Privatnost i sigurnost podataka unutar IoT okruženja

Rendulić, Jelena

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:864590

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-05-06**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Jelena Rendulić

PRIVATNOST I SIGURNOST PODATAKA UNUTAR IOT OKRUŽENJA

DIPLOMSKI RAD

Zagreb, 2022.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

PRIVATNOST I SIGURNOST PODATAKA UNUTAR IOT OKRUŽENJA

PRIVACY AND DATA SECURITY IN THE IOT ENVIRONMENT

Mentor: izv. prof. dr. sc. Goran Vojković **Student: Jelena Rendulić**

JMBAG: 0177045174

Zagreb, svibanj 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 25. svibnja 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Telekomunikacijska legislativa i standardizacija**

DIPLOMSKI ZADATAK br. 6502

Pristupnik: **Jelena Rendulić (0177045174)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Privatnost i sigurnost podataka unutar IoT okruženja**

Opis zadatka:

Internet stvari (eng. Internet of things) relativno je novi pojam u današnjem svijetu iako se razvija već dugi niz godina. Tome najviše doprinosi napredak i razvoj tehnologija i sustava koji omogućuju takva okruženja. Veliki problem koji se danas javlja je pitanje sigurnosti podataka, odnosno privatnosti pojedinca u takvom okruženju bilo da se radi o pametnim kućama, pametnim gradovima ili drugim pametnim sustavima. Ovaj rad stavit će naglasak na sigurnosne propuste Internet of things okruženja i kroz različite primjere prikazati probleme s kojima se suočavaju pojedinci koji takva okruženja razvijaju, staviti kontekst takvog okruženja unutar pravnih okvira na razini Europske Unije i na razini Republike Hrvatske, te na kraju analizirati rezultate provedene ankete.

Mentor:

izv. prof. dr. sc. Goran Vojković

Predsjednik povjerenstva za diplomski ispit:

SAŽETAK

Internet stvari postao je sastavni dio svakodnevnog života ljudi diljem svijeta. Od pametnih mobilnih uređaja pa sve do pametnih domova i gradova, ljudi su okruženi brojnim senzorima i kamerama koji neumorno prikupljaju statističke podatke o njima. Sastavljanjem svih prikupljenih podataka može se dobiti cjelokupna slika o načinu života pojedinca, njegovim navikama, ponašanju, rutama kretanja, stavovima, njegovom zdravstvenom stanju i privatnom životu. Slikovito, to bi značilo da je život pojedinca izložen kao na dlanu. Zvuči kao špijuniranje i narušavanje zakona, ali ne, to je samo tehnologija koja je dio Industrije 4.0. Stvari u okolini postaju sve pametnije i sve više preuzimaju ulogu čovjeka, a ljudi sve više ovise o toj tehnologiji ne shvaćajući koliko su podaci u takvom sustavu ugroženi. Sve to povlači pitanja odgovornosti pojedinaca, kompanija, državnih, standardizacijskih i pravnih tijela. U konačnici tehnologiju je nemoguće zaustaviti, ali je moguće poduzeti korake za kontrolu iste.

KLJUČNE RIJEČI: Internet stvari; privatnost; sigurnost; uređaj; podaci

SUMMARY

Internet of things technology has become an integral part of daily human's life. From smart mobile phones to smart homes and cities, people are surrounded by numerous sensors and cameras that collect statistics about them. Compiling all collected data would give a complete picture of the individual's lifestyle, his habits, behaviour, movements, attitudes, health and private life. Figuratively, this would mean that human life is exposed as in the palm of hand. It sounds as spying and breaking the law, but no, it's just part of Industry 4.0 technology. Things in the environment are getting smarter and more taking the human role, so people are becoming more dependent on this technology not realizing how much data is compromised in such system. But, question is who is responsible, starting from individuals, companies, states, standardization companies and legislators. In the end, technology is impossible to stop, but is possible to control it.

KEYWORDS: Internet of things; privacy; security; device; data

SADRŽAJ

1. UVOD

Internet stvari najraširenija je tehnologija na svijetu. Postala je neizostavan dio svakodnevnice čovjeka i život bez nje danas je gotovo nezamisliv. Gotovo je nemoguće zamisliti život bez mobilnih uređaja, sve više pametnih satova i ostalih prijenosnih uređaja na koje se ljudi sve više oslanjaju i koji čine njihov život jednostavnijim i organiziranim. Pametni uređaji sve su više počeli preuzimati ulogu čovjeka, toliko da ljudi ponekad zaborave loše osobine takvog pametnog okruženja. Zvuči idealno pratiti svoju statistiku treninga na pametnom satu, broj otkucaja srca, broj prijeđenih koraka, pa na kraju dana i pogledati svoju rutu kretanja uspoređujući podatke s podacima prethodnih dana. Razne kompanije i gospodarstva opstala su za vrijeme krize uzrokovane COVID-19 virusom upravo iz razloga što su se okrenule tehnologiji Internet stvari pa im je danas nezamislivo vratiti se na stare navike jer im je posao postao automatiziran i olakšan upravljanjem na daljinu. Zvuči idealno do onog trenutka kada na portalu osvane vijest o još jednoj hakerskoj kampanji.

Svakodnevno raste broj uređaja Interneta stvari, sve više su gradovi opremljeni novim kamerama i senzorima u svrhu postizanja statusa „pametnog“ grada. Rastom broja uređaja raste i broj podataka koji se mogu prikupiti o pojedincu, te zaokružiti cijelu sliku njegova privatnog i društvenog života. Zvuči kao da se privatnost u takvom okruženju gubi, no zapravo je i više od toga. U pitanju je privatnost, sigurnost, reputacija, imovina, integritet, zaštita, zdravlje i sami život pojedinca koji u takvom sustavu lako može biti ugrožen.

Tehnologija svakim danom sve više napreduje i taj je razvoj nemoguće zaustaviti. No međutim, moguće je stvoriti prije svega standardizacijske i zakonske okvire koji će tu istu pametnu tehnologiju kontrolirati i nadzirati, prema kojima će biti moguće povući kaznenu i pravnu odgovornost. Također, moguće je raditi na buđenju svijesti pojedinaca prisiljavajući korisnike da koriste metode zaštite počevši od minimalnih sigurnosnih politika poput konkretnih složenih zaporka, pa do onih većih, sve u svrhu njihove zaštite. Premda je Internet stvari već dugo poznata tehnologija, dan danas je njen najveći nedostatak nedovoljna privatnost i sigurnost podataka, odnosno korisnika. Upravo ovaj rad razrađuje temu privatnosti i sigurnosti podataka analizirajući ugroze i ranjivosti sustava te nudeći određene metode zaštite istog, a sve to u standardizacijskim i pravnim okvirima kroz sedam tematskih jedinica.

1. Uvod
2. Okruženje Internet stvari
3. Narušavanje privatnosti i sigurnosti
4. Metode zaštite
5. Zakonski okvir Interneta stvari
6. Analiza provedene ankete
7. Zaključak

U drugom poglavlju opisano je okruženje Internet stvari i pojedinačne komponente sustava. Uz to opisane su različite referentne i aktualne arhitekture Interneta stvari te područja primjene istog u privatnom životu čovjeka i industriji.

U trećem poglavlju opisano je narušavanje privatnosti i sigurnosti kroz četiri sloja arhitekture Interneta stvari konkretno kroz fizički sloj, sloj mreže, podataka i aplikacije. Ovo poglavlje opisuje najčešće mete napada kroz primjere različitih industrija i objekata. Uz to bavi se pitanjem nepovjerenja korisnika u sustav Interneta stvari, te utjecajem krize uzrokovane COVID-19 virusom na okruženje Interneta stvari s aspekta privatnosti i sigurnosti.

Četvrto poglavlje bavi se okvirom kibernetičke sigurnosti, sigurnosti prema referentnoj arhitekturi i sigurnosnim praksama.

