

# Internet stvari: pregled područja

---

**Zadavec, Hana**

**Undergraduate thesis / Završni rad**

**2023**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Pula / Sveučilište Jurja Dobrile u Puli**

*Permanent link / Trajna poveznica:* <https://um.nsk.hr/um:nbn:hr:137:163044>

*Rights / Prava:* [In copyright](#)/[Zaštićeno autorskim pravom.](#)

*Download date / Datum preuzimanja:* **2024-11-23**



*Repository / Repozitorij:*

[Digital Repository Juraj Dobrila University of Pula](#)



Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

**Hana Zdravec**

**Internet stvari: Pregled područja**

Završni rad

Pula, srpanj, 2023.

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

**Hana Zadravec**

**Internet stvari: Pregled područja**

Završni rad

**JMBAG: 0303094592, redoviti student**

**Studijski smjer: Informatika**

**Kolegij: Mrežni sustavi**

**Znanstveno područje: Društvene znanosti**

**Znanstveno polje: Informacijske i komunikacijske znanosti**

**Znanstvena grana: Informacijski sustavi i informatologija**

**Mentor: izv. prof. dr. sc. Siniša Sovilj Dalibor Fonović (sumentor)**

Pula, srpanj, 2023.

# SADRŽAJ

<b>1. UVOD</b> .....	1
<b>2. POVIJEST IOT-A</b> .....	3
<b>3. ARHITEKTURA IOT-A</b> .....	5
<b>3.1. Troslojna arhitektura</b> .....	5
<b>3.2. Petoslojna arhitektura</b> .....	6
<b>3.3. Sedmeroslojna arhitektura</b> .....	8
<b>4. KOMUNIKACIJSKI MODELI</b> .....	10
<b>4.1 Komunikacija između uređaja (Device-To-Device)</b> .....	10
<b>4.2 Komunikacija između uređaja i oblaka (Device-To-Cloud)</b> .....	11
<b>4.3 Model komunikacije između uređaja i usmjerivača (Device-To-Getaway)</b> .....	12
<b>4.4. Model Dijeljenja Podataka na strani Poslužitelja (Back-End Data-Sharing)</b> ..	14
<b>5. PRIMJENE IOT-A</b> .....	16
<b>5.1. Primjena u kućanstvu</b> .....	16
5.1.1. <i>Osvjetljenje</i> .....	16
5.1.2. <i>Kupaonica</i> .....	17
5.1.3. <i>Okućnica</i> .....	17
5.1.4. <i>Kuhinja</i> .....	17
5.1.5. <i>Sigurnosni sustavi</i> .....	18
5.1.6. <i>Kontrola temperature</i> .....	18
5.1.7. <i>Vrata</i> .....	18
5.1.8. <i>Prozori</i> .....	19
5.1.9. <i>Multimedija</i> .....	19
<b>5.2. Primjena u industriji</b> .....	19
<b>5.3. Primjena u zdravstvu</b> .....	20
<b>5.4. Primjena u prometu (transpotru) i logistici</b> .....	23
<b>5.5. Primjena u poljoprivredi</b> .....	23
<b>5.6. Primjeri iz stvarnog svijeta</b> .....	24
5.6.1. <i>Google Home</i> .....	24
5.6.2. <i>August Doorbell Cam Pro</i> .....	25
5.6.3. <i>Mr. Coffee Smart Coffee Maker</i> .....	26
5.6.4. <i>Philips Hue Hue Go</i> .....	27

5.6.5. <i>Foobot Air Quality Monitor</i> .....	28
<b>6.    TEHNOLOGIJE KOJE PODRŽAVAJU IOT</b> .....	<b>29</b>
<b>6.1.    WiFi</b> .....	<b>29</b>
<b>6.2.    Bluetooth</b> .....	<b>29</b>
<b>6.3.    ZigBee</b> .....	<b>30</b>
<b>6.4.    RFID</b> .....	<b>30</b>
<b>6.5.    NFC</b> .....	<b>31</b>
<b>7.    PROBLEMI TEHNOLOGIJE IOT-A</b> .....	<b>32</b>
<b>7.1.    Sigurnosni problemi</b> .....	<b>32</b>
7.1.1. <i>Ranjivosti softvera i firmwarea</i> .....	32
7.1.2. <i>Nesigurne komunikacije</i> .....	33
7.1.3. <i>Curenje podataka</i> .....	33
7.1.4. <i>Rizici od zlonamjernog softvera</i> .....	34
7.1.5. <i>Kibernetički napadi</i> .....	35
<b>7.2.    Problemi privatnosti</b> .....	<b>35</b>
<b>7.3.    Regulatorna, pravna i etička pitanja</b> .....	<b>36</b>
<b>8.    BUDUĆNOST IOT-A</b> .....	<b>37</b>
<b>9.    ZAKLJUČAK</b> .....	<b>38</b>
<b>10.   POPIS LITERATURE</b> .....	<b>39</b>
<b>11.   POPIS SLIKA</b> .....	<b>42</b>
<b>12.   POPIS TABLICA</b> .....	<b>43</b>

# 1. UVOD

U današnje vrijeme tehnologija nam omogućuje da upravljamo svjetlima u našim domovima s radnih stanica na udaljenim radnim mjestima te da na vrlo brz način otkrijemo što se nalazi na našim policama i kada se nekom proizvodu bliži rok trajanja pomoću ugradbenih kamera i senzora (Hamza, 2021). Navedeni primjeri nisu ilustracije iz neke futurističke perspektive već samo nekoliko od mnogobrojnih IoT okvira koji se danas koriste. Trenutno na svijetu, gdje se tehnologija svakodnevno razvija, koncept Internet stvari (IoT) zaokuplja sve veću pozornost i postao je jedna od najvažnijih inovacija posljednjih godina. Internet stvari označava četvrtu industrijsku revoluciju, zajedno s robotikom, umjetnom inteligencijom, nanotehnologijom, kvantnim računalstvom, biotehnologijom, 3D ispisom i autonomnim vozilima (Alkhatib et al., 2014). IoT tehnologija naširoko se koristi u mnogim industrijama, a neke od najzujbudljivijih primjena koje će uključivati i ovaj završni rad su primjene u zdravstvu, kućanstvu, industriji, poljoprivredi te prometu i logistici. Tehnologija internet stvari ima brojne prednosti, a neke od njih su poboljšana učinkovitost kod različitih procesa, lakše i bolje praćenje i upravljanje različitim uređajima, poboljšana učinkovitost i održivost, ali to ne znači da nema i neke svoje nedostatke. Upravo ti nedostaci mali su dio ovog završnog rada.

Američka tvrtka Gartner definira IoT (Internet of Things) kao mrežu fizičkih objekata opremljenih ugrađenom tehnologijom za komunikaciju, osjećaj ili interakciju s njihovim unutarnjim stanjem ili vanjskim okruženjem (Gartner, n.d.). Uređaji tehnologija internet stvari su opskrbljeni kamerama, senzorima i ostalom elektronikom te se mogu spojiti na internet i tako razmjenjivati podatke uzajamno ili s ostalim računalima. Većina populacije koja nema veliki doticaj s tehnologijom zasigurno ne zna što je to IoT i kako tehnologije IoT-a zapravo rade. Koliko se zapravo IoT koristi i napreduje svakim danom pokazuje nam predviđanje koje govori da će do 2030. godine broj povezanih IoT uređaja biti i do 29.42 bilijuna (Statista, 2021).

Svrha ovog završnog rada je objasniti što je Internet of Things (IoT), opisati povijest razvoja IoT tehnologije, predstaviti arhitekturu IoT-a, objasniti komunikacijski model IoT tehnologije, te navesti primjene IoT-a.

Također će biti detaljno opisane tehnologije koje pružaju podršku internetu stvari, te će biti objašnjeni i primjeri problema koji su nastali s IoT tehnologijama. Nadalje, bit će iznesena predviđanja za budućnost IoT tehnologija.

Završni rad raspoređen je u deset poglavlja.

Prvo poglavlje je uvod koji kratko opisuje što je tehnologija Internet stvari te navodi temeljnu ideju završnog rada. Drugo poglavlje govori o povijesti Internet stvari gdje se opisuje razvitak tehnologija IoT-a od svojih početaka pa do danas. Treće poglavlje definira i objašnjava arhitekturu tehnologija internet stvari. Četvrto poglavlje navodi modele komunikacija u IoT tehnologijama. Ovo poglavlje će opisati četiri varijante komunikacijskog modela povezane s IoT tehnologijom, uključujući komunikaciju uređaj-uređaj, komunikaciju uređaj-oblak, komunikacijski model uređaj-usmjerivač i model dijeljenja podataka s drugim poslužiteljima. Peto poglavlje vezano je uz primjene tehnologija IoT-a. U ovom poglavlju navest će se najpoznatiji primjeri iz stvarnog života te primjeri iz raznolikih sektora. Šesto poglavlje detaljnije opisuje tehnologije koje podržavaju internet stvari i čemu one služe. Sedmo poglavlje opisuje probleme koji se javljaju korištenjem IoT tehnologija i koji su uvelike slični ili jednaki kao i kod svih današnjih novih tehnologija. Osmo poglavlje tiče se budućnosti IoT tehnologija. Opisat će se predviđanja koja se smatraju mogućima u budućnosti za tehnologiju internet stvari. Deveto poglavlje je zaključak, a deseto ujedno i posljednje poglavlje jest popis literature gdje će se nalaziti popis korištene literature te popis slika.

## 2. POVIJEST IOT-A

Koncept Internet stvari (IoT) pojavio se prije gotovo tri desetljeća, no tehnologija koja stoji iza njega postojala je i razvijala se dugi niz godina. Na tablici 1. moguće je vidjeti kronološki poredane važne događaje vezane uz pojam Internet stvari. Kronološki prva i najbitnija stvar je pojava interneta 1969. godine pod imenom Advanced Research Project Agency Network (ARPANET) i postao glavna tehnologija iz Internet stvari. Glavni ciljevi ARPANET tehnologije bili su omogućiti akademskoj i istraživačkoj zajednici dijeljenje istraživačkih radova, razvoju novih mrežnih tehnologija i povezivanje računala s brojnim zajedničkim centrima unutar Ministarstva obrane SAD-a te javnog i privatnog sektora (Bolt, Beranek, & Newman, 1981). Drugi bitan kronološki događaj je pojava RFID (Radio Frequency Identification) tehnologije zato što je ona jedna od ključnih tehnologija za Internet stvari. Premda počeci RFID-a datiraju još iz Drugog svjetskog rata, a razvitak se nastavio tijekom 1950-ih i 1960-ih godina, prvi američki patent ta RFID oznaku s memorijom koja se može prepisivati nastao je i odobrio 1973. Godine Mario W. Cardullo. U 1973. godini još je važno naglasiti da je kalifornijski poduzetnik Charles Walton primio patent za pasivni transponder za daljinsko otključavanje vrata. 1974. godine zbio se treći bitan kronološki događaj. Te godine pojavio se ugradbeni računalni sustav koji je još jedna važna tehnologija za IoT. Ugradbeni računalni sustavi implementirani su pomoću računala s jednom pločom i mikrokontrolera te se oni ugrađuju u veće sustave kako bi činili njihov sastavni dio (Manley, 1974). 1984. godine dogodio se rani primjer upotrebe Internet stvari bez da se za to onda znao naziv. Priča o tome je zapravo vrlo malo poznata, a radi se o tome da su studenti na Sveučilištu Carnegie Mello razvili sustav za praćenje sadržaja automata za prodaju Coca-Cole u kampusu kako bi izbjegli gubljenje vremena kako bi provjerili ako je automat za prodaju prazan ili ne (Teicher, 2018). Osim što su imali izvješća o zalihama, mogli su dobiti i informaciju o tome ako su novopristigla pića hladna. Peti događaj vezan uz Internet stvari jest početak rasprostranjenosti interneta na tržištima kupaca i poslovanja 1990. godine. Doduše, upotreba interneta je još uvijek bila ograničena zbog niskih performansi mrežne povezanost. Još jedna bitna stavka koja se dogodila jest ta da je John Romkey prvi u povijesti spojio toster na internet. Taj događaj smatra se nevjerojatnim zato što ljudi onda nikad nisu mogli zamisliti da će se uređaj poput tostera



moći spojiti na internet. Sredinom 1990-ih godina razvijeni su senzorski čvorovi za očitavanje podataka s jedinstveno identificiranih ugradbenih uređaja koji bi neprimjetno razmjenjivali informacije kako bi se ostvarila osnovna ideja Internet stvari (Khan, 2012). Konačno, 1999. godine Kevin Ashton kreirao je pojam Internet stvari u govoru koji je održao pred multinacionalnom tvrtkom široke potrošnje Procter & Gamble (Ashton, 2009). On je tada predložio da svaki proizvod ima RFID oznaku kako bi se proizvod mogao identificirati i kako bi se mogla pratiti određena stavka u cijelom opskrbnom lancu. U kasnim 2000-ima i ranim 2010-ima, organizacije diljem svijeta postale su jako uzbuđene zbog Internet stvari. IBM (International Business Machines) je počeo raditi na inicijativi Smarter Planet Initiative, a počinje se i objavljivati prva studija o stanju IoT tehnologije. Naposljetku, tvrtka Cisco 2011. godine dala je izjavu kako je tehnologija Internet stvari “rođena” između 2008. i 2009. godine. Cisco je to izjavio zato što je u tom razdoblju bilo više uređaja spojenih na internet nego što je bilo ljudi na planetu Zemlji.

