shian Liu, Xiaojuan Peng: „Improved ID Binary Tree Stack Anti-collision Algorithm in RFID Systems,“ 2012.

[4] Shirin Zarghami: „Middleware for Internet of Things,“ 2013.

[5] Sachin Babar, Neeli Prasad: „Proposed Security Model and Threat Taxonomy for the Internet of Things,“ 2011.