Peto poglavlje razrađuje zakonske okvire i legislativu u kontekstu Interneta stvari. Za okosnicu je naveden primjer zakonodavstva Sjedinjenih Američkih Država kao svjetske velesile u tehnologiji i industriji, uredbe i direktive Europske Unije te kako su iste implementirane u zakonodavni sustav Republike Hrvatske. U ovom poglavlju navedena su i tijela zadužena za informacijsku sigurnost Republike Hrvatske.

U šestom poglavlju prikazana je analiza provedene ankete kojom su se ispitivale svakodnevne navike i svijest potrošača o okruženju Interneta stvari s aspekta sigurnosti, odnosno koliko su svjesni činjenice koji se podaci o njima prikupljaju, te koliko vjeruju takvom sustavu.

2. Okruženje Internet stvari

U današnje vrijeme, svjedoci smo sve većeg i bržeg razvoja tehnologije i promjena modernog doba. Taj napredak najviše se vidi i osjeti u informacijsko komunikacijskim tehnologijama (eng. Information and Communications Technology – ICT), koje su postale neizostavan dio svakodnevnice današnjeg čovjeka. Brzim rastom tehnologije, dolazi do velikog razvoja i proizvodnje raznih bežičnih uređaja, što dovodi i do sve većeg broja ljudi povezanih na Internet.

Jedan od prvih primjera Interneta stvari (eng. Internet of things – IoT) iz ranih je 1980-ih, a bio je Coca Cola stroj smješten na Sveučilištu Carnegie Mellon[1]. Lokalni programeri povezivali bi se putem Interneta s hlađenim aparatom i provjerili ima li piće na raspolaganju i je li hladno prije nego što bi krenuli da ga kupe.[1] Britanski tehnolog Kevin Ashton "skovao" je frazu „Internet of Things" još 1999. godine kao naslov prezentacije dok je radio za Procter i Gamble, a trebalo je još barem čitavo desetljeće da tehnologija uhvati korak sa vizijom o međusobnoj povezanosti uređaja.[2] U članku iz 2009. godine "Ta 'Internet stvari' stvar" (eng. "That 'Internet of things' thing"), Ashton navodi da su danas računala, a samim tim i Internet, gotovo u potpunosti ovisni o ljudima. Gotovo svih otprilike 50 petabajta[2] podataka dostupnih na Internetu prvo su snimili i stvorili ljudi, upisivanjem, snimanjem kamerom i mikrofonom ili skeniranjem barkoda.[3]

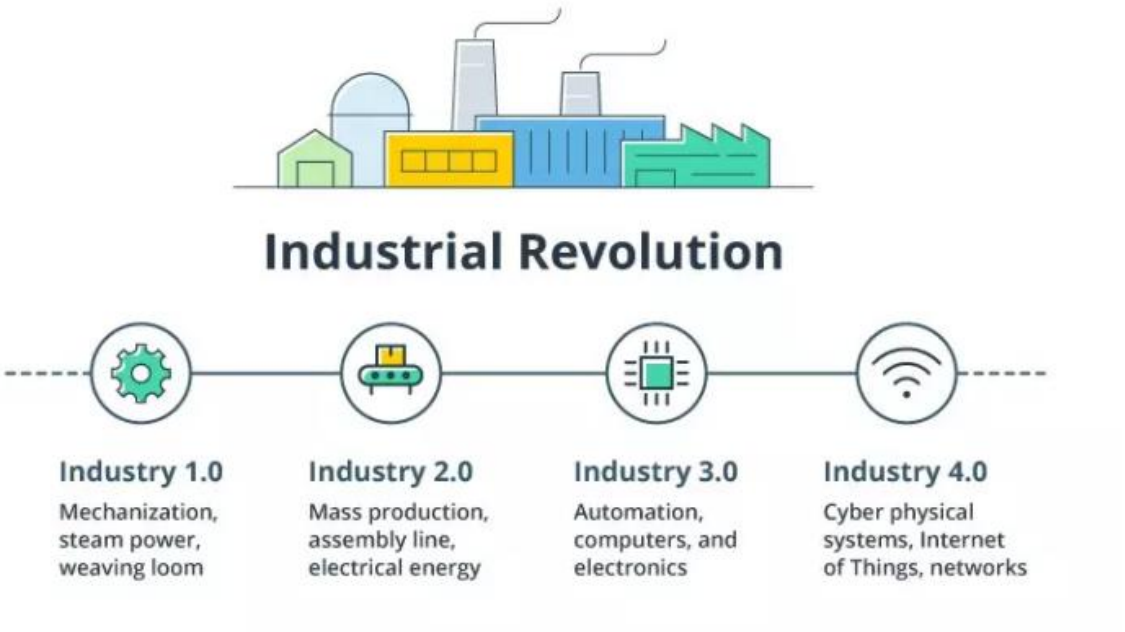
Mnogo je različitih definicija IoT-a, no jedna od najkraćih je iz projekta IoT-A (eng. Internet of Things Architecture) prema kojoj je to globalna mreža koja povezuje pametne stvari. Uređaji koji aktivno sudjeluju u komunikaciji u takvoj mreži najčešće su senzori ili aktuatori, a "stvar" u takvom okruženju može biti bilo koja stvar iz naše okoline s mogućnošću komunikacije s Internetom poput primjerice elektromotora, termometra, automobila, nadzornih kamera i dr.[4] Ukratko, IoT je sustav u kojem će objekti u stvarnom svijetu imati senzore, biti spojeni na Internet i dijeliti informacije s uređajima na mreži. Svaki senzor pratit će specifične informacije poput pomaka odnosno kretanja, temperature, lokacije, vibracije i bit će povezan sa senzorima ostalih uređaja u okolini. Specifičnosti objekta iz fizičkog svijeta su:

- Ima jedinstveni identifikator i povezan je na Internet;
- Komunicira i kontinuirano generira podatke;
- Ima mogućnost primanja podatka iz mreže i naredbi za konfiguraciju;
- Može izvršiti određene aktivnosti – aktuator (električki ili mehanički);
- Može primati podatke od drugih objekata, obrađivati ih i slati dalje na obradu u računalni oblak.[5]

[1] Carnegie Mellon University je privatno istraživačko sveučilište smješteno u Pittsburghu, Pennsylvania, SAD.

[2] 1Petabajt = 1024 terabajta.

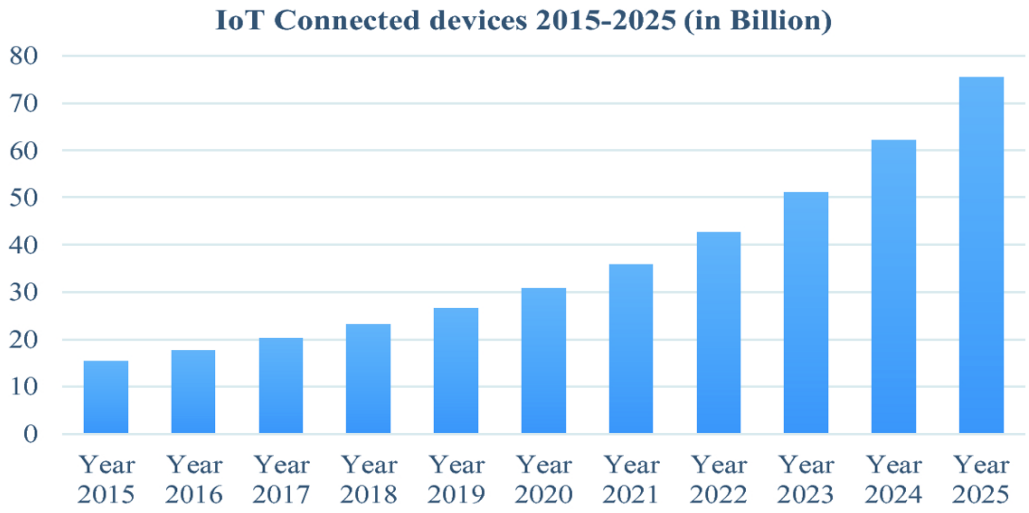
Internet stvari dio je 4. Industrijske revolucije[3]. Na slici 1. kronološki su prikazane industrijske revolucije do danas. Prisutan je u različitim područjima poput kućanstva, financija, zdravstva, logistike, pametnih gradova, autoindustrije, poljoprivrede, a cilj mu je povezati sve uređaje na Internet koji će stalno biti povezani i neprekidno razmjenjivati informacije u svrhu pravovremenosti, ekonomičnosti, povećanja kvalitete života ljudi, smanjenja troškova i povećanja prihoda.[6]