<b>GODINA/E</b>	<b>DOGAĐAJ</b>
1969.	Nastao je internet kao Advanced Research Project Agency Network (ARPANET)
1973.	Prvi američki patent za RFID oznaku s izmjenjivom memorijom, Charles Walton – pasivni transponder za daljinsko otključavanje vrata
1974.	Ugradbeni računalni sustav
1984.	Coca-Cola aparat izvještavao o dostupnosti i hladnoći pića
1990.	Početak rasprostranjenosti interneta na tržištima kupaca i poslovanja, prvi puta spojen toster na internet
Sredina 1990-ih	Razvijeni senzorski čvorovi
1999.	Predstavljena komunikacija između dva uređaja (D2D), Kevin Ashton osmislio izraz “Internet stvari”
Kraj 2000-tih i početak 2010-ih	Organizacije diljem svijeta postale uzbuđene zbog Internet stvari, prva studija o stanju IoT tehnologije
2011.	Cisco objavio kako se Internet stvari “rodio” oko 2008. i 2009. Godine

*Tablica 1. Razvoj IoT-a kroz povijest*

### **3. ARHITEKTURA IOT-A**

Kako se tehnologija Internet stvari razvija kroz vrijeme tako su se razvijale i nove arhitekture tih tehnologija. Zbog naglog porasta broja uređaja povezanih s internetom, potrebne su nove arhitekture za upravljanje velikim količinama podataka i osiguravanje sigurnosti mreže. Kao odgovor na ovu potrebu razvijene su IoT arhitekture. Tako danas imamo dostupnu troslojnu arhitekturu, petoslojnu arhitekturu i sedmeroslojnu arhitekturu. U sljedećim odjeljcima bit će predstavljane nabrojane arhitekture, a s njima ujedno i njihove karakteristike.

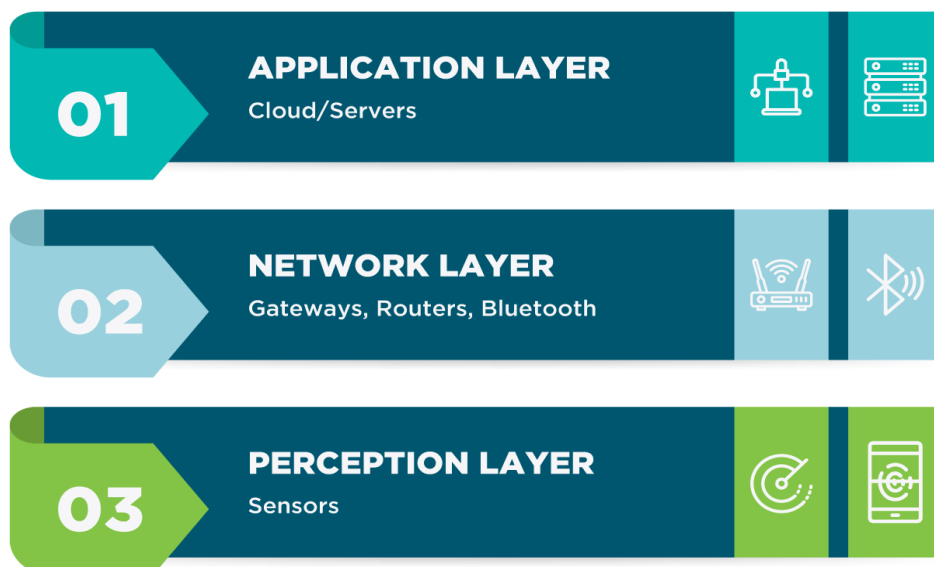
#### **3.1. Troslojna arhitektura**

Troslojna arhitektura je osnovna arhitektura Internet stvari (Wu et al., 2010). Na samom početku razvoja Internet stvari, jedina priznata arhitektura upravo je bila troslojna arhitektura. Ona se sastoji od tri sloja, a to su sloj percepcije, mrežni sloj i sloj aplikacije koji su prikazani na slici 1. Percepcijski sloj je zapravo fizički sloj ove IoT arhitekture. Njegova uloga je identificirati odnosno prepoznati svaku stvar u sustavu Internet stvari. To se ostvaruje tako da se prikupljaju informacije o svakom objektu. Percepcijski sloj uključuje tehnologije kao što su senzori, kamere, RFID oznake i čitače, 2D barkod naljepnice, GPS i druge uređaje.

Najpoznatiji senzori koji se koriste u ovom sloju su temperaturni, infracrveni i senzori tlaka. Također ovaj sloj sve prikupljene informacije pretvara u digitalne signale, koji se zatim prenose mrežnom sloju na daljnju obradu (Farooq, 2015). Drugi sloj ove arhitekture je mrežni sloj kojeg se smatra srži Internet stvari. Ovaj sloj poznat je još kao i transportni sloj. Mrežni sloj dohvaća informacije prikupljene u percepcijskom sloju gdje je onda njegova svrha ta da ih on onda prenosi i obrađuje. Također za svrhu ima još i povezivanje drugim pametnih objekata, poslužitelja i mrežnih uređaja. Tehnologije koje uključuje ovaj sloj su WiFi, Bluetooth, ZigBee, GSM, 3G, usmjerivači i drugo (Zhang, 2011). Treći i zadnji sloj troslojne arhitekture je aplikacijski sloj. Cilj ovog sloja je spojiti društvene potrebe IoT-a i industrijske tehnologije (može se smatrati srednjim slojem između industrijske

tehnologije i načina na koji se njome upravlja da se zadovolje ljudske potrebe) (Miao, 2010).

## THREE-LAYER ARCHITECTURE



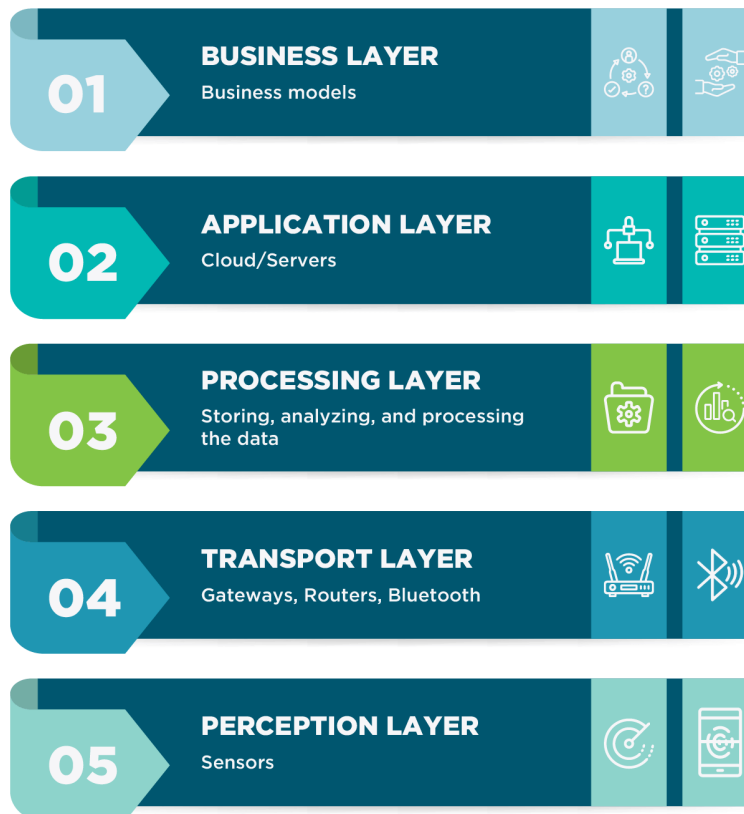
Slika 1. Troslojna arhitektura Internet stvari (izvor: <https://jelvix.com/blog/iot-architecture-layers>)

### 3.2. Petoslojna arhitektura

Kako se tehnologija Internet stvari s vremenom počela razvijati tako je troslojna arhitektura postala nedovoljna. Shodno tome nastala je petoslojna arhitektura koja je prikazana na slici 2. Ova arhitektura sastoji se od pet slojeva, a to su poslovni, aplikacijski, prijenosni, percepcijski i sloj za obradu podataka. Prvi sloj je poslovni sloj koji osigurava da korisnici mogu koristiti sustav Internet stvari bez ikakvih poteškoća. Ovaj sloj uzima neobrađene podatke i omogućuje oblikovanje uvida u grafikonima i tablicama. Pošto omogućuje da se oblikuju grafikoni i tablice na temelju toga ovaj sloj je povezan s donošenjem odluka te komunicira s dionicima. Cilj ovog prvog sloja je zapravo definirati naplatu i upravljanje IoT aplikacijama (Said & Masud, 2013). Drugi sloj zove se aplikacijski sloj i njegova svrha je odrediti vrstu aplikacije koja će se koristiti u IoT-u. Također ovaj sloj prikuplja informacije o različitim zadacima koje treba obaviti na temelju zahtjeva klijenta. Kada govorimo o IoT aplikacijama, njih je nužno stalno razvijati kako bi bile pametnije, autentificiranije i sigurnije. Sloj za obradu podataka treći je sloj petoslojne arhitekture Internet stvari. Ovaj

sloj je specijaliziran za pohranu informacija, analizu i obradu podataka, gdje podatke prikuplja percepcijski sloj. Koriste se baze podataka, računalstvo u oblaku, sveprisutno računalstvo i inteligentna obrada kako bi se pohranila velika količina prikupljenih informacija. Treći sloj ove arhitekture je iznimno bitan zato što donosi odluke na temelju analize sakupljenih podataka. Ovaj sloj ima dvije glavne faze obrade podataka, a to su prikupljanje podataka i apstrakcija podataka. Prva faza za cilj ima sortiranje prikupljenih podataka kako bi se mogli učinkovito pohraniti. U drugoj fazi podaci se usklađuju i harmoniziraju u određeni format te ih se onda smjesti na jedno mjesto kako bi im korisnici s različitih lokacija mogli vrlo lako pristupiti. Najpopularnije prijetnje trećeg sloja peteroslojne arhitekture su malware i iscrpljenost. Iscrpljenost je tip napada kojem je cilj da isprazni bateriju uređaja ili da uzme 100% obrade i memorije računala kako uređaj ne bi mogao rješavati druge zadatke koji mu se zadaju. Malware se spominje kao prijetnja zbog toga što se u ovom sloju skuplja veliki broj podataka te postoji šansa da u sustav uđu neki računalni virusi ili trojanci. Četvrti sloj je transportni sloj i on je zapravo vrlo sličan mrežnom sloju u troslojnoj arhitekturi. On prima informacije od percepcijskog sloja i šalje ih sloju za obradu podataka i obrnuto. Uključuje mnoge tehnologije, a neke id njih su WiFi i Bluetooth koje se pojavljuju i kod mrežnog sloja u troslojnoj arhitekturi te infracrvenu svjetlost. Primarni zadatak ovog sloja je adresiranje svake stvari u sustavi koristeći IPV6. Peti i posljednji sloj ove arhitekture je percepcijski sloj koji također postoji i kod troslojne arhitekture. Cilj ovog sloja je da se definira fizičko značenje svake stvari u sustavu Internet stvari, kao što su npr. lokacija i temperatura. Ovaj sloj prikuplja informacije o okolini odnosno o svakom objektu u sustavu i transformira ih u signale kao i u troslojnoj arhitekturi. Tehnologije koje se koriste u ovom sloju su RFID oznake, senzori i mnoge druge.

## FIVE-LAYER ARCHITECTURE

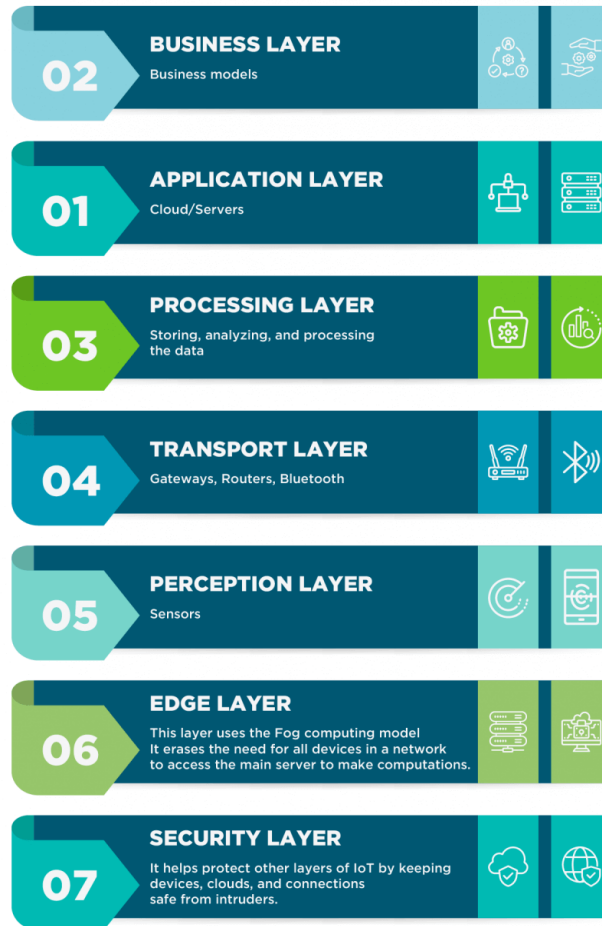


Slika 2. Petoslojna arhitektura Internet stvari (izvor: <https://jelvix.com/blog/iot-architecture-layers>)

### 3.3. Sedmeroslojna arhitektura

Sedmeroslojna arhitektura je predložena od strane istraživača tako što uzima u obzir lokalno okruženje blizu uređaja, osjetne objekte i tako dalje (Darwish, 2015). Kod ove arhitekture pojavila su se dva nova sloja koja su dodana zbog značajnog povećanja količine podataka koje obrađuju uređaji Internet stvari. Ta dva nova sloja su rubni i sigurnosni sloj. Rubni sloj se pojavio zato što kako mreže Internet stvari rastu u veličini tako se latencija pojavljuje kao jedan od glavnih izazova u pogledu performansi jer velik broj povezanih uređaja s mrežnim hubom zagušuje mrežu. Zato ovaj sloj koristi Fog računalni model koji poboljšava sustave Internet stvari koji imaju veliki opseg. Taj model uklanja potrebu da svi uređaji u mreži moraju biti povezani s glavnim poslužiteljem radi izvođenja izračuna. Umjesto toga, većina izračuna se obavlja lokalno na uređaju.