Slika 1. Prikaz industrijskih revolucija kroz povijest, [7]

Iako je ideja Interneta stvari već odavno poznata, razlog zbog kojeg se danas sve više spominje je broj uređaja spojenih na Internet, koji raste eksponencijalno. Već 2011. godine broj uređaja povezanih na Internet bio je veći od broja stanovnika na Zemlji, a predviđa se da će 2025. godine broj uređaja povezanih na Internet premašiti 80 milijardi.[8] Prikaz rasta broja uređaja spojenih na Internet kroz godine vidljiv je na slici 2.

[3] Četvrta industrijska revolucija ili Industrija 4.0 odnosi se na industriju današnjeg doba koja je usredotočena na kombiniranje tradicionalne proizvodnje s najnovijom praksom, pametnom tehnologijom. Prvenstveno radi na ostvarenju *machine to machine* (M2M) komunikacije i implementacije Interneta stvari radi pružanja automatizacije, poboljšanja komunikacije i kontrole, te na pametnim uređajima koji mogu vršiti analizu i dijagnosticirati probleme bez potrebe posredovanja čovjeka.[9]



Slika 2. Rast broja uređaja na Internetu kroz godine, [10]

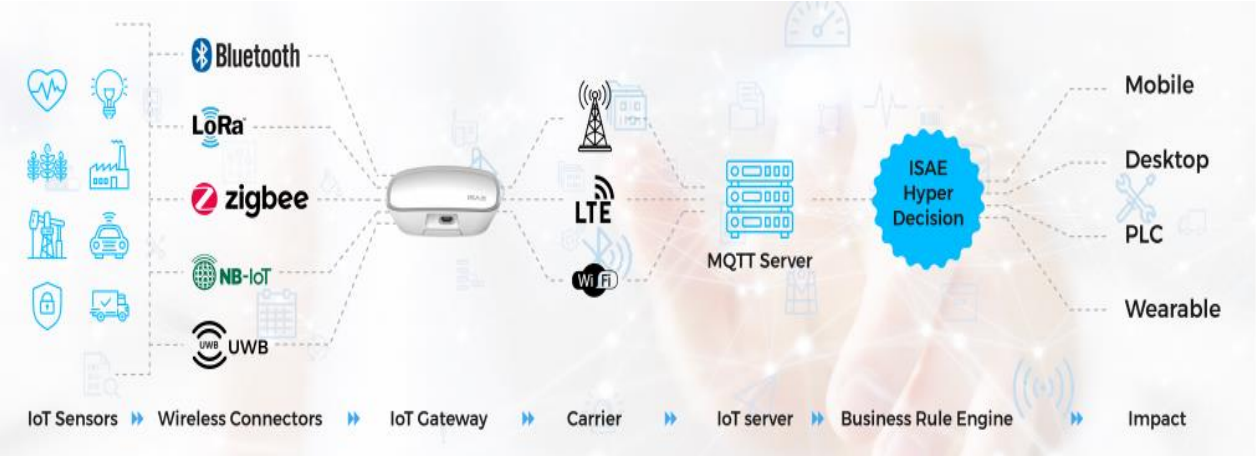
2.1. Komponente Interneta stvari

Okruženje IoT, sastoji se od pametnih uređaja spojenih na Internet koji koriste ugrađene sustave kao što su procesori, senzori i komunikacijski hardver za prikupljanje, slanje, djelovanje na podatke koji su prikupljeni iz okruženja. IoT uređaji dijele podatke prikupljene preko senzora sa IoT pristupnikom (eng. Gateway) preko kojeg se podaci šalju u oblak (eng. Cloud) kako bi se analizirali. Ponekad ti uređaji komuniciraju jedni s drugima (M2M[4] tehnologija) te djeluju na temelju prikupljenih informacija bez potrebe za ljudskom interakcijom.[11]

Kao što svaki sustav ima svoje komponente, tako je i IoT sustav sastavljen od različitih komponenti koje obavljaju svoju ulogu i koje su prikazane na slici 3. Jedna od podjela je sljedeća:

1. Senzori,
2. Mreža,
3. Oblak,
4. Korisničko sučelje.[12]

[4] Machine to Machine (M2M) odnosi se na postavljanje bežične ili žičane mreže koje omogućuje uređajima iste vrste mogućnost slobodne komunikacije. Ova vrsta sustava može se koristiti na različite načine i napredovala je tijekom posljednjih nekoliko desetljeća stvaranjem globalnih internetskih i IP mreža, omogućujući poboljšanu i učinkovitu komunikaciju na velikim udaljenostima i između velikog broja uređaja.[13]



Slika 3. Komponente IoT sustava, [12]

2.1.1. Senzori

"Stvari" u IoT okruženju "oživljavaju" zahvaljujući senzorima. Postoje različiti senzori primjerice temperaturni, senzori vlage, tlaka, ugljikovog dioksida (CO_2), senzori pokreta, svjetla, blizine, RFID (eng. Radio Frequency Identification) oznake[5] i dr. Oni su ti koji su na neki način prva linija IoT okruženja i preko njih se prikupljaju podaci koji se dalje transferiraju u mehanizam odlučivanja.[12] Primjer iz stvarnog života bio bi temperaturni senzor u kući. Senzor prikuplja podatke u prostoriji i u onom trenutku kada temperatura premaši postavljeni temperaturni prag, šalje se informacija mehanizmu za odlučivanje, koji obradom prosljeđuje uputu elektromotoru za otvaranje vrata i prozora kako bi se prostorija rashladila. Ovaj primjer ujedno je primjer prednosti IoT-a jer na ovaj način moguće je pravovremeno djelovanje na izvanredne okolnosti. Takvih primjera uz ovaj ima mnogo, a neke od prednosti su također očuvanje života, sprječavanje krađa ili jednostavno olakšavanje svakodnevnih radnji.

[5] RFID je naziv za tehnologije koje koriste radio valove kako bi automatski identificirali objekte. Radio frekvencijska komunikacija temelji se na stvaranju elektromagnetskih valova u odašiljačima i njihovom otkrivanju na udaljenom prijamniku. Postoji nekoliko metoda identifikacije objekata, no najčešća je pohranjivanje identifikacijskog serijskog broja ili neke druge informacije na mikročip koji zajedno s antenom čini RFID transponder. Transponder komunicira s čitačem putem radio signala, jednosmjerno ili dvosmjerno, a čitač je povezan s računalom ili računalnom mrežom na kojemu se nalazi baza podataka. Jednostavna identifikacijska oznaka pohranjena na transponderu u ovoj bazi povezana je s informacijama o označenom proizvodu.[14]

2.1.2. Mreža

Poslužitelji u oblaku obrađuju podatke koje prikupljaju senzori. Ali, da bi to učinili, potrebne su im platforme. Povezivost je veza između svih IoT uređaja u bilo kojem IoT ekosustavu uključujući senzore, usmjerivače, pristupnike, korisničke aplikacije i platforme. Povezivost omogućuje preuzimanje kontrole nad cijelim IoT sustavom.[15] Posljednjih godina pojavili su se različiti protokoli povezivanja koji koriste tehnologiju radio frekvencija. Neke od najčešće korištenih tehnologija su BLE (eng. Bluetooth Low Energy), LoRa (eng. Long Range Technology), ZigBee, SigFox i NBIoT (eng. Narrow Band IoT). Sve ove tehnologije modulirale su radiofrekvencije kako bi osigurale bežično povezivanje za podatke koji su prikupljeni pomoću IoT senzora. Iako sve ove navedene tehnologije imaju aplikacije temeljene na slučajevima korištenja u IoT -u, ona koja je stekla najveću popularnost je BLE. Većina IoT senzora može slati svoje podatke BLE-u koristeći UART[6] i Modbus komunikacijske protokole. BLE uređaji imaju mogućnost bežičnog prijenosa ovih informacija na druge BLE uređaje i/ili BLE pristupnike. Nakon što primatelji prime podatke, mogu poslati te informacije mehanizmima odlučivanja, koji se uglavnom nalaze u privatnom ili javnom oblaku koristeći ugrađeni GPRS, Wi-Fi, LTE[12], a u zadnje vrijeme i 5G.

Jedna od navedenih tehnologija, ZigBee, specifikacija visokih komunikacijskih protokola koristi male digitalne radio stanice male snage i niske brzine prijenosa podataka temeljene na standardima IEEE (eng. Institute of Electrical and Electronics Engineers) 802.15.4[16] za WPAN mreže (eng. Wireless personal area network), kao što su bežične slušalice koje se povezuju s mobitelima putem radija kratkog dometa. ZigBee je usmjeren na radio-frekventne (eng. Radio frequency - RF) aplikacije koje zahtijevaju nisku brzinu prijenosa podataka, dugo trajanje baterije i sigurno umrežavanje.[17] Zigbee WPAN-ovi rade na frekvencijama 2,4 Ghz, 900MHz i 868 MHz, a za zaštitu podataka koristi se simetrična AES enkripcija s ključem duljine 128 bita za prijenos podataka.[18] Koristi *mesh* mrežnu topologiju. Zigbee Alliance radi na pojednostavljenju bežične integracije proizvoda kako bi pomogao proizvođačima proizvoda da brže i isplativije uvedu energetski učinkovitu bežičnu kontrolu u svoje proizvode. Postoje tri Zigbee specifikacije, a to su:

- *Zigbee PRO* – cilj mu je pružanje temelja za IoT sa značajkama koje podržavaju jeftine i pouzdane mreže za komunikaciju.
- *Zigbee RF4CE* – dizajniran za jednostavne i dvosmjerne aplikacije za upravljanje od uređaja do uređaja koje ne trebaju potpuno opremljene *mesh* mrežne funkcionalnosti.
- *Zigbee IP* – optimizira standard za potpuno bežične mreže temeljene na Ipv6, nudeći internetske veze za kontrolu uređaja niske potrošnje i niske cijene.[19]

[6] Hardverski komunikacijski protokol koji koristi asinkronu serijsku komunikaciju s podesivom brzinom.

ZigBee karakterizira mala potrošnja energije i velika međusobna kompatibilnost. Također karakterizira ga i *open source code* te je otvoren za sve proizvođače za slobodnu implementaciju funkcija što ponekad rezultira i sa nekompatibilnosti uređaja iz razloga što implementacijom funkcija i specifikacija proizvođača, stariji uređaji više nisu kompatibilni ali uvođenjem Zigbee 3.0, standard je postao ujednačeniji. S obzirom da u *mesh* tehnologiji čvorovi služe kao repetitori karakterizira ga i dugi domet.[18]

Glavni cilj ovog protokola je smanjenje ljudskog napora daljinskim upravljanjem uređajima u kućnoj automatizaciji što je jedna od njegovih prednosti Tako je njegova široka primjena poznata u kontroli kućne rasvjete iz razloga što je Zigbee mreža učinkovitija jer ovisi o niskim zahtjevima za energijom.[17] Koriste ga svjetski pametni uređaji poput Amazon Echo, Philips Hue, IKEA Tradfri te Homey.[20] Također osim rasvjetom, pomoću njega se može daljinski upravljati i ostalim kućanskim aparatima na način da se podaci šalju putem radija na prijemnik. Standardna specifikacija za do 254 čvora uključuje jedan glavni uređaj kojim se upravlja s jednog daljinskog upravljača. Praktični primjeri upotrebe ZigBee-a uključuju zadatke kućne automatizacije kao što su paljenje svjetla, postavljanje kućnog sigurnosnog sustava ili pokretanje videorekordera. Uz ZigBee, svi ovi zadaci mogu se postići s bilo kojeg mjesta u domu pritiskom na gumb. Sigurnost je temeljena na prethodno navedenom IEEE 802.15.4 standardu koji specificira sigurnosne usluge kao što je kontrola pristupa za uređaje za održavanje popisa pouzdanih uređaja unutar mreže i enkripcije podataka.[17]

2.1.3. Obrada podataka

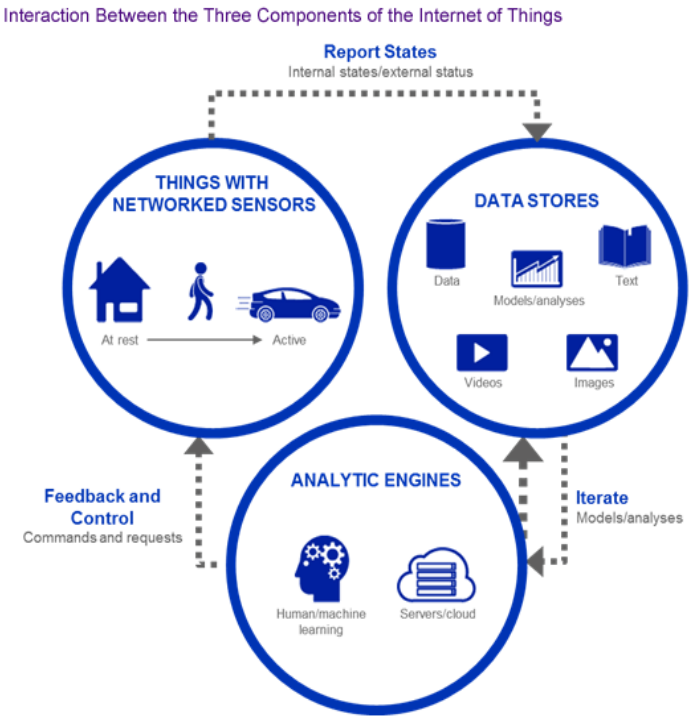
IoT stvara velike količine podataka prikupljene s uređaja i aplikacija s kojima se mora upravljati na učinkovit način. IoT oblak nudi različite alate za prikupljanje i obradu ogromnih količina podataka u realnom vremenu. U principu, IoT oblak sofisticirana je mreža poslužitelja visokih performansi optimiziranih za izvođenje velike brzine obrade podataka milijardi uređaja, upravljanje prometom i isporuku točne analitike. Sustavi za upravljanje distribuiranim bazama podataka jedna su od najvažnijih komponenti IoT oblaka.[21]

Primjerice, uzme li se da je mreža temperaturnih senzora u kući povezana mrežnim pristupnikom na Internet putem *Cloud* infrastrukture. Oblak posjeduje detaljne zapise o svakom uređaju (ID, status, zadnji pristup, koji je korisnik zadnji pristupao i dr.), a veza s oblakom implementirana je pomoću web servisa primjerice RESTful[7]. Komunikacija se odvija na sljedeći način:

[7] RESTful API je sučelje za programiranje aplikacije koje je u skladu s ograničenjima REST arhitektonskog stila i omogućuje interakciju s RESTful web uslugama Ponekad se naziva ugovorom između davatelja informacija i korisnika informacija – utvrđivanje sadržaja koji se zahtijeva od potrošača (poziv) i sadržaja koji zahtijeva proizvođač (odgovor). API pomaže da prijenos sustavu onoga što korisnik želi, kako bi mogao razumjeti i ispuniti zahtjev.[22]

1. Krajnji korisnici komuniciraju s oblakom preko mobilne aplikacije.
2. Zahtjev je poslan u oblak s podacima o autentifikaciji i uređaju.
3. Autentifikacija je konfigurirana kako bi se osigurala kibernetička sigurnost.
4. Oblak zatim identificira uređaj pomoću ID-a te šalje zahtjev odgovarajućoj senzorskoj mreži preko pristupnika.
5. Senzor očitava temperature, te vraća informaciju u oblak.
6. Oblak zatim vraća podatke korisniku koji je zatražio informaciju koji istu očitava na svom ekranu.[23]

Nakon što se cijeli podaci prenesu na oblak, nad tim se podacima izvode funkcije kako bi se podaci obrađivali i slali natrag potrebni rezultati. Drugim riječima, mora se izvršiti analiza podataka. Ovaj korak je najvažniji korak u IoT tehnologijama i mora se odvijati brzo kako bi se dobili bolji rezultati.[15] Na slici 4 prikazana je interakcija između tri komponente IoT-a.