## 7 IOT ARCHITECTURE LAYER



Slika 3. Sedmeroslojna arhitektura Internet stvari (izvor: <https://jelvix.com/blog/iot-architecture-layers>)

Između ostalog ovaj model pomaže smanjiti pohranu i prijenos podataka, budući da se većina informacija pohranjuje lokalno na uređaju. Svi dodatni slojevi, u usporedbi s osnovnom IoT referentno arhitekturom (troslojna arhitektura), poboljšavaju sigurnost. Naime, sigurnost je najvažniji zahtjev za arhitekturu IoT sustava zbog mnogo različitih prijetnji s kojima se IoT uređaji i sustavi susreću svakodnevno. Kao odgovor, razvijen je sigurnosni sloj koji obuhvaća tri ključna aspekta: sigurnost uređaja, sigurnost oblaka i sigurnost veze. Sigurnost uređaja tiče se zaštite IoT uređaja od hakiranja i zlonamjernih softvera. Sigurnost u oblaku je iznimno bitna zato što se većina podataka Internet stvari obrađuje u oblaku. Posljednje glavno područje sigurnosnog sloja je sigurnost veze koja se usredotočuje na zaštitu svih podataka koji se prenose preko mreže.

## 4. KOMUNIKACIJSKI MODELI

Glavna svrha IoT tehnologije je omogućiti ljudima komunikaciju s različitim ljudima i objektima bez obzira na vrijeme, mjesto, mrežu ili uslugu koju koriste. Ovaj odlomak opisuje četiri komunikacijska modela koje je u ožujku 2015. godine Internet Architecture Board (IAB) uključio i objasnio u svom arhitektonskom dokumentu (Thaler, Hannes & Barnes, 2015). U sljedećim odjeljcima objašnjene su ključne karakteristike svakog komunikacijskog modela.

### 4.1 Komunikacija između uređaja (Device-To-Device)

Prvi komunikacijski model je komunikacija između uređaja gdje se dva ili više uređaja povezuju i komuniciraju izravno jedan s drugim, umjesto preko posredničkog poslužitelja aplikacije (Rose, Eldridge, & Chapin, 2015) što je i prikazano na slici 4. Komunikacija uređaja događa se preko interneta ili IP mreže. Međutim, često se koriste protokoli za uspostavljanje izravne komunikacije između uređaja, kao što su Bluetooth, Z-Wave ili ZigBee što se vidi i na slici 5.



Slika 4. Interakcija među uređajima u kontekstu IoT-a  
(izvor: <https://www.rfpage.com/how-does-device-to-device-communication-works/>)

Ova metoda komunikacije često se koristi u aplikacijama kao što je kućna automatizacija, gdje je potrebno razmijeniti male količine podataka između različitih uređaja pri vrlo niskim brzinama prijenosa podataka. Neki od primjera uređaja za kućnu automatizaciju koji

koriste ovaj komunikacijski model su žarulje, prekidači za svjetlo, termostati i brave na vratima. Svi ovi uređaji šalju male količine podataka jedni drugima, poput naredbe za paljenje svjetla u dnevnoj sobi. Problem koji se javlja kod ovog komunikacijskog modela je taj da uređaji koji imaju različite komunikacijske protokole ne mogu komunicirati, već uređaji moraju imati iste protokole kako bi mogli komunicirati. Primjerice, uređaji koji koriste ZigBee protokol nisu kompatibilni sa skupinom uređaja koji koriste Z-Wave protokol. Jedno ograničenje koje se javlja s ovim komunikacijskim problemom je sigurnost sustava. Uređaji koji koriste različite protokole mogu imati različite sigurnosne mehanizme i ranjivosti, što može predstavljati izazove u održavanju integriteta i zaštite podataka koji se razmjenjuju između uređaja. Uz sve navedeno, javljaju se i problemi ograničenog dometa i skalabilnosti. Ovaj komunikacijski model ima raspon komunikacije na kratke udaljenosti, što je izazovno u širim IoT mrežama koje obuhvaćaju veća područja. Kod problema skalabilnosti zapravo je potrebno osigurati IoT sustav da može učinkovito upravljati velikim brojem uređaja i održavati pouzdanu komunikaciju bez značajnog degradiranja performansi.



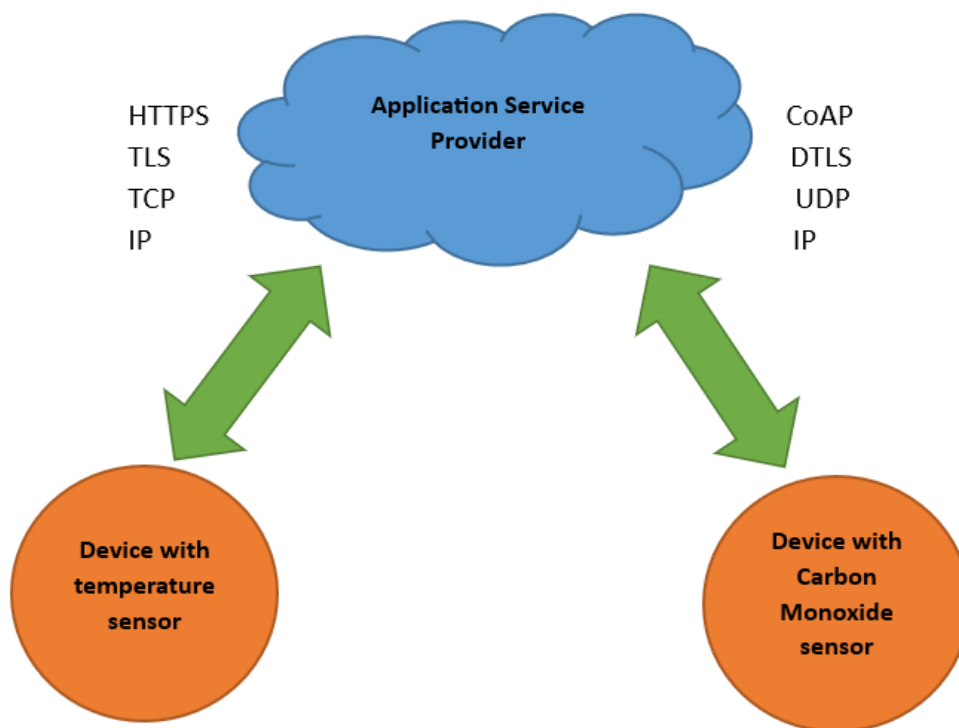
Slika 5. Komunikacija između uređaja (izvor: obrada autorice završnog rada)

#### 4.2 Komunikacija između uređaja i oblaka (Device-To-Cloud)

U komunikacijskom modelu između uređaja i oblaka, uređaj Internet stvari povezuje se direktno s Internet oblakom uslugom poput usluge aplikacija, radi razmjene podataka i upravljanja prometom poruka. Integracija IoT uređaja s oblakom omogućuje iznimno brzu razmjenu podataka i mogućnost upravljanja u trenutnom vremenu, što je posebno korisno kod uporabe IoT uređaja u industriji i kućnoj automatizaciji. Kako bi se uspostavila veza između uređaja i IP mreže te kako bi se pristupila uslugama u oblaku obično se koriste postojeći komunikacijski mehanizmi (Ethernet ili WiFi veza). To je ilustrirano na slici 6.



Uređaji komuniciraju s uslugama u oblaku pomoću protokola kao što su HTTP, TCP/IP i TLS. Nest Labs Learning termostata i Samsung SmartTV popularni su primjeri gdje se koristi komunikacija između uređaja i oblaka. Navedeni primjeri i svi ostali uređaji koji koriste ovaj komunikacijski model, bilježe podatke te ih onda šalju u bazu podataka u oblaku, gdje se ti podaci analiziraju za daljnju upotrebu. Koristi se cloud tehnologija koja omogućuje daljinski pristup uređajima koji se može ostvariti putem web sučelja ili pametnog mobitela, a omogućuje i nadogradnju softvera za te uređaje. Izazov koji predstavlja ovaj komunikacijski model je interoperabilnost pri pokušaju integracije uređaja različitih proizvođača. Kako bi komunikacijski model ispravno radio, uređaj i oblak trebaju biti od istog dobavljača (Marsan, 2015). Takvo stanje često se naziva “zaključavanjem dobavljača” gdje se sprječava korištenje drugih pružatelja usluga.

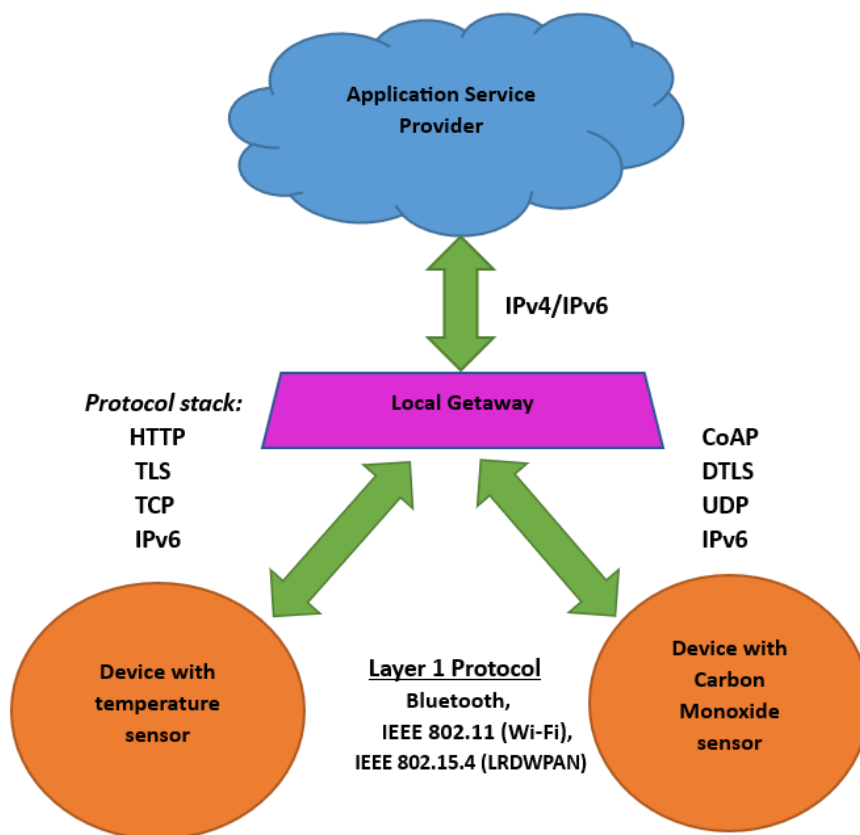


Slika 6. Komunikacija između uređaja i oblaka (izvor: obrada autorice završnog rada)

#### 4.3 Model komunikacije između uređaja i usmjerivača (Device-To-Getaway)

Treći komunikacijski model u kontekstu IoT-a je veza između uređaja i usmjerivača za razmjenu podataka s internetskim uslugama u oblaku. Ovaj tip komunikacijskog modela

prikazan je na slici 7. Pristupni uređaj radi na aplikacijskom sloju, koji se naziva aplikacijski sloj-getaway (ALG). On pokreće aplikacijski softver, djeluje kao posrednik između uređaja Internet stvari i usluga u oblaku te pretežno podržava konverziju podataka ili protokola kako bi se osigurala sigurnost. U ovom komunikacijskom modelu pametni telefon se najčešće ponaša kao pristupni uređaj gdje on ima instaliranu aplikaciju kako bi mogao komunicirati s IoT uređajima i prenositi podatke na usluge u oblaku. Pametni telefon omogućuje korisnicima da na jednostavan način upravljaju IoT uređajima putem intuitivnog korisničkog sučelja. Najpoznatiji i najčešći primjer pristupnog uređaja aplikacijskog sloja je fitness aplikacija na pametnom telefonu koja se povezuje s uređajem za praćenje tjelesne aktivnosti. Sam uređaj ne može se izravno povezati s uslugama na oblaku pa se za povezivanje mora osloniti na aplikaciju za pametno telefon kao pristupni uređaj. Osim pametnih telefona, kao primjer pristupnog uređaja navodi se hub uređaj koji se uglavnom koristi za aplikacije kućne automatizacije. Hub uređaj djeluje kao središnji

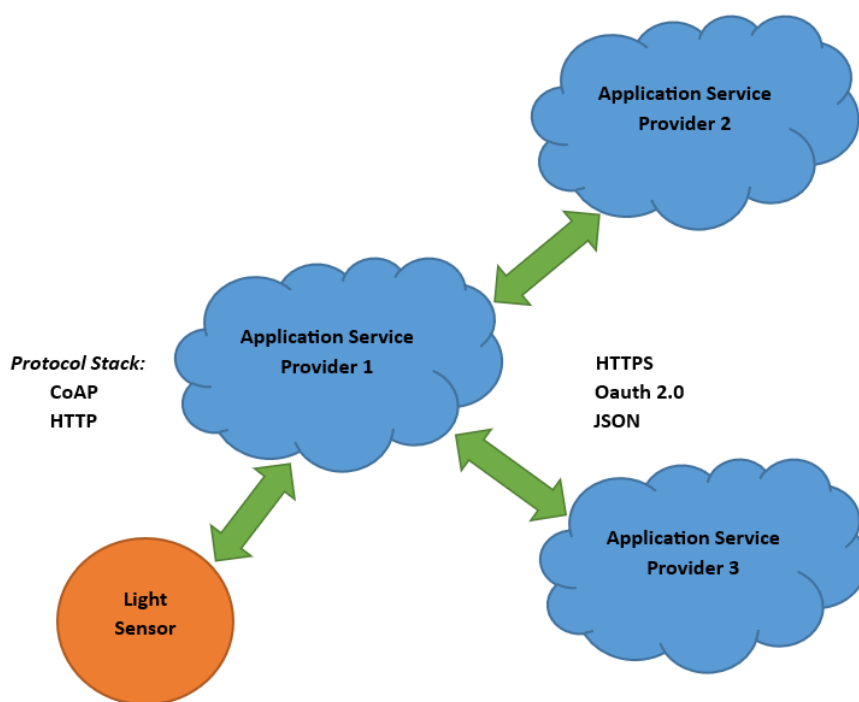


Slika 7. Model komunikacije između uređaja i usmjerivača (izvor: obrada autorice završnog rada)

upravljač te omogućuje komunikaciju između različitih uređaja internet stvari. Izazov ovog modela je to što se treba dodati sloj softverske aplikacije što na kraju rezultira povećanjem troškova i složenošću dizajna sustava. Međutim, dodatan sloj softverskih aplikacija pruža fleksibilnost i praktičnost kod upravljanja IoT uređaja putem intuitivnog korisničkog sučelja pametnog telefona ili sučelja hub uređaja.

#### 4.4. Model Dijeljenja Podataka na strani Poslužitelja (Back-End Data-Sharing)

Posljednji model komunikacije podrazumijeva dijeljenje podataka senzora koji se pohranjuju u oblaku s trećim stranama na zahtjev korisnika. Ovaj komunikacijski model omogućuje korisnicima izvoz podataka IoT uređaja iz baza podataka u oblaku te analizu podataka integracijom s drugim izvorima. Na slici 8 prikazan je model dijeljena podataka na pozadini. Taj model podržava agregaciju i analizu podataka prikupljenih s više uređaja Internet stvari. Ovaj komunikacijski model smatra se proširenjem modela komunikacije između uređaja i oblaka te ujedno pokušava prevladati ograničenja tog modela. U tradicionalnom modelu komunikacije između uređaja i oblaka, podaci s IoT uređaja prenose se samo jednom pružatelju usluge aplikacije u oblaku, tvoreći podatkovne silose.



Slika 8. Model dijeljenja podataka na strani poslužitelja (izvor: obrada autorice završnog rada)

Međutim, model dijeljenja podataka na strani poslužitelja koristi pristup federiranih usluga u oblaku kako bi omogućio interoperabilnost IoT uređaja putem sučelja za programiranje aplikacija u oblaku. Federirani pristup uslugama u oblaku zapravo omogućuje da se korisnici mogu prijaviti na jednu središnju točku provjere autentičnosti i autorizacije za pristup svim različitim uslugama u oblaku bez potrebe da se moraju prijavljivati na svaku pojedinu uslugu. Ovakav pristup uslugama u oblaku pruža korisnicima praktičnost i olakšava dijeljenje informacija s trećim stranama. To je korisno u pojedinim scenarijima kao što je korištenje podataka za analizu, istraživanje ili stvaranje novih usluga.

## 5. PRIMJENE IOT-A

U suvremenom svijetu Internet of Things (IoT) sve se više koristi u raznim područjima. Stoga će u nastavku biti navedeni primjeri različitih domena u kojima se IoT aplikacije primjenjuju, kao što su kućanstvo, industrija, zdravstvo, transportna logistika, poljoprivreda. Spomenuti će se i neki popularni uređaji internet stvari koji su trenutno u uporabi.

### 5.1. Primjena u kućanstvu

S razvojem tehnologije Interneta stvari (IoT), ona je uspješno integrirana u razna područja uključujući dom. Kako tehnologija interneta stvari ulazi u dom, pojavile su se pametne kuće koje mogu automatizirati upravljanje i kontrolu raznih kućnih uređaja i sustava. Pametna kuća je sustav upravljanja pametnim domom koji se temelji na sensorima, upravljačkim jedinicama i računalnoj tehnologiji, a obiteljima omogućuje kontrolu nad klima uređajima, rasvjeti, sigurnosti i kućanskim uređajima te drugim uređajima i sustavima putem računalne mreže (Al-Fuqaha, 2015). Primjene Internet stvari u pametnim kućama očituju se u osvjetljenju, kupaonicama, vrtovima, kuhinjama, sigurnosnim sustavima, kontroli temperature, vratima, prozorima i multimediji.

#### 5.1.1. Osvjetljenje

Danas kućna rasvjeta ima mogućnost prilagodbe osobnim potrebama (Shapel, 2023). Na primjer, kada gledate film, svjetla se mogu programirati tako da se automatski prilagode i priguše kako ne bi odvlačila pažnju i smetala prilikom gledanja filma. Također još jedan primjer pametnog osvjetljenja je da se svjetla mogu automatski upaliti kada osoba uđe u prostoriju bez potrebe za pritiskivanjem prekidača. A kada se izlazi iz kuće, sustav automatski gasi svjetla zbog uštede energije, a da o tome osoba ne mora niti razmišljati. Sva kućna rasvjeta može se povezati s pametnim telefonom, prijenosnim računalom i nekim drugim povezanim uređajima, što omogućuje da se aplikacija programira da npr. ujutro kad se oglasi alarm da se svjetla automatski upale ili kada se osoba legne u krevet da se automatski ugase svjetla.

### *5.1.2. Kupaonica*

IoT tehnologija u pametnim kućama može poboljšati udobnost i užitak svakodnevnih kupaonskih rutina te ih učiniti zabavnijima i praktičnijima. Prvi primjer IoT tehnologije u kupaonici je pametno zrcalo koje se može povezati s drugim uređajima, poput računala i pametnih telefona, kako bi moglo prepoznati lica ljudi u blizini i automatski prikazati personalizirane informacije koje osoba želi imati kao što je npr. vremenska prognoza ili specifične web stranice. Također postoje i posebni senzori koji se koriste u kupaonicama koji otkrivaju kretanje i automatski zatvaraju protok vode kada nitko nije prisutan. U tuševima u pametnim kućama postoje pametne kontrole koje omogućuju da se personalizira temperatura vode kroz aplikaciju te da se ograniči vrijeme tuširanja radi uštede vode.

### *5.1.3. Okućnica*

Tehnologija Internet stvari revolucionizira način na koji se uzgajaju biljke tako da omogućuje svakome da ima uspješan vrt bez obzira na razinu iskustva koje posjeduje. Kod upotrebe internet stvari u vrtlarstvu aplikacija prati trenutno stanje tla, provjerava ima li dovoljno vlažnosti i ako je potrebno automatski aktivira pametni sustav navodnjavanja. Ako nema dovoljno vlage, sustav pokreće navodnjavanje, a kada razina vlage dosegne optimalnu razinu, senzor to detektira i zaustavlja sustav za navodnjavanje kako bi se izbjeglo pretjerana uporaba vode. Pomoću aplikacije korisnici također mogu provjeriti ako su temperatura i vlažnost prikladni za vrstu biljke koju oni uzgajaju.

### *5.1.4. Kuhinja*

IoT i AI tehnologije u kuhinji mogu se koristiti za podršku zdravijim prehrabnim navikama potrošača, pružaju personalizirane prehrabne preporuke, omogućuju automatske kontrole obroka te prate kvalitetu hrane u stvarnom vremenu (Johare, Wagh & Shaligram, 2022). U kuhinji se koriste pametni senzori koji prate ako postoji prisutnost dima ili ugljikovog monoksida te se prati i temperatura i vlažnost zraka. Pametne ploče u kuhinji također mogu koristiti tehnologiju internet stvari gdje se oni mogu povezati s

aplikacijom kako bi se mogla prilagoditi temperatura i vrijeme kuhinja u skladu sa željama korisnika.

#### *5.1.5. Sigurnosni sustavi*

Mnogi ljudi često provjeravaju jesu li ostavili vrata i prozore zatvorene te ako su računalo, televizor ili neki drugi električni uređaj isključili prije nego što su napustili svoj dom. U takvim slučajevima u spas dolaze sigurnosni sustavi koji sve te stvari mogu napraviti pomoću specijalnih senzora. Sigurnosni sustavi u pametnim kućama mogu otkriti i spriječiti pokušaje provale, otkriti požare i upozoriti vatrogasce te koristiti senzore pokreta i kamere za praćenje aktivnosti u kući (Rupareliya, 2022). Prednost aplikacije sigurnosnog sustava je u tome što korisnik u svakom trenutku može provjeriti stanje u svom domu. Ako starije osobe borave kod kuće, vrlo ih je lako pratiti putem aplikacije kako bi im se po potrebi pružila pomoć.

#### *5.1.6. Kontrola temperature*

Pojavom pametnih kuća pojavila se i automatizacija kontrole temperature koja omogućuje prilagodbu temperature u kući prema korisničkim željama. Na primjer, korisnik u aplikaciji može podesiti da se temperatura automatski smanji kada odradi tjelovježbu ili povisi kada se otušira. Postoji i mogućnost automatske prilagodbe temperature na temelju lokacije korisnika, tako da temperatura bude optimalna kada korisnik uđe u svoj dom.

#### *5.1.7. Vrata*

Tehnologija pametnih vrata značajno se razvila u posljednjih nekoliko godina, nudeći niz značajki kao što su prepoznavanje lica, glasovne naredbe i daljinska kontrola pristupa (Paranagama & Hettige, 2022). U budućnosti, ključevi više neće biti potrebni kako bi se otvorila vrata, umjesto toga će pametna vrata koristiti tehnologiju prepoznavanja lica kako bi se otvorila. Osobe koje neće biti prepoznate kao stanovnici kuće morat će biti uvedeni u kuću od strane stanara koji tamo žive. Vrata će također imati značajku da se mogu otvoriti kako osoba prilazi kući ili zatvarati kada osoba izlazi iz kuće. Funkcija pametnih vrata koja je vrlo korisna je ta da je moguće podesiti kada se otvore ulazna vrata odnosno

kada se identificira ovlašteni korisnik kuće da se odmah upale svjetla te se također tako može upaliti TV ili bilo koji drugi uređaj koji korisnik odabere.

#### *5.1.8. Prozori*

Dinamičkom kontrolom količine sunčeve topline i vidljive svjetlosti koja ulazi u zgradu, pametni prozori imaju potencijal značajno smanjiti potrošnju energije i poboljšati udobnost korisnika (Brzezicki, 2021). Pametni prozori mogu automatski reagirati na vremenske uvjete poput kiše, snijega, oluje ili jakog vjetera te se mogu konfigurirati da se automatski zatvore kada nastupe takvi uvjeti, što je vrlo praktična značajka.

#### *5.1.9. Multimedija*

U pametnim kućama multimedija ima bitnu ulogu. Uobičajeni uređaji vezani uz multimediju koji se pojavljuju u pametnim kućama su zvučnici, televizori, uređaji za video i igranje kao što su Oculus i VR uređaji. Nešto u čemu većina ljudi danas uživa je slušanje glazbe te pristup uslugama strujanja glazbe na zvučnicima i pametnim televizorima proširuje i poboljšava iskustvo slušanja glazbe u vlastitom domu.

### **5.2. Primjena u industriji**

IoT je dobro prilagođen u arhitekturi inteligentnih proizvodnih industriji, tako da IoT uključuje posebnu kategoriju usmjerenu na aplikacije i slučajeve uporabe u modernoj industriji i proizvodnji, nazvanu industrijski internet stvari (IIoT) (Lampropoulos, Siakas & Anastasiadis, 2018). IIoT upotrebljava pametne senzore i aktuatora kako bi poboljšali proizvodnju i industrijske procese. Ključna ideja IIoT-a je da su inteligentni strojevi bolji od ljudi u hvatanju i analizi podataka u stvarnom vremenu. Jedna od karakteristika IIoT-a je da povezani senzori i aktuatori omogućuju tvrtkama da ranije identificiraju neučinkovitosti i probleme kako bi uštedjeli vrijeme i novac. Tehnologija IIoT-a je ključna u industrijskom okruženju za procese kao što su prediktivno održavanje, poboljšana terenska usluga, upravljanje energijom i praćenje imovine. Veliki broj industrija koristi tehnologije IIoT-a. Najpoznatije industrije su automobilska industrija i industrija nafte i plina. Automobilska industrija koristi IIoT uređaja u procesu proizvodnje dok se u industriji nafte i plina IIoT uređaji koristi kako bi se otkrili mogući problemi u cjevovodima. Prednosti IIoT tehnologije



su prediktivno održavanje, terensko održavanje i praćenje imovine. Kod prediktivnog i terenskog održavanja IIoT omogućuje da se problemi uvide prijevremeno kako bi se problemi mogli riješiti prije nego dođe do nekog većeg problema. Pomoću praćenja imovine proizvođači i dobavljači dobivaju informacije ako je njihova imovina oštećena ili postoji opasnost od oštećenja kako bi mogli poduzeti preventivne radnje za rješavanje problema. Najveći nedostatak vezan uz IIoT uređaje su rizici koji se odnose na sigurnost.