Slika 4. Obrada podataka u IoT-u, [24]

Analiza podataka vrlo je važna, jer prema njoj mehanizam odlučivanja radi određene radnje. On dakle na temelju podataka odlučuje hoće li se grijanje isključiti ili uključiti, hoće li se aktivirati alarm tijekom provale u kuću; hoće li se poslati obavijest ovlaštenim djelatnicima prilikom neovlaštenog pristupa sustavu određene osobe; hoće li se otvoriti ili zatvoriti vrata prilikom prilaska garaži; hoće li se aktivirati protupožarni sustav itd.

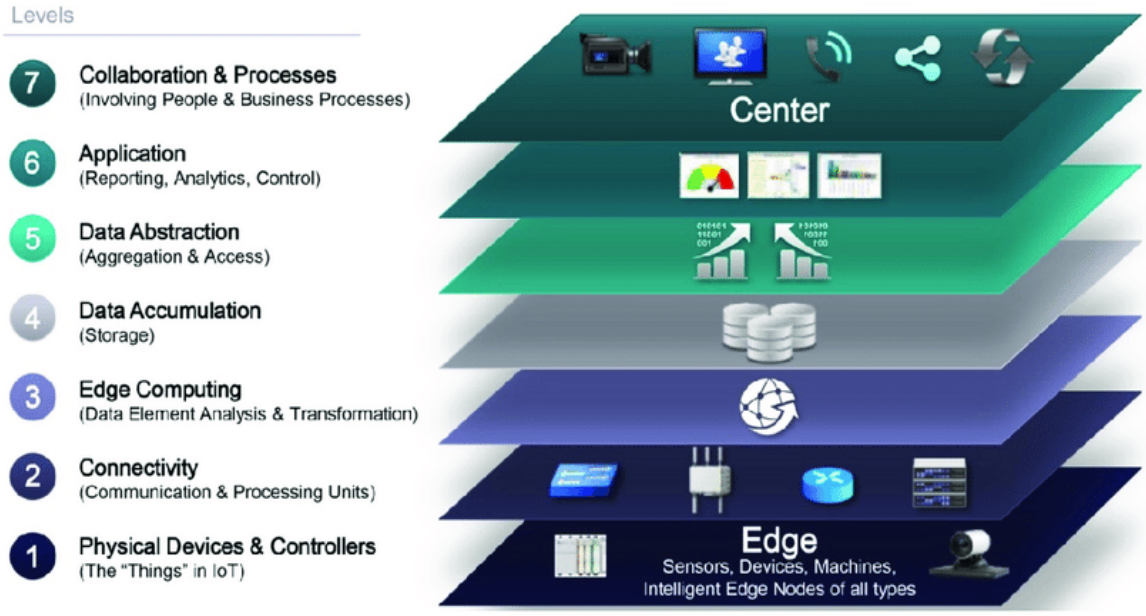
2.1.4. Korisničko sučelje

Korisnička sučelja vidljivi su i opipljivi dio IoT sustava kojem korisnici mogu pristupiti. Ovo je završna faza u izravnom kontaktu s korisnikom i daje rezultat koji korisnici vide na svom ekranu. Svaki IoT uređaj ima različito sučelje jer svaki uređaj ima drugačiji zadatak i namjenu.[15]

2.2. Arhitektura Interneta stvari

Danas na svijetu postoji čitav niz alata i standarda koji pomažu dizajnerima IoT-a pri stvaranju i primjeni IoT komponenti. Jedan od najpoznatijih je ISO/IEC standard opisa arhitekture, a osim njega dostupni su brojni standardi usmjereni na IoT, a neki od njih su opisani u ovom poglavlju.

Također, bitno je napomenuti kako izgleda i klasični IoT referentni model koji se sastoji od sedam slojeva prikazanih na slici 5.[25]

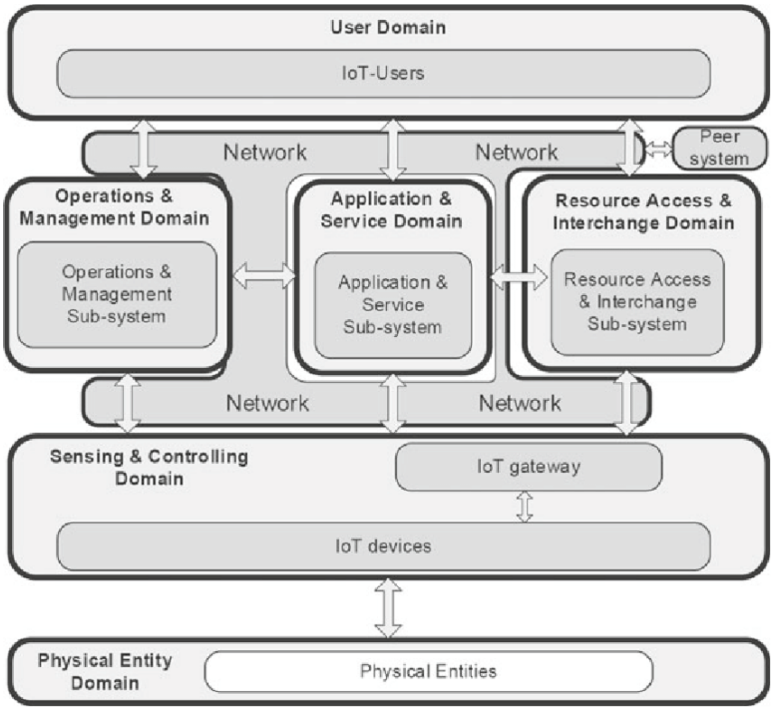


Slika 5. IoT referentni model, [25]

Svaki od prikazanih slojeva ima svoju ulogu, slično kao i u OSI modelu[8], a to su: sloj fizičkih uređaja i kontrolera, sloj povezanosti, rubni sloj, sloj akumulacije podataka, sloj apstrakcije podataka, aplikacijski sloj i sloj suradnje i obrade.[25] No, međutim, postoje različite referentne arhitekture IoT-a, a u nastavku su opisane neke.

2.2.1. Referentna arhitektura Interneta stvari prema ISO/IEC 30141

ISO/IEC 30141[26] međunarodno je standardizirana generička IoT referentna arhitektura (eng. Internet of things reference architecture - IoT RA). Određuje osnovne karakteristike IoT sustava, konceptualni model, referentni model i četiri arhitektonska pogleda. ISO/IEC IoT RA prikaz domene, poznat kao model šest domena, inovativna je struktura koja proširuje konvencionalnu slojevitu referentnu arhitekturu koja se tradicionalno primjenjuje za dizajn IT sustava.[27] Prikaz ISO/IEC 20141 arhitekture je na slici 6.



Slika 6. ISO/IEC IoT RA, [28]

[8] OSI model je konceptualni okvir koji se koristi za opisivanje funkcija mrežnog sustava. OSI model karakterizira računalne funkcije u univerzalni skup pravila i zahtjeva kako bi se podržala interoperabilnost između različitih proizvoda i softvera. U OSI referentnom modelu, komunikacija između računalnog sustava podijeljena je u sedam različitih slojeva: fizički, podatkovni, mreža, transport, sesija, prezentacija i aplikacija.[29]

Svaka domena sadrži skup funkcija koje se mogu odabrati ovisno o konkretnom slučaju primjene:

- *Korisnička domena* – sadrži funkcije korisničkog sučelja.
- *Domena operacija i upravljanja* (eng. Operations & Management Domain - OMD) - olakšava operativno upravljanje usredotočavajući se na prikupljanje funkcija kao što su praćenje, izvješćivanje, upravljanje uređajima i optimizacija performansi sustava u stvarnom vremenu.
- *Domena za pristup resursima i razmjenu* (eng. Resource Access & Interchange Domain - RAID) komunicira s vanjskim entitetima i pruža mehanizme za izlaganje resursa IoT sustava.
- *Domena za detekciju i kontrolu* (eng. Sensing and Controlling Domain - SCD) pruža senzorske i aktivacijske funkcije. Senzorska funkcija čita podatke sa senzora, dok funkcija aktiviranja kontrolira fizičke objekte.
- *Domena aplikacija i servisa* – baza usluga.
- *Domena fizičkih entiteta* (eng. Physical Entity Domain - PED) predstavlja sve fizičke objekte koji su podložni otkrivanju ili kontroli u IoT sustavu.

Standard također opisuje tri vertikalne funkcije između domena, odnosno mrežnu povezanost, dinamičku kompoziciju i pouzdanost. Dimenzija pouzdanosti usredotočuje se na osiguravanje visoke sigurnosti, privatnosti, pouzdanosti i otpornosti na razne napade, greške sustava i ljudske pogreške.

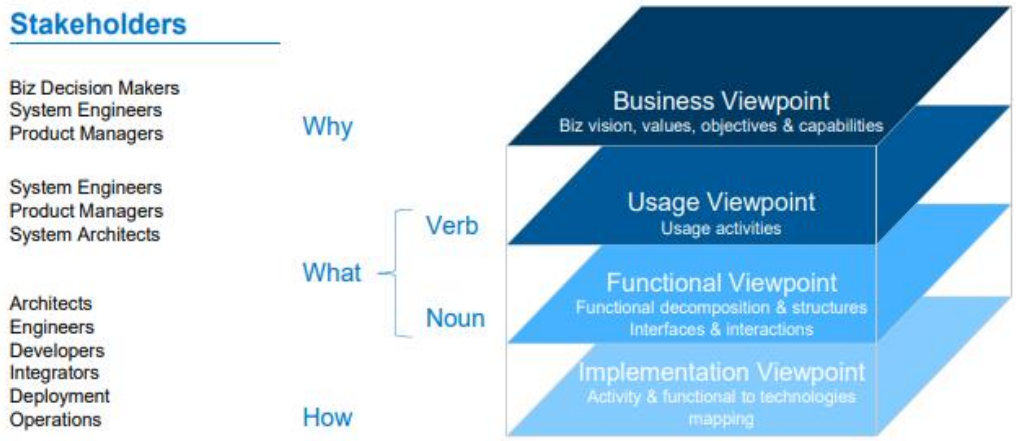
ISO/IEC 30141 IoT RA ne raspravlja o tehničkim detaljima ili konkretnim rješenjima. Međutim, to je prva harmonizirajuća referentna arhitektura koja pruža zajednički temelj i okvir za mnoge primjenjive standarde koje je izradio ISO/IEC JTC1/SC 41[30], čiji dobro zaokruženi opseg pokriva interoperabilnost i sigurnost.[27]

2.2.2. Referentna arhitektura Interneta stvari prema IIC

The Industrial Internet Consortium (IIC) usredotočen je na industrijsku primjenu IoT-a. IIC industrijska Internet referentna arhitektura (IIRA) definira 4 gledišta kao što je prikazano na slici 7, a to su poslovni pogled, pogled uporabe, funkcionalni te implementacijski pogled.

Poslovni pogled i pogled korištenja određuju važnost koja se pridaje poslovnim interesima pri implementaciji industrijskih sustava, te značaj domene i kontekst u kojem se sustav koristi u svom dizajnu. Poseban tehnički naglasak stavljen je na funkcionalna i provedbena gledišta. Funkcionalno gledište dijeli arhitektonski pogled na funkcionalne domene – kontrola, operacije, informacije, primjena i poslovanje. Implementacijski pogled fokusira se na opću arhitekturu, pružanje tehničkog opisa komponenti sustava (sučelja, protokoli, ponašanja, itd.), provedbeno mapiranje gledišta upotrebe, aktivnosti funkcionalnih

komponenti kao i na implementaciju komponenti. Pogledi su vodiči arhitektima za stvaranje vlastitog pogleda na arhitekturu. Ključni dio ovog sustava je i pitanje sigurnosti ali i privatnost, povjerenje, otpornost, interoperabilnost i sastavljanje, povezanost, upravljanje podacima, analitika, inteligentno i automatska integracija.[31]



Slika 7. IIC Internet referentna arhitektura, [31]

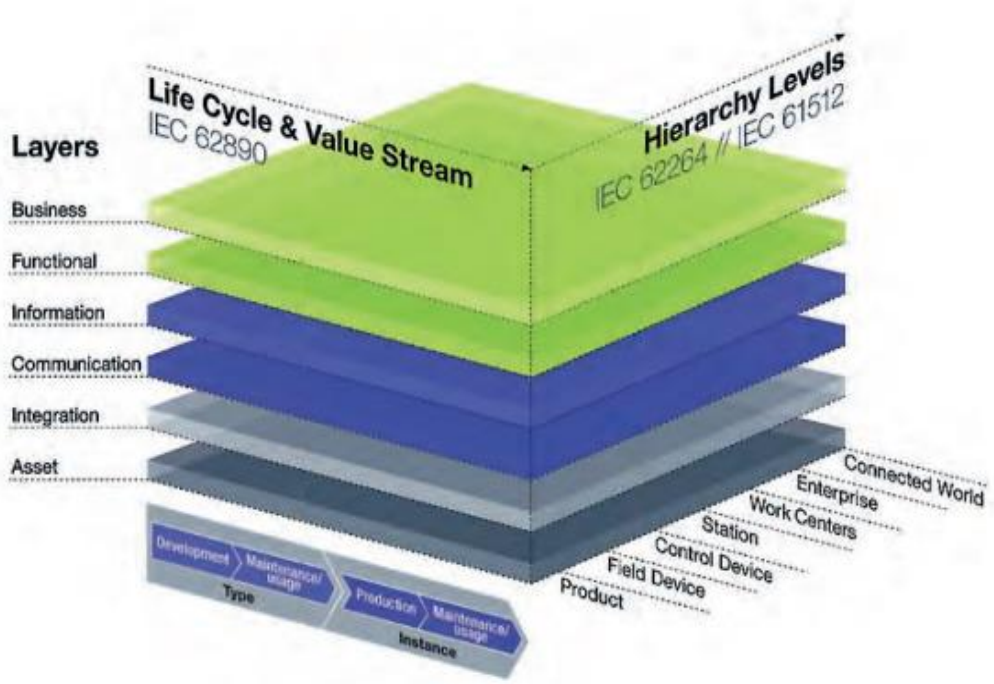
2.2.3. Referentna arhitektura Interneta stvari prema Industriji 4.0

Referentni arhitektonski model Industrije 4.0 (eng. The Reference Architectural Model Industrie 4.0 - RAMI 4.0), trenutno je u aktivnom razvoju i predstavlja zajednički napor velikih kompanija BITKOM-a, ZVEI-a te VDMA. Kao što se vidi na slici 8, jezgra RAMI 4.0 je trodimenzionalni slojeviti model koji se koristi za klasifikaciju tehnologije Industrije 4.0.