### **5.3. Primjena u zdravstvu**

Tehnologija interneta stvari (IoT) je revolucionirala zdravstvo omogućavanjem daljinskog praćenja pacijenata, olakšavanjem prikupljanja podataka u stvarnom vremenu i unaprjeđenjem personalizirane dostave zdravstvene skrbi (Abdalkafor, Al-Ani & Nassar, 2018). Također ta tehnologija internet stvari kroz vrijeme postaje sve više korištenija i popularnija u zdravstvenom sustavu zbog njezinih brojnih prednosti. Goleme prednosti koje se pojavljuju kod korištenja tehnologija IoT-a u zdravstvu se prije svega pojavljuju u prevenciji budućih bolesti i jednostavnom svakodnevnom praćenju zdravlja korisnika. Komponente koje se koriste za praćenje zdravlja postale su kompaktnije i prenosnije što omogućuje pacijentima da ih nose tijekom dana kako bi im se lakše pratilo trenutno zdravstveno stanje. Kako bi se to sve moglo pratiti, koristi se mreža aktuatora, senzora i drugih mobilnih komunikacijskih uređaja koji su najpoznatiji pod nazivom internet stvari-medicinski uređaji (IoTMD). Uređaji za praćenje zdravlja koji podržavaju IoT omogućuju kontinuirano praćenje vitalnih znakova, omogućujući rano otkrivanje zdravstvenih problema i pravovremenu intervenciju (Haghi Kashani et al., 2021). Veza koja se postiže između pacijenta i liječnika s udaljenim praćenjem rezultira povezanim zdravstvenim okruženjem koje olakšava brzi protok informacija i osigurava jednostavan pristup informacijama. Također još jedna prednost ove tehnologije je ta da se smanjuju ukupni troškovi skrbi za zdravlje pacijenata te se također ti prikupljeni podaci mogu analizirati u stvarnom vremenu. Sustavi zdravstva temeljeni na Internetu stvari proizvode velike količine podataka koji mogu biti iskorišteni za naprednu analitiku, prediktivno modeliranje i pružanje personalizirane medicine, unaprjeđujući tako ishode liječenja i zadovoljstvo pacijenata (Darshan & Anandakumar, 2015). Osim brojnih prednosti koje donosi primjena IoT tehnologije u zdravstvu, tehnologija se suočava i s izazovima. Neki od izazova su da

je potrebna odgovarajuća infrastruktura za obradu velikih količina podataka koji se brzo objavljuju, arhitektura aplikacija mora biti skalabilna i sposobna integrirati se s različitim vrstama uređaja i sustava te treba implementirati sigurno upravljanje identitetom budući da su povezani uređaji potencijalni sigurnosni rizik zbog svoje ranjivosti na hakiranje. Primjeri IoT uređaja u zdravstvu su Milk Nanny, Pacemaker i TempTraq. Milk Nanny uređaj je kojoj maloj djeci daje mlijeko napravljeno od mlijeka u prahu. Omjer praha i vode uvijek mora biti isto raspoređen jer ako nije to utječe na probavni sustav bebe. Ovaj uređaj je prvi potpuno automatski pametno uređaj u svijetu za pripremu formule za dojenčad te on brzo i precizno priprema svježe i toplo mlijeko za bebe tako što se pritisne gumb. Dodatna značajka uređaja je ta što se njime može upravljati izravno s pametnog mobitela (Lee, Hong, & Ryu, 2015).



Slika 9. Milk Nanny (izvor: <https://www.cnet.com/reviews/wicoz-milk-nanny-smart-formula-maker-preview/>)

Prikaz kako zapravo Milk Nanny uređaj izgleda vidljiv je na slici 9. Pacemaker je vrsta uređaja koji kontrolira ritam srca i zatim šalje odgovarajuće signale kada je to potrebno kako bi srce održalo ispravan ritam. Uređaj također bilježi obrasce srčane aktivnosti kada

se otkrije nepravilnost kod rada srca. Tu liječnici igraju važnu ulogu zato što pregledavaju i prate te podatke kako bi mogli isplanirati buduće liječenje pacijenta. Sve informacije koje Pacemaker prikupi bežično se prenose na vanjske uređaje. Sam izgled pacemakera prikazan je na slici 10. Posljednji primjer je TempTraq uređaj koji je jedini termometar s omogućenom Bluetooth tehnologijom koji kontinuirano mjeri i bilježi temperaturu djeteta 24 sata, a u obliku je mekog flastera kao što se može i vidjeti na slici 11. Sve informacije koje TempTraq sakupi šalje u stvarnom vremenu na pametni mobilni uređaj skrbnika.



Slika 10. Pacemaker (izvor: <https://kardiocentar.com/my-heart/pacemaker/>)



Slika 11. TempTraq (izvor: <https://www.prnewswire.com/news-releases/temptraq-at-ces-wearable-bluetooth-patch-monitors-body-temperature-continuously-for-48-hours-300386464.html>)

#### **5.4. Primjena u prometu (transpotru) i logistici**

Sektor transporta i logistike smatra se jednim od najnaprednijih sektora u osvajanju tehnologija internet stvari (Kumar & Dash, 2017). Također smatra se da ovaj sektor ima ključnu ulogu u razvoju. Potražnja za transportom ovisi o ponudi robe, mobilnosti putnika, logistici i mnogim drugim aspektima. Transport je ključan element u povezivanju kupaca s timovima opskrbnog lanca kroz logistiku. Logistika je sposobnost isporuke pravog proizvoda pravom kupcu po pravoj cijeni u pravom stanju, količini, mjestu i vremenu (Erturgut, 2011). Tehnologija internet stvari daje ideje za rješavanje problema koji se pojavljuju kod suvremenog transporta, a to su problemi sigurnosti, odgovornosti, pouzdanosti usluge, udobnosti, navigacije i troškova. IoT tehnologija u sektoru transporta i logistike nudi brojne mogućnosti. Upotrebljavanjem IoT tehnologije vozila se mogu pratiti u pogledu njihovog kretanja, lokacije, statusa (jesu li u pokretu ili zaustavljena) i potencijalnih rizika te se svi ti aspekti mogu inteligentno nadzirati uz pomoć sustava internet stvari. Još jedna mogućnost IoT tehnologije u ovom sektoru je to što se uz pomoć matičnog broja vozača i broja vozila putem tehnologije internet stvari može automatizirati plaćanje usluga na naplatnim kućicama ili parkiralištima. Postoje mnoge prednosti implementacije IoT tehnologije, uključujući mogućnost povećanja prihoda za vlasnike tvrtki u području transporta i logistike. Primjena IoT tehnologije omogućuje optimizaciju udaljenosti koju vozilo treba prevaliti gdje je cilj smanjenje potrošnje goriva i povećanje profita, kao i optimizacija ili preusmjeravanje ruta vozila kako bi se izbjegli nepovoljni uvjeti ili potencijalni problemi. IoT tehnologija u ovom sektoru koristi peteroslojnu arhitekturu internet stvari gdje se ta arhitektura sastoji od aplikacijskog sloja, sloja senzora, sloja komunikacije, sloja usluge i sloja infrastrukture (Rostrypa, 2022).

#### **5.5. Primjena u poljoprivredi**

IoT u poljoprivredi odnosi se na korištenje povezanih uređaja i senzora za prikupljanje i analizu podataka o rastu usjeva, vlažnosti tla i drugim čimbenicima okoliša. Jedna od ključnih primjena tehnologija internet stvari u poljoprivredi je korištenje senzora u sustavima za praćenje tla i navodnjavanje. Senzori koji se koriste mogu otkriti razinu vlage u tlu i upozoriti poljoprivrednike kada je potrebno navodnjavanje. To pomaže u

sprječavanju prekomjernog ili premalog zalijevanja, što može rezultirati oštećenjem usjeva ili smanjenim prinosima. Dodatno, IoT uređaji mogu se koristiti za udaljeno praćenje rasta i razvoja usjeva. To omogućuje poljoprivrednicima da rano prepoznaju potencijalne probleme i poduzmu korektivne mjere. Konačno, IoT se također može koristiti za automatizaciju otkrivanja i kontrole nametnika. Senzori mogu otkriti prisutnost štetočina i upozoriti poljoprivrednike na djelovanje, smanjujući potrebu za štetnim pesticidima. IoT tehnologija donosi brojne prednosti kao što su povećanje učinkovitosti i produktivnosti, automatiziranje specifičnih zadataka te poljoprivrednici uštedeju svoje vrijeme i mogu se usredotočiti na neke druge važnije stvari vezane uz njihove poljoprivredne operacije. Bez obzira na to što postoje brojne prednosti uvođenja IoT tehnologija u poljoprivredu, postoje i izazovi kod implementacije te iste tehnologije. Prvi izazov, a ujedno i najbitniji je taj što su početna ulaganja i troškovi održavanja visoki što predstavlja prepreku za male poljoprivrednike koji nemaju dovoljno financijskih sredstava kako bi uložili u tehnologiju internet stvari. Drugi izazov je taj da poljoprivrednicima nedostaju tehničke vještine i znanje odnosno određeni poljoprivrednici možda neće znati kako koristiti uređaje internet stvari ili kako analizirati podatke koji su ti uređaji prikupili. Problem koji se javlja kod svih sektora je problem upravljanja podacima i privatnosti. Većina poljoprivrednika još uvijek oklijeva dijeliti svoje podatke s pružateljima usluga trećih strana te su zabrinuti zbog kibernetičkih napada.

## **5.6. Primjeri iz stvarnog svijeta**

S razvojem vremena napreduje i tehnologija interneta stvari, a broj novih uređaja koji dolaze s njom također postaje iznimno sveprisutan u svakodnevnom životu ljudi. U nastavku su navedeni neki od najznačajnijih primjera trenutno popularnih IoT uređaja.

### *5.6.1. Google Home*

Google Home pametno je IoT uređaj koji korisnicima omogućuje uživanje u značajkama poput medija, budilice, rasvjete, termostata, upravljanja glasnoćom i mnogim drugim funkcijama koristeći samo svoj glas odnosno rečenicu "Hey Google!". Osnovne funkcije ovog IoT uređaja uključuju mogućnost upravljanja pametnim domom pomoću glasa putem platformi kao što su Nest, ZigBee, mogućnost postavljanja pitanja o vremenu, radnom

vremenu trgovine ili drugim temama, postavljanje alarma i reprodukciju glazbe sa servisa kao što je YouTube Music, Spotify i Google Play Music, s jednostavnim glasovnim naredbama (GTA, n.d.). Prikaz Google Home uređaja vidljiv je na slici 12.



Slika 12. Google Home (izvor: <https://www.wired.com/2016/11/review-google-home/>)

#### 5.6.2. August Doorbell Cam Pro

August Doorbell Cam Pro je IoT uređaj koji omogućuje korisnicima da se jave na zvono s bilo kojeg mjesta ili s udaljene lokacije. Kada se pritisne zvono na vratima, korisnik ovog IoT uređaja dobije obavijest na svojem pametnom mobitelu, a uz pomoć HD kamere u boji može se vidjeti i tko je osoba koja zvoni putem aplikacije August za pametne telefone. Također s ovim uređajem postoji i mogućnost ugradnje August pametno brave gdje pomoću nje korisnici mogu ili pustiti posjetitelja da uđe u dom jednim dodirrom u aplikaciji ili pristojno odbiti osobu (Walsh, 2017). Neke od glavnih značajka August Doorbell Cam Pro uređaja su 24 satno besplatno snimanje, jednostavan i brz postupak instalacije te kontinuirano nadziranje kućnog prilaza. Izgled samog uređaja vidljiv je na slici 13.



Slika 13. August Doorbell Cam Pro (izvor: <https://www.pcmag.com/reviews/august-doorbell-cam-pro>)

### 5.6.3. Mr. Coffee Smart Coffee Maker

Ovaj IoT uređaj olakšava korisniku da planira, prati i mijenja pripremu kave putem pametnog telefona gdje god da se korisnik nalazio. Preko mobilne aplikacije korisnicu mogu postaviti rasporede pripreme kave kako bi svježe skuhanu kava bila poslužena točno kada je korisniku potrebna. Također pomoću aplikacije može se pratiti i status pripreme kave u stvarnom vremenu, bilo da je korisnik kod kuće ili izvan kuće. Jedna od



Slika 14. Mr. Coffee Smart Coffee Maker (izvor: <https://coolmaterial.com/food-drink/the-mr-coffee-smart-coffee-maker-is-controlled-by-an-app/>)

glavnih značajka ovog pametnog uređaja je da se može prilagoditi omjer jačine kave i vode prema korisnikovim željama. Korisna značajka koju posjeduje ovaj uređaj, a bitna je svim kavoljupcima je ta da uređaj prati potrošnju vode i kave te šalje obavijest kada je potrebno promijeniti filter ili očistiti aparat. Mr. Coffee Smart Coffee Maker ima nekoliko ključnih značajki. Nudi optimalnu tehnologiju pripreme za bržu pripremu kave u manje od 7 minuta i zagrijava vodu na idealnu temperaturu za izdvajanje punog okusa kave. Također sam uređaj ima uslužni gumb za ručno upravljanje koji je vidljiv zajedno sa samim uređajem na slici 14. Dodatno, aplikacija koja se koristi za upravljanje ovim uređajem dostupna je i za Android i za Apple uređaje, što korisnicima daje potpunu kontrolu nad kuhanjem kave sa svog pametnog telefona bez obzira koji pametan uređaj posjeduju (Bennett, 2014).

#### 5.6.4. Philips Hue Hue Go

Philips Hue Hue Go svestrano je prijenosno svjetlo koje donosi beskrajne mogućnosti kao što su mogućnost prilagodbe scene osvjetljenja ili odabir neke od unaprijed programiranih opcija, a vidljiv je na slici 15. Karakteristike ovog IoT uređaja su da se može upravljati putem Bluetootha ili WiFi-ja, ima prirodne dinamičke efekte te ima klizač na vrhu koji je vrlo praktičan kako bi korisnik mogao podesiti osvjetljenje i prilagoditi ambijent prema svojim preferencama. Također ovaj uređaj se može glasovno upravljati. Philips Hue podržava usluge kao što su Amazon Alexa i Google Assistant kada je povezan s kompatibilnim uređajima kao što su Google Nest ili Amazon Echo (Samsung, n.d.).



Slika 15. Philips Hue Hue Go (izvor: <https://simply-leds.com.au/products/philips-hue-go-portable-light>)



### 5.6.5. Foobot Air Quality Monitor

Foobot je pouzdan uređaj internet stvari koji pomaže u mjerenju onečišćenja zraka u zatvorenim prostorima i poboljšava kvalitetu zraka u domovima, radnim okruženjima i zatvorenim javnim mjestima. On osjeća nevidljive zagađivače bez mirisa u okolišu i prikazuje ih na svom LED zaslonu. Jednim pogledom na LED zaslon, boja i intenzitet svjetla korisniku odmah govori ako je zrak u njegovom domu kao da je u šumama Alpa ili na ulicama Los Angelesa (Foobot, n.d.). Prednosti korištenja Foobota su da pomaže u poboljšanju koncentracije i energije tako što korisnik udiše svježiji zrak te korisnik može kontrolirati razinu vlažnosti i temperature što je vrlo korisna značajka. Sam prikaz uređaja vidljiv je na slici 16.



Slika 16. Foobot Air Quality Monitor (izvor: <https://techgage.com/article/understanding-your-air-quality-a-review-of-the-foobot-indoor-air-quality-monitor/>)

## 6. TEHNOLOGIJE KOJE PODRŽAVAJU IOT

Razne tehnologije igraju ključnu ulogu u omogućavanju IoT sustava. Neke od njih koje će biti i objašnjene u nastavku su WiFi, Bluetooth, ZigBee, senzori, RFID i NFC.

### 6.1. WiFi

Wi-Fi je tehnologija bežičnog umrežavanja koja koristi radiovalove za pružanje brzog bežičnog pristupa internetu (WaTech, n.d.). WiFi je imao primarnu ulogu u donošenju inovacija u Internet stvari, pružajući sveprisutnu povezanost kako bi povezao različite "stvari" jedne s drugima, s internetom i s ostalim velikim brojem uređaja diljem svijeta koji koriste WiFi. Korištenje WiFi tehnologije sa sustavom internet stvari omogućuje automatizaciju pametnih domova, praćenje opskrbnih lanaca i drugih važnih funkcija u stvarnom vremenu te povećava produktivnost i učinkovitost u poslovnim radnim okruženjima. IoT aplikacije imaju različite zahtjeve povezivanja u smislu pokrivenosti, protoka podataka, energetske učinkovitosti i cijene uređaja. Najčešće se odabire WiFi zato što pomoću njega signal je pokriven gotovo posvuda u zgradi, ali nekad WiFi tehnologija nije pravi izbor. Kod prijenosa podataka u IoT-u mogu se prenositi ili male količine podataka ili iznimno velike količine podataka te domet može varirati između iznimno malih dometa pa čak do nekoliko kilometara dometa. Svi ti faktori utječu na izbor tehnologije koje će IoT sustav koristiti. Prednosti korištenja WiFi-ja su niski troškovi infrastrukture i uređaja, lakoća implementacije te prisutnost pristupne točke. Neki od nedostataka su velika potrošnja energije, srednji domet te zagušenje frekvencijskog spektra.

### 6.2. Bluetooth

Bluetooth bežična tehnologija je jeftina bežična tehnologija kratkog dometa. Učinkoviti domet Bluetooth tehnologije je od 10 do 100 metara i obično komunicira brzinama ispod 1 Mbps. Ova tehnologija koristi standardnu specifikaciju IEEE 802.15.1. te se koristi za stvaranje osobne mreže (PAN) (Chadha, Singh & Pardeshi, 2013). Skupina Bluetooth uređaja koji dijele zajednički komunikacijski kanal zove se Piconet. Piconet može podržavati maksimalno 8 uređaja za razmjenu podataka u isto vrijeme, a ti podaci mogu

biti tekst, slika, video ili zvuk. Postoji Bluetooth Low Energy ili skraćeno BLE koji je oblik Bluetootha optimiziran za uređaje niske potrošnje te pomaže uređajima internet stvari da ostanu u stanju mirovanja kada nisu povezani kako bi štedjeli energiju. BLE je idealna tehnologija za IoT aplikacije zato što se može upariti i ponovno povezati s uređajima u 6 milisekundi dok je tradicionalnom Bluetoothu potrebno 6 sekundi. Ta činjenica poboljšava operativnu učinkovitost i povećava dostupnost opreme. Velika prednost Bluetooth tehnologije je to što je jeftinija za implementaciju od drugih komunikacijskih protokola.

### **6.3. ZigBee**

ZigBee je bežični mrežni protokol male snage temeljen na standardu IEEE 802.15.4 (Chen & Jin, 2012). Ovaj proizvod karakterizira niska cijena, niska brzina prijenosa podataka, relativno mali domet prijenosa, skalabilnost, pouzdanost i fleksibilan dizajn protokola. ZigBee ima domet od oko 100 metara i propusnost od 250 kbps, a topologije u kojima se primjenjuje su zvijezda, klaster stablo i mreža. Ova tehnologija najčešće se koristi u kućnoj automatizaciji, digitalnoj poljoprivredi, industrijskoj kontroli, medicinskom nadzoru i sustavima napajanja, sa sigurnom mrežnom vezom i dugim vremenom rezervnog napajanja baterije. Jedna od glavnih razlika u usporedbi s Bluetoothom i WiFijem je ta što je ZigBee jeftiniji. Samim time što je jeftiniji povećava mu se izvedivost njegove primjene u aplikacijama internet stvari.

### **6.4. RFID**

Radiofrekvencijska identifikacija (RFID) je sustav koji koristi radio valove za bežični prijenos identiteta predmeta ili osobe u obliku serijskog broja (Sun, 2012). RFID tehnologija ima važnu ulogu kod IoT-a zato što rješava problem identifikacije objekata oko nas na ekonomičan način (Aggarwal & Lal Das, 2012). Ovisno o tome kako se RFID oznaka opskrbljuje energijom, dijeli se u tri kategorije: aktivni RFID, pasivni RFID i poluaktivni RFID. Aktivni RFID sustav upotrebljuje oznake s ugradbenim izvorom napajanja, a najčešće je to obična baterija. Aktivne RFID oznake imaju veći domet te mogu prikupiti i prenijeti više podataka, ali su uz sve te prednosti skuplje od pasivnih oznaka. Pasivni RFID sustavi nemaju vlastiti izvor napajanja nego se napajaju elektromagnetskim poljem koje stvara RFID čitač. Također pasivne RFID oznake imaju kraći domet i prenose

manju količinu podataka. Poluaktivna RFID oznaka ima kombinaciju aktivnih i pasivnih komponenti. RFID tehnologija sastoji se od oznake, čitača, antene, kontrolera pristupa, softvera i poslužitelja. Prednosti korištenja RFID tehnologije su pouzdanost, učinkovitost, sigurnost, preciznost, cijena te sićušna veličina oznake koja omogućuje njihovo upotrebu u bilo kojem području bez obzira na uvjete okoline. Primjer upotrebe RFID tehnologije koji je iznimno bitan je 24-satna podrška pacijentima u zdravstvu tako što se stalno prati srčani ritam te se obavještava medicinsko osoblje s redovitim ažuriranjem kako bi medicinsko osoblje uvijek znalo u kojem stanju su njihovi pacijenti.

### **6.5. NFC**

Near-Field Communication ili skraćeno NFC je skup komunikacijskih protokola koji omogućuju komunikaciju između dva uređaja na bliskom dometu (Ong, 2021). NFC uređaji dijele se na dva tipa, a to su pasivni i aktivni uređaji. Aktivni mogu slati i primiti informacije, a primjer aktivnog NFC uređaja je pametni telefon. Pasivni NFC uređaji mogu prenositi informacije kada ih aktivni uređaj čita, ali oni sami ne mogu čitati informacije. U današnjem svijetu NFC tehnologija koristi se u brojne svrhe, a neke od njih su povezivanje s elektroničkim uređajima samo jednim klikom, preuzimanje digitalnog sadržaja i obavljanje bežičnih transakcija. Prednosti ove tehnologije su jednostavno povezivanje, brze transakcije i lakoća razmjena podataka. Također ova tehnologija obuhvaća značajke kao što su enkripcije za smanjenje mogućnosti prisluškivanja i drugih zlonamjernih aktivnosti.

## 7. PROBLEMI TEHNOLOGIJE IOT-A

Tehnologija IoT-a omogućuje velik broj mogućnosti i prednosti, ali s time dolaze i brojni izazovi. Kako tehnologija internet stvari sve više prodire u naš svakodnevni život, pojavljuju se razni problemi na koje se treba obratiti pažnja. Najveći problemi vezani uz navedenu tehnologiju su sigurnosni problemi, problemi privatnosti i regulatorna, pravna i etička pitanja. U sljedećim odlomcima bit će svaki problem detaljnije objašnjen.

### 7.1. Sigurnosni problemi

Da bi korisnici prihvatili i na kraju i koristili tehnologiju interneta stvari, bitno je da imaju povjerenje u sigurnost interneta, povezanih aplikacija i uređaja. Ako korisnici ne vjeruju u sigurnost tih elemenata, postoji mala vjerojatnost da će se takva tehnologija široko prihvatiti i koristiti globalno. Pet uobičajenih IoT sigurnosnih problema koja će u nastavku biti opisani su ranjivosti softvera i firmwarea, nesigurne komunikacije, curenje podataka, rizici od zlonamjernog softvera i kibernetički napadi.

#### 7.1.1. Ranjivosti softvera i firmwarea

Osigurati sustav internet stvari vrlo je izazovno zato što pametno uređaji imaju ograničene resurse i računalnu snagu te zbog toga ne mogu pokrenuti snažne sigurnosne značajke koje zahtijevaju velike resurse. Zbog toga se stvaraju sigurnosni nedostaci vezani uz ranjivost softvera i firmwarea. Jedan od ključnih problema u sigurnosti sustava internet stvari su slabe kontrole pristupa. Korisnici često ne slijede najbolje prakse pri postavljanju sigurnosnih postavki ili ne mijenjaju zadane lozinke na svojim uređajima. Osim toga, korisnici često ne ažuriraju svoje uređaje, što ograničava zakrpavanje sigurnosnih rupa. Ažuriranja često više ne podržavaju starije verzije softvera i firmvera što pruža priliku za napadanje otkrivenih sigurnosnih rupa. Kako bi se smanjile ranjivosti softvera i firmwarea u tehnologiji internet stvari, iznimno je bitno provoditi redovita ažuriranja softvera i firmwarea. Ažuriranja daju proizvođačima priliku da poprave sigurnosne nedostatke i uvedu poboljšanja značajki. Također od iznimne važnosti su sigurnosni mehanizmi kao što su enkripcija i autentifikacija kako bi se zaštitili podaci i spriječili neovlašteni pristupi povezanim uređajima.

### *7.1.2. Nesigurne komunikacije*

Tradicionalne sigurnosne mjere nisu učinkovite u osiguravanju komunikacije IoT uređaja zbog toga što većina postojećih sigurnosnih mehanizama je izvorno dizajnirana za stolna računala. Nesigurna komunikacija izaziva brojne prijetnje, a jedna od najopasnijih je mogućnost napada čovjeka u sredini (MitM). Ako uređaj internet stvari ne koristi sigurnu enkripciju i mehanizme provjere autentičnosti, napadač može vrlo lako izvesti MitM napad kako bi poremetio proces ažuriranja i preuzeo kontrolu nad željenim uređajem. Uz to napadači također mogu i instalirati zlonamjerni softver ili čak promijeniti funkcionalnosti uređaja te time ugroziti privatnost i sigurnost korisnika. Kibernetički kriminalci mogu presresti podatke koji se razmjenjuju između povezanih uređaja ako uređaj šalje podatke u obliku otvorenih poruka. Time se otvara mogućnost prisluškivanja i krađe osjetljivih podataka, poput osobni podataka ili povjerljivih poslovnih informacija. Prethodno navedene sigurnosne prijetnje ukazuju na potrebu implementacije snažnih sigurnosnih mehanizama kao što su šifriranje lozinkom, autentifikacija i sigurni komunikacijski protokoli. Vrlo je važno educirati korisnike o sigurnosnim praksama i potaknuti ih da redovito ažuriraju softver i firmware svojih IoT uređaja kako bi se smanjile ranjivosti i zaštitili osjetljivi podaci.