RAMI 4.0. ima horizontalne i vertikalne dimenzije. Horizontalne dimenzije su životni ciklus i tok vrijednosti, dok su vertikalne poslovanje, funkcionalnost, informacija, komunikacija, integracija te imovina. Također, uključuje dijelove međunarodnih standarda IEC 62264[9][32] i IEC 62890[10][33] za opisivanje različitih aspekata sustava sljedeće generacije.

[9] IEC 62264 definira tehnološki neovisan model za skup apstraktnih usluga koji se nalazi iznad sloja aplikacije OSI modela, a koji se koristi za razmjenu transakcijskih poruka na temelju transakcijskih modela. Model, koji se naziva Messaging Service Model (MSM), namijenjen je interoperabilnosti između aplikacija domene proizvodnih operacija i aplikacija u drugim domenama.[34]

[10] IEC 62890 uspostavlja osnovna načela za upravljanje životnim ciklusom sustava i komponenti koje se koriste za mjerenje, kontrolu i automatizaciju industrijskih procesa. Ova načela su primjenjiva na različite industrijske sektore.[36]

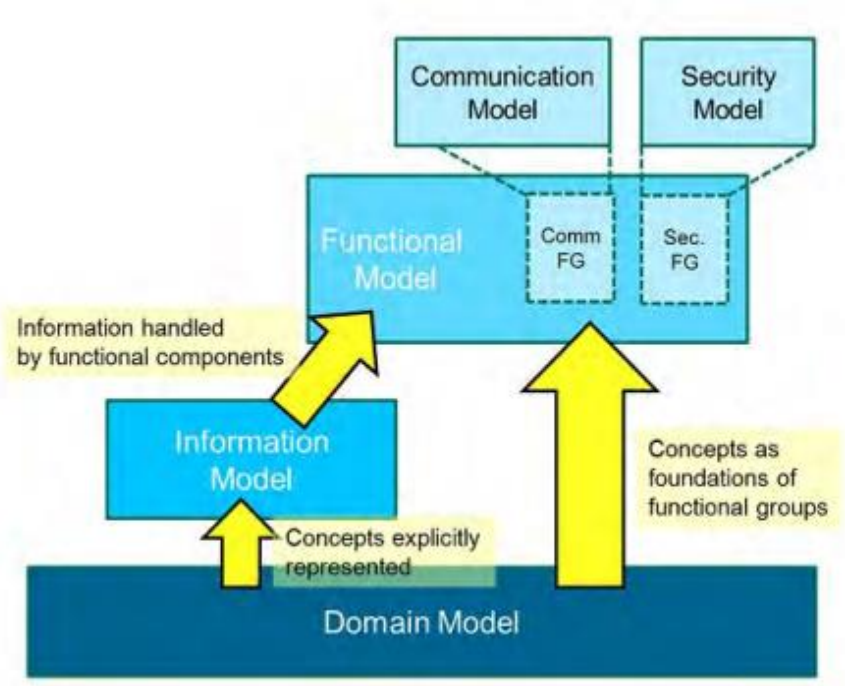


Slika 8. Referentna arhitektura industrije 4.0, [31]

Model definira “razine hijerarhije” prema standardu IEC 62264 s proširenjem za potrebe industrije 4.0 te uključivanje povezanosti s IoT-om i Internet uslugama. Model također pokriva cijeli životni ciklus proizvoda uključujući dizajn, proizvodnju, isporuku, korištenje, održavanje itd., a temelji se na IEC 62890 uz dodatak razlikovanja faza dizajna i prototipa u odnosu na proizvodnju. Osnovni RAMI model proširen je na način da je sigurnost integrirana u svaki sloj i svaku dimenziju modela.[31]

2.2.4. Referentna arhitektura Interneta stvari prema projeku IoT-A

IoT-A projekt razvio je arhitektonski referentni model (eng. Architectural Reference Model - ARM) kao temeljni dokument referentne arhitekture kako bi se olakšao rast i razvoj IoT tehnologije.[35] IoT-A ARM sastoji se od tri komponente, kao što je prikazano na slici 9, a to su domenski, informacijski i funkcionalni model koji se sastoji od komunikacijskog i sigurnosnog modela.

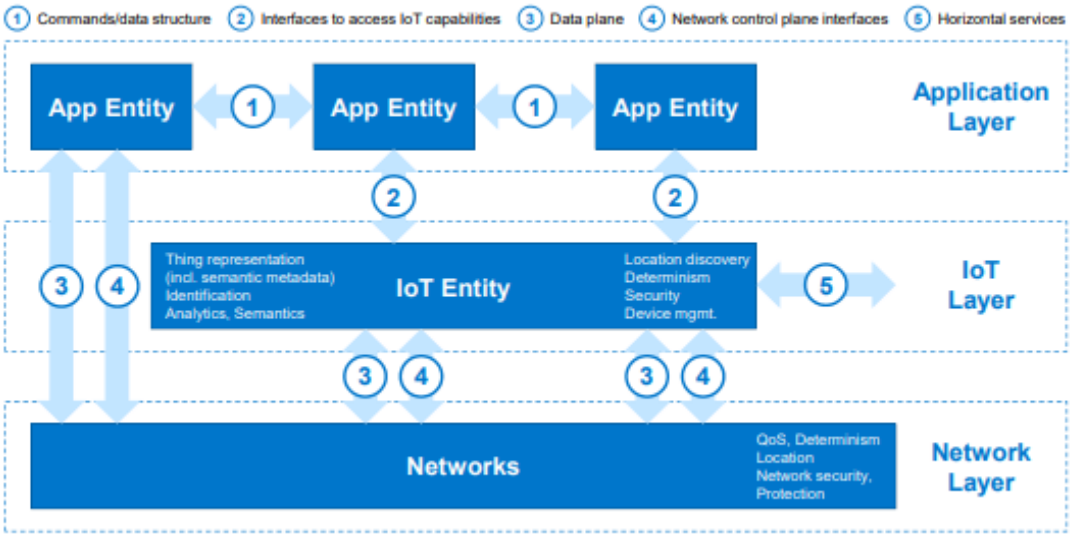


Slika 9. IoT ARM, [31]

Model domene odgovoran je za ocrtavanje temeljnih koncepata u IoT-u kao što su uređaji, IoT usluge i virtualni entiteti. Informacijski model definira generički strukturna svojstva informacija u IoT-u sustav. Funkcionalni model identificira skupine funkcionalnosti temeljene na odnosima definiranih u modelu domene, komunikacijski model rješava složenost komunikacija u IoT okruženjima, a model povjerenja, sigurnosti i privatnosti posebno je identificiran svojom važnosti za IoT scenarije korištenja.[31]

2.2.5. Referentna arhitektura Interneta stvari prema prema AIOTI

AIOTI (eng. The Alliance for Internet of Things Innovation) model, izveden je iz modela IOT-A prikazanog na slici 9. U ovom modelu korisnik stupa u interakciju s fizičkim entitetom, a interakcija je posredovana IoT uslugom s virtualnim entitetom. IoT usluga tad stupa u interakciju sa stvari putem IoT uređaja koji otkriva sposobnosti stvarnog fizičkog subjekta. AIOTI model, prikazan na slici 10, opisuje funkcije i sučelja (interakcije) unutar domene, ne isključujući interakcije izvan domena, a sastoji se od 3 dijela: sloj aplikacije, sloj IoT-a te sloj aplikacije.[31]



Slika 10. AIOTI referentna arhitektura, [31]

2.3. Područja primjene

Mogućnosti primjene IoT-a u svakodnevnom životu su raznolike, a prožimaju gotovo sva područja ljudskog djelovanja pojedinaca, poduzeća i društva u cjelini.[37] Kada se govori o mogućnostima primjene, moguće je govoriti o potrošačkoj primjeni IoT-a (eng. The Consumer Internet of Things – CIoT) te industrijskoj primjeni IoT-a (eng. The Industrial Internet of Things - IIoT).