### *7.1.3. Curenje podataka*

Curenje podataka u sustavu internet stvari je situacija u kojoj osjetljivi podaci iz IoT sustava dopijevaju u ruke neovlaštenim osobama. Ti osjetljivi podaci najčešće uključuju lokaciju korisnika, podaci o bankovnom računu, medicinsku dokumentaciju ili podatke o korisniku kako bi se ti podaci iskoristili za krađu identiteta. Curenje podataka najčešće se događa zbog nesigurnosti komunikacijskih kanala, nedostatka enkripcije ili lošeg upravljanja podacima. Primjer curenja podataka iz stvarnog svijeta je da su Ring pametno zvona slala korisničke podatke tvrtkama kao što je to Facebook i Google bez njihovog osobnog pristanka. Do ovakvog curenja podataka došlo je zato što je bila aktivirana usluga praćenja trećih strana u mobilnog aplikaciji za pametno uređaj Ring. Ovakvi incidenti jasno pokazuju važnost sigurnosti i zaštite privatnosti u IoT sustavima, te potrebu za strožim sigurnosnim mjerama i transparentnošću u prikupljanju i korištenju podataka.

#### 7.1.4. Rizici od zlonamjernog softvera

Kod tehnologija internet stvari rizici od zlonamjernog softvera su iznimno veliki problem. Napadači koji uspe pronaći način kako da ubace zlonamjerni softver u sustav internet stvari mogu promijeniti njihovu funkcionalnost, prikupiti korisnikove osobne podatke te čak pokrenuti i neke druge napade. Pojedini uređaji mogu već biti zaraženi virusom kada se tek otvore i uključe zato što proizvođač uređaja nije osigurao odgovarajuću sigurnost softvera. Ako malware uspije ući u IoT uređaj može iznimno brzo proširiti svoju infekciju na druge postojeće uređaje na mreži te stvari lančanu reakciju zaraze. Svi navedeni rizici zahtijevaju da se pažljivo upravlja sigurnošću i zaštitom sustava internet stvari kako bi se izloženost zlonamjernim prijetnjama svela na potpuni minimum. To uključuje redovito ažuriranje softvera i firmwarea, korištenje antivirusnih i sigurnosnih programa te strogo praćenje i kontrolu pristupa uređajima i mrežama. Na slici 17 može se vidjeti prikaz tri glavne kategorije prijetnji IoT sustavu.

Area of concern	Threats
<b>Devices/Things</b> <ul style="list-style-type: none"><li>• Devices capable of two-way data transmission</li><li>• Active sensors, meters, traffic light, camera, local gateways</li></ul>	<ul style="list-style-type: none"><li>• Compromised device:<ul style="list-style-type: none"><li>○ Botnet</li><li>○ Cryptojacking</li><li>○ Proxy for malicious activities</li><li>○ Data leakage</li></ul></li><li>• Infected software installation and access to IoT Application server</li><li>• SIM removal</li></ul>
<b>Network</b> <ul style="list-style-type: none"><li>• 2G/3G/4G</li><li>• Sigfox, Lora</li><li>• NB-IoT, CAT-M1</li><li>• 5G</li><li>• WiFi</li></ul>	<ul style="list-style-type: none"><li>• Eavesdropping</li><li>• Device DoS</li><li>• Call, SMS, Data interception</li><li>• IMSI profile reconfiguration</li><li>• DDoS</li></ul>
<b>IoT Application cloud/server</b> <ul style="list-style-type: none"><li>• Interface with customer</li><li>• Data processing</li><li>• Device connectivity provisioning and management</li></ul>	<ul style="list-style-type: none"><li>• Remote access to the devices</li><li>• Device DoS</li><li>• User data leakage</li></ul>

Slika 17. glavne kategorije prijetnji IoT sustavu (izvor: <https://procomp.ba/blog/kako-odabrati-najbolji-antivirusni-program/>)

### *7.1.5. Kibernetički napadi*

Sustavi internet stvari podložni su raznim kibernetičkim napadima, a najčešće vrste napada su napadi uskraćivanja usluge (DoS), napadi uskraćivanja stanja mirovanja (DoSL), pokušaj krivotvorenja uređaja, fizička provala i napad temeljen na aplikacijama. Napad uskraćivanjem usluge ili skraćeno DoS je kibernetički napad koji pokušava spriječiti ispravno funkcioniranje sustava internet stvari tako što ih preplavljuje zahtjevima, čime se onda preopterećuju resursi. DoSL je kibernetički napad koji iskorištava ranjivost u MAC protokolu kako bi natjerao senzore uređaja internet stvari da se nepotrebno probude iz stanja mirovanja, kako bi im ispraznio bateriju i onesposobio ih. Pokušaj krivotvorenja uređaja je kibernetički napad u kojem napadač nastoji lažirati identitet uređaja internet stvari kako bi mogao steći kontrolu nad mrežom ili pokušava ugroziti integritet podataka. Fizička provala vrsta je kibernetičkog napada koji se svodi na fizički pristup i manipulaciju nad uređajima i infrastrukturom sustava internet stvari. Posljednja vrsta napada je napad temeljen na aplikacijama koji se usredotočuje na sigurnosne propuste u aplikacijama koje se koriste u sustavima internet stvari. Napadi temeljeni na aplikacijama iskorištavaju slabost u firmwareu ili softveru samog uređaja.

### **7.2. Problemi privatnosti**

Kod tehnologije internet stvari pojavljuju se mnogi problemi vezani uz privatnost zbog masovnog prikupljanja i analize osobnih podataka. Glavni nedostatak ove tehnologije je što korisniku nedostaje kontrola nad podacima odnosno IoT uređaji često nemaju korisničko sučelje putem kojeg korisnici mogu konfigurirati postavke privatnosti kako bi moguće prikupljanje podataka o njima bilo prihvatljivo. Ako se koristi više različitih izvora podataka istovremeno može se iznimno detaljno stvoriti korisnički profil gdje se onda povećava mogućnost zlouporabe korisničkih podataka. Trenutak kada se pojavio problem s privatnošću je kada je započela migracija tehnologije nadzora iz javnih u privatne prostore zbog toga što su očekivanja privatnosti drugačija u privatnom prostoru svake osobe. Također problem koji se javlja da u današnje vrijeme IoT uređaji često rade u okruženjima gdje se prikupljaju isti podaci za više ljudi kao što je npr. kada senzori u automobile prate lokaciju svih osoba prisutnih u vozila, bez obzira željeli to putnici vozila



ili ne. U današnjem svijetu većina ljudi zbog česte prisutnosti uređaja internet stvari stvaraju lažni osjećaj sigurnosti što potiče pojedine ljudi da otkrivaju svoje osjetljive podatke bez da su svjesni toga te uz to ne razume posljedice koje dolaze s otkrivanjem vlastitih osjetljivih podataka. Svi problemi vezani uz privatnost podataka dovode do potrebe jasnih smjernica i propisa kako bi se definiralo kako se podaci prikupljeni putem IoT uređaja prikupljaju, koriste i dijele. Nadalje iznimno je bitno educirati korisnike o mogućim rizicima kako bi mogli imati kontrolu nad svojim osobnim podacima. Zadnja bitna stvar kod rješavanja problema privatnosti je da je potrebno povećati odgovornost za proizvođače uređaja internet stvari. Svaki proizvođač bi trebao jasno objasniti o svrsi prikupljanja podataka te pružiti korisniku da odabere postavke privatnosti koji njemu odgovaraju.

### **7.3. Regulatorna, pravna i etička pitanja**

Kako se tehnologija internet stvari brzo razvija, tako rastu i regulatorni, pravni i etički izazovi povezani s privatnošću korisnika (European Commission, 2013). Pojava uređaja internet stvari uvodi nove pravne i političke izazove koji prije nisu postojali, a istovremeno pojačavaju mnoge postojeće probleme. Pojava IoT uređaja povezanih s osobama s invaliditetom stvorila je nove izazove za pristupačnost tih uređaja. Uvođenje novih vrsta IoT uređaja zahtijeva usklađivanje s postojećim standardima gdje bi se umjesto toga trebalo stvoriti novi standardi za te uređaje. Novi izazovi koji se javljaju su pravna i regulatorna pitanja povezana s intelektualnim vlasništvom, odlaganjem IoT uređaja u okoliš te vlasništvom uređaja u smislu treba li IoT uređaj biti u vlasništvu osobe ili samo u iznajmljivanju. Uzimajući u obzir sve te izazove, iznimno je važno razmotriti načine zaštite privatnosti korisnika na temelju internetskih društvenih načela koja potiču povezanost, izražavanje, inovacije, dijeljenje izbor i povjerenje. Pravne i regulatorne smjernice trebale bi postojati kako bi se zaštitila privatnost korisnika te ujedno i osigurala odgovornost pružatelja IoT usluga. Posebno treba voditi računa o transparentnosti prikupljanja i korištenja podataka kako bi sami korisnici mogli imati kontrolu nad svojim osobnim podacima.

## 8. BUDUĆNOST IOT-A

U budućnosti tehnologije internet stvari potrebno je riješiti probleme s kojima se trenutno uređaji internet stvari suočavaju, a navedeni su u prošlom odjeljku. Zbog ranjivosti u dizajnu i implementaciji IoT uređaja može se dogoditi neovlašteni pristup podacima, pa čak i kontrola samog uređaja (Abomhara & Koien, 2018). Posljedica toga je da se trebaju razviti sigurnosni standardi i mehanizmi koji će osigurati zaštitu korisničkih podataka i privatnosti. Kako su se pojavili problemi vezani uz privatnost tako je u budućnosti potrebno uskladiti regulatorne okvire i pravne norme s tim problemima kako bi se osigurala zaštita privatnosti korisnika (European Commission, n.d.). Bitna stvar koju je potrebno riješiti u budućnosti je interoperabilnost između različitih uređaja i platformi internet stvari. Kako će vrijeme prolaziti tako će sve više različitih uređaja morati raditi zajedno i međusobno razmjenjivati podatke kako bi svojim korisnicima mogli pružiti najbolje iskustvo. Zbog toga potrebna je standardizacija kako bi se postigla kompatibilnost i integracija između različitih ekosustava internet stvari (Miorandi et al., 2012). U budućnosti, razvitak energetski učinkovitih uređaja postat će značajan faktor zato što će milijarde uređaja biti povezane te bi razvoju takvih uređaja smanjio utjecaj na okoliš. Kao i u svim područjima tako i u ovom umjetna inteligencija (AI) imat će bitu ulogu u budućnosti internet stvari. Integracijom umjetne inteligencije u uređaje internet stvari omogućit će analizu ogromne količine podataka te automatizaciju procesa. Prednosti koje donosi integracija umjetne inteligencije su povećanje učinkovitosti, povećana produktivnost i smanjenje troškova.

## 9. ZAKLJUČAK

U posljednjih nekoliko godina tehnologija internet stvari doživjela je značajan razvoj. Kako se razvijala tako je postala i dio svakodnevice većine ljudi u današnjem svijetu. Tehnologija internet stvari ima bogatu povijest gdje se razvilo više vrsta arhitektura, a to su troslojna arhitektura koja se smatra osnovnom arhitekturom, petoslojna i sedmeroslojna arhitektura. Razvojem tehnologije internet stvari razvijale su se i različite vrste komunikacijskih modela koje omogućuju razmjenu podataka i informacija između različitih uređaja u mreži. Tehnologija internet stvari sve više se uvodi u različite industrije, kućanstva, zdravstvo, transport i logistiku, poljoprivredu i druge brojne sektore. Zbog pojave IoT uređaja u brojnim sektorima pojavljuju se i brojni popularni uređaji koji se koriste svakodnevno kao što su to Google Home, Philips Hue Hue Go, Foobot Air Quality Monitor, Mr. Coffee Smart Coffee Maker, August Doorbell Cam Pro i mnogi drugi.

IoT tehnologija igra bitnu ulogu u omogućavanju povezivanja i komunikacije između uređaja u sustavu internet stvari. Primjenom IoT uređaja osigurava se mogućnost prikupljanja podataka u stvarnom vremenu, automatizacija procesa, povećanje učinkovitosti i optimizacije, praćenje te analitiku i prediktivno održavanje.

Iz ovog završnog rada lako je zaključiti kako prednosti IoT tehnologije brojčano premašuju nedostatke, ali ti nedostaci nikako se ne bi trebali ignorirati jer se tiču sigurnosti i privatnosti. Zbog problema koji se javljaju jasno je kako tehnologija internet stvari još uvijek nije postigla svoj maksimum.

Uspjeh odnosno postizanje maksimuma tehnologije internet stvari u budućnosti ovisi o rješavanju sigurnosnih problema i problema privatnosti, regulatornih, pravnih i etičkih pitanja te problema interoperabilnosti. Također u budućnosti iznimno je bitno razviti energetske učinkovite IoT uređaje koji bi smanjili onečišćenje okoliša.

## 10. POPIS LITERATURE

1. Disruptive Technologies. (2021). Beginner's Guide to Internet of Things (IoT). Dostupno na: [Beginner's Guide to IoT](#). [Pristupljeno: 28.04.2023.]
2. Alkhatib, H., Faraboschi, P., Frachtenberg, E., Kasahara, H., Lange, D., Laplante, P., Merchant, A., Milojevic, D., Schwan, K. (2014). What Will 2022 Look Like? The IEEE CS 2022 Report. Washington, DC, USA: IEEE Computer Society.
3. Gartner. (n.d.). Internet of Things. Dostupno na: <https://www.gartner.com/en/information-technology/glossary/internet-of-things> [Pristupljeno: 04.05. 2023.]
4. Statista. (2021). Number of connected devices in the Internet of Things (IoT) worldwide from 2015 to 2030 (in billions) [Graph]. [online] Dostupno na: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/> [Pristupljeno: 01.05.2023.]
5. Bolt, R., Beranek, L., Newman, R. (1981). A history of the ARPANET: the first decade. DARPA Report No. 4799. Cambridge, MA, USA: Bolt Beranek and Newman Inc.
6. Manley, J.H. (1974). Embedded computers: software cost considerations. In AFIPS '74 Proceedings of the May 6–10, 1974, National Computer Conference and Exposition (pp. 343-347). New York, NY, USA: ACM Press.
7. Teicher, J. (2018). The little-known story of the first IoT device. [online] Dostupno na: <https://www.ibm.com/blog/little-known-story-first-iot-device/>. [Pristupljeno: 04.05.2023.]
8. Khan, R., Khan, S.U., Zaheer, R., & Khan, S. (2012). Future internet: the internet of things architecture, possible applications and key challenges. In Proceedings of Frontiers of Information Technology (FIT), pp. 257-260.
9. Ashton, K. (2009). That 'Internet of Things' Thing. RFID Journal.
10. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010). Research on the architecture of internet of things. In Proceedings of the 3rd IEEE international conference on advanced computer theory and engineering, China.
11. Farooq, M., Waseem, M., Khairi, A., & Kamal, T. (2015). A Review on Internet of Things (IoT). International Journal of Computer Applications, 113, 1-7.
12. Zhang, Y. (2011). Technology Framework of the Internet of Things and Its Application. In Electrical and Control Engineering (ICECE), pp. 4109-4112.
13. Miao, W., Ting, L., Fei, L., Ling, S., & Hui, D. (2010). Research on the architecture of Internet of things. In IEEE International Conference on Advanced Computer Theory and Engineering (ICACTE), Sichuan province, China (pp. 484-487).
14. Said, O., & Masud, M. (2013). Towards Internet of Things: Survey and Future Vision. International Journal of Computer Networks (IJCN), 5(1), 1-17.
15. Darwish, D. (2015). Improved Layered Architecture for Internet of Things. International Journal of Computing Academic Research (IJCAR), 4(4), 214-223.
16. Thaler, D., Hannes, T., & Barnes, M. (2015). Architectural considerations in smart object networking. IETF 92 Technical Plenary—IAB RFC 7452.
17. Rose, K., Eldridge, S., & Chapin, L. (2015). The Internet of Things: An Overview. Internet Society.

18. Marsan, D. C. (2015). IAB releases guidelines for internet-of-things developers. IETF Journal, 11(1), 6-8. Internet Engineering Task Force.
19. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.
20. Shapel, M. (2023). IoT Home Automation. Sam-Solutions. [online] Dostupno na: <https://www.sam-solutions.com/blog/iot-home-automation/>. [Pristupljeno: 09.05.2023.]
21. Johare, K. P. (1), Wagh, V. G. (2), Shaligram, A. D. (3). (2022). Present and Future Possibilities for Intelligent Kitchen with AI and IoT. IRE Journals, 6(3), 122.
22. Rupareliya, K. (2022). IoT Smart Home Security: Benefits, Use Cases, and Top Devices. Intuz. [online] Dostupno na: <https://www.intuz.com/blog/iot-smart-home-security-benefits-use-cases-and-top-devices>. [Pristupljeno: 15.05.2023.]
23. Paranagama, C., & Hettige, B. (2022). A Review on Existing Smart Door Lock Systems.
24. Brzezicki, M. (2021). 'A Systematic Review of the Most Recent Concepts in Smart Windows Technologies with a Focus on Electrochromics', Sustainability, 13(17), 9604.
25. Lampropoulos, G., Siakas, K., & Anastasiadis, T. (2018). Internet of Things (IoT) in Industry: Contemporary Application Domains, Innovative Technologies and Intelligent Manufacturing. International Journal of Advanced Scientific Research and Engineering, 4, 109-118.
26. Abdalkafor, Ahmed & Al-Ani, Khalid & Nassar, Aiman. (2018). The Internet of Things-A Survey.
27. Haggi Kashani, M., Madanipour, M., Nikravan, M., Asghari, P., Mahdipour, E. (2021). A systematic review of IoT in healthcare: Applications, techniques, and trends. Journal of Network and Computer Applications.
28. K. R., Darshan, R., & K. R., Anandakumar. (2015). A Comprehensive Review on Usage of Internet of Things (IoT) in Healthcare System. In International Conference on Emerging Research in Electronics,
29. Lee, J., Hong, M., & Ryu, S. (2015). Sleep Monitoring System Using Kinect Sensor. International Journal of Distributed Sensor Networks, 2015, 1-9.
30. Kumar, N. M., & Dash, A. (2017). Internet of Things: An Opportunity for Transportation and Logistics.
31. Erturgut, R. (2011). Increasing demand for logistics technician in business world and rising trend of logistics programs in higher vocational schools: Turkey case. Procedia - Social and Behavioral Sciences, 15, 2776-2780.
32. Rostrypa, D. (2022). IoT in Logistics & Transportation: How It Works, Use Cases, and Benefits. Stormotion. [online] Dostupno na: <https://stormotion.io/blog/iot-in-logistics-transportation/#iot-transportaion-industry-layers> [Pristupljeno: 05.05.2023.]
33. GTA. (n.d.). Google Home. [online] Dostupno na: <https://www.gta.net/iot-devices/google-home/>. [Pristupljeno: 29.04.2023.]
34. Walsh, T. (2017). August Doorbell Cam Pro review. Digital Trends. [online] Dostupno na: <https://www.digitaltrends.com/home/august-doorbell-cam-pro-review/>. [Pristupljeno: 16.05.2023.]

35. Bennett, B. (2014). Mr. Coffee Smart Optimal Brew review: A smarter Mr. Coffee that brews weakly and needs more connected-home links. CNET. [online] Dostupno na: <https://www.cnet.com/reviews/mr-coffee-10-cup-smart-optimal-brew-coffeemaker-wemo-enabled-review/>. [Pristupljeno: 11.05.2023.]
36. Samsung. (n.d.). Hue White i Color Ambiance Prijenosno svjetlo Go (najnoviji model). [online] Dostupno na: <https://www.lighting.philips.hr/consumer/p/hue-white-i-color-ambiance-prijenosno-svjetlo-go--najnoviji-model-/7602031P7.reviewandawards> . [pristupljeno: 04.05.2023.]
37. Foobot. (n.d.). The air quality monitor you need. [online] Dostupno na: <https://foobot.io/features/>. [Pristupljeno: 07.05.2023.]
38. WaTech. (n.d.). WiFi definition and meaning. Dostupno na: <https://watech.wa.gov/WiFi-definition-and-meaning>. [Pristupljeno: 09.05.2023.]
39. Chadha, S. S., Singh, M., & Pardeshi, S. K. (2013). Bluetooth Technology: Principle, Applications and Current Status.
40. Chen, X.-Y., & Jin, Z.-G. (2012). Research on Key Technology and Applications for the Internet of Things. *Physics Procedia*, 33, 561-566.
41. Sun, C. (2012). Application of RFID Technology for Logistics on Internet of Things. *AASRI Procedia*, 1, 106-111.
42. Aggarwal, R., & Lal Das, M. (2012). RFID Security in the Context of "Internet of Things". *First International Conference on Security of Internet of Things, Kerala*, 17-19, 51-56.
43. Ong, D. (2021). How Near-Field Communication (NFC) Works: Benefits of NFC for IoT and the Real-world. *Seeed Studio*. [online] Dostupno na: <https://www.seeedstudio.com/blog/2021/05/19/how-near-field-communication-nfc-works-benefits-of-nfc-for-iot-and-the-real-world/>. [Pristupljeno: 07.05.2023.]
44. European Commission, Directorate-General for Communications Networks, Content and Technology, Cave, J., Robinson, N., Hackett, P. et al. (2013) Europe's policy options for a dynamic and trustworthy development of the Internet of things – Final report. *Publications Office*.
45. Abomhara, M., & Koien, G. M. (2018). Internet of Things Security and Privacy: Challenges and Solutions. In *2018 4th International Conference on Information Management (ICIM)* (pp. 104–109).
46. European Commission. (n.d.). Internet of Things Policy. [online] Dostupno na: <https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy>. [Pristupljeno: 10.05.2023.]
47. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), 1497-1516.

## 11. POPIS SLIKA

Slika 1. Troslojna arhitektura Internet stvari (izvor: <a href="https://jelvix.com/blog/iot-architecture-layers">https://jelvix.com/blog/iot-architecture-layers</a> ).....	6
Slika 2. Petoslojna arhitektura Internet stvari (izvor: <a href="https://jelvix.com/blog/iot-architecture-layers">https://jelvix.com/blog/iot-architecture-layers</a> ).....	8
Slika 3. Sedmeroslojna arhitektura Internet stvari (izvor: <a href="https://jelvix.com/blog/iot-architecture-layers">https://jelvix.com/blog/iot-architecture-layers</a> ).....	9
Slika 4. Interakcija među uređajima u kontekstu IoT-a.....	10
Slika 5. Komunikacija između uređaja (izvor: obrada autorice završnog rada).....	11
Slika 6. Komunikacija između uređaja i oblaka (izvor: obrada autorice završnog rada)..	12
Slika 7. Model komunikacije između uređaja i usmjerivača (izvor: obrada autorice završnog rada).....	13
Slika 8. Model dijeljenja podataka na strani poslužitelja (izvor: obrada autorice završnog rada) .....	14
Slika 9. Milk Nanny (izvor: <a href="https://www.cnet.com/reviews/wicoz-milk-nanny-smart-formula-maker-preview/">https://www.cnet.com/reviews/wicoz-milk-nanny-smart-formula-maker-preview/</a> ).....	21
Slika 10. Pacemaker (izvor: <a href="https://kardiocentar.com/my-heart/pacemaker/">https://kardiocentar.com/my-heart/pacemaker/</a> ) .....	22
Slika 11. TempTraq (izvor: <a href="https://www.prnewswire.com/news-releases/temptraq-at-ces-wearable-bluetooth-patch-monitors-body-temperature-continuously-for-48-hours-300386464.html">https://www.prnewswire.com/news-releases/temptraq-at-ces-wearable-bluetooth-patch-monitors-body-temperature-continuously-for-48-hours-300386464.html</a> ).....	22
Slika 12. Google Home (izvor: <a href="https://www.wired.com/2016/11/review-google-home/">https://www.wired.com/2016/11/review-google-home/</a> ) .	25
Slika 13. August Doorbell Cam Pro (izvor: <a href="https://www.pcmag.com/reviews/august-doorbell-cam-pro">https://www.pcmag.com/reviews/august-doorbell-cam-pro</a> ) .....	26
Slika 14. Mr. Coffee Smart Coffee Maker (izvor: <a href="https://coolmaterial.com/food-drink/the-mr-coffee-smart-coffee-maker-is-controlled-by-an-app/">https://coolmaterial.com/food-drink/the-mr-coffee-smart-coffee-maker-is-controlled-by-an-app/</a> ) .....	26
Slika 15. Philips Hue Hue Go (izvor: <a href="https://simply-leds.com.au/products/philips-hue-go-portable-light">https://simply-leds.com.au/products/philips-hue-go-portable-light</a> ).....	27
Slika 16. Foobot Air Quality Monitor (izvor: <a href="https://techgage.com/article/understanding-your-air-quality-a-review-of-the-foobot-indoor-air-quality-monitor/">https://techgage.com/article/understanding-your-air-quality-a-review-of-the-foobot-indoor-air-quality-monitor/</a> ).....	28
Slika 17. glavne kategorije prijetnji IoT sustavu (izvor: <a href="https://procomp.ba/blog/kako-odabrati-najbolji-antivirusni-program/">https://procomp.ba/blog/kako-odabrati-najbolji-antivirusni-program/</a> ) .....	34

## 12. POPIS TABLICA

Tablica 1. Razvoj IoT-a kroz povijest.....	4
--	---



## **Sažetak i ključne riječi (Abstract and keywords)**

Danas Internet stvari (IoT) igra sve važniju ulogu u životima ljudi. Koncept IoT-a odnosi se na povezivanje različitih uređaja i objekata putem interneta kako bi se podaci mogli razmjenjivati i analizirati na daljinu. Primjena IoT tehnologije proširila se na mnoga područja, a neka od njih su zdravstvo, industrija i poljoprivreda. Cilj ovog završnog rada je dati detaljan pregled IoT tehnologije, uključujući njezinu povijest i razvoj, kao i prednosti i nedostatke. Također cilj je objasniti kako IoT zapravo funkcionira i kako se koristi u različitim područjima. Predstaviti će se i primjeri iz stvarnog svijeta koji pokazuju kako IoT tehnologija može poboljšati učinkovitost i produktivnost u različitim sektorima. Opisat će se prognoze i trendovi u budućnosti koji su povezani s IoT tehnologijom. Ovaj završni rad istaknuti će i izazove ove tehnologije, a to su sigurnosti problemi, problemi privatnosti i regulatorna, pravna i etička pitanja.

Abstract - Today, the Internet of Things (IoT) is increasingly important in people's lives. IoT refers to the interconnection of various devices and objects through the internet, enabling data exchange and remote analysis. The application of IoT technology has expanded to many areas, including healthcare, industry, and agriculture. This final paper aims to provide a detailed overview of IoT technology, including its history and development, as well as its advantages and disadvantages. The report also aims to explain how IoT works and how it is used in different fields. Real-world examples will demonstrate how IoT technology can enhance efficiency and productivity in various sectors. Future forecasts and trends related to IoT technology will be described. This final paper will also highlight the challenges of this technology, including security issues, privacy concerns, and regulatory, legal, and ethical issues.

**Ključne riječi:** internet stvari, budućnost internet stvari, primjena internet stvari, povijest internet stvari, komunikacija internet stvari, arhitektura internet stvari

**Keywords:** Internet of Things, future of IoT, IoT applications, history of IoT, IoT communication, IoT architecture