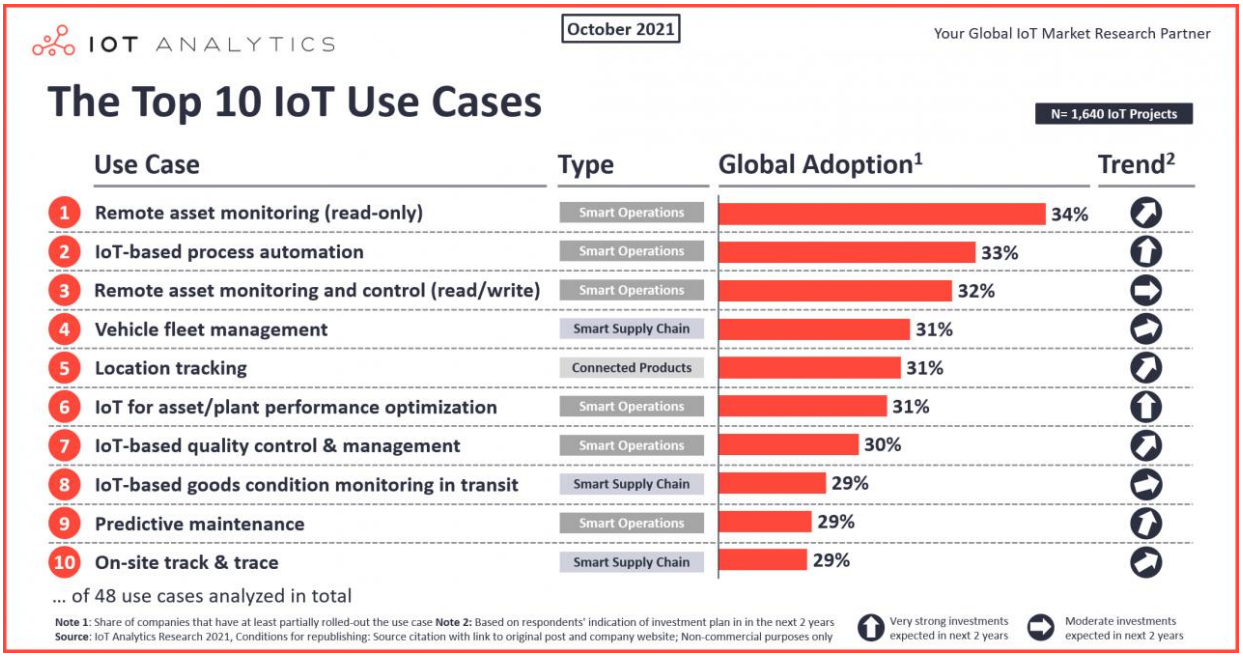
Potrošačka primjena je ona primjena dobro poznata svakom pojedincu, jer se o njoj najviše i govori, a uključuje uređaje, aplikacije te slučajeve korištenja za praćenje osobne imovine, odnosno uključuje elemente nosivih uređaja te koncept pametne kuće (eng. Smart home). Ova primjena odnosi se prvenstveno na praćenje vlastite imovine, kućanskih aparata, kontroliranje grijanja u domu, praćenje kućnog ljubimca, kontroliranje vrata i kamera te uključuje nosive elemente poput pametnih mobitela, pametnih satova i uređaja koje čovjek može imati na sebi. Aplikacije postaju sve bolje i pametnije, a također postaju sve neovisnije od drugih uređaja kao što su pametni telefoni. To je svakako slučaj s pametnim nosivim uređajima. Obično su u potrošačkom IoT-u količine podataka i potrebe za podatkovnom komunikacijom male i ograničene. Zato postoje mnoge tehnologije od kojih su neke posebno dizajnirane za potrošačke aplikacije, u rasponu od standarda povezivanja pametnog doma do posebnih operativnih sustava za nosive uređaje.[38]

Industrijski IoT opisuje tipične slučajeve industrijske uporabe u različitim sektorima. Industrija uključuje zrakoplovnu, brodsku i automobilsku industriju, područje transporta i logistike, telekomunikacije, zdravstvo, energetske sustave, urede, poljoprivredu, Vladine

organizacije, ekološke organizacije, područje meteorologije i brojna druga kojih je svakim danom sve više.

Dva su primjera uporabe IIoT-a, a to su prediktivno održavanje i upravljanje imovinom. Kao što je navedeno prethodno, pojam industrije obično se stavlja u kontekst „teške“ industrije poput proizvodnje, no također koristi se i za slučajeve upotrebe na primjer, u pametnim gradovima (eng. Smart city) te upravljanju zgradama. Ako ga promatramo kao neku vrstu 'Poslovnog Interneta stvari', jasno je da postoje neka preklapanja s potrošačkim Internetom stvari. Na primjer: ako u kući pojedinac posjeduje pametni termostat i pametni mjerač potrošnje energije, oni su s jedne strane potrošačke aplikacije jer su za osobnu upotrebu. No, iz perspektive tvrtke koja ga koristi za slanje računa i pomoć pri optimizaciji potrošnje energije, to je poslovna stvar. Stoga ova vrsta podjele i nije najzahvalnija al ipak većina IIoT aplikacija ipak se odnosi na digitalnu transformaciju proizvodnje ili na uspon pametne industrije.[38]

Prema izvješću IoT Analyticsa[39] u 2021. godini prosječna velika proizvodna, zdravstvena, automobilska, maloprodajna ili energetska tvrtka uvela je osam različitih slučajeva korištenja IoT-a, prikazanih na slici 11.



Slika 11. Deset najčešćih područja primjene IoT-a za 2021. godinu, [40]

Izvješće pokazuje gdje su tvrtke ulagale i planiraju ulagati, koje industrije i regije prednjače i koji slučajevi korištenja obećavaju najveći povrat ulaganja. Naftne i plinske tvrtke te energetske tvrtke su ispred ostalih. Izveli su u prosjeku 15 slučajeva korištenja. Prosječna intervjuirana tvrtka imala je 9,6 milijardi dolara prihoda i trenutno troši samo 33 milijuna dolara na slučajeve korištenja IoT-a (0,34% prihoda). Činjenica da je slučaj najveće upotrebe usvojilo samo 34% ispitanika što pokazuje kolike su mogućnost IoT-a. Šest od 10 najčešćih slučajeva korištenja IoT-a ima za cilj učiniti operacije pametnim, čime se poboljšavaju proizvodni procesi tvrtki za proizvodnju, poboljšavaju operacije održavanja ili unapređuju bilo koje druge operacije (npr. proizvodnja energije u slučaju energetske tvrtke, vođenje poslova zdravstvene skrbi u slučaju bolnice, vođenje poslova trgovine u slučaju maloprodajnog poduzeća).[40]

Sukladno slici 11., deset najčešćih područja primjene su:

1. Daljinsko praćenje imovine, samo čitanje

Ovaj najjednostavniji slučaj korištenja, ujedno je i najzastupljeniji, a radi svoje jednostavnosti najjeftiniji za postavljanje. Odnosi se na sredstva povezana na daljinu samo za čitanje (eng. read only), što znači da se podaci o imovini mogu vizualizirati, ali se istoj ne mogu poslati nikakve naredbe.[40] Porast ovog slučaja korištenja porastao je za vrijeme krize uzrokovane COVID-19 virusom, a jedan od primjera implementacije je slučaj tvrtke Hinduistan Coca Cola Beverages Pvt.Ltd[11] koja se nalazi u Indiji, poradi praćenja imovine linija plastične ambalaže te limenki. Na ovaj način kontinuirano se prate kritični parametri poput brzine protoka sirupa, tlak za ispiranje limenke ili temperature vode, te primjenom ovog koncepta zamijenila se fizička prisutnost ljudi. Na temelju unaprijed definiranih uvjeta, koriste se i alarmi za praćenje stanja.[41]

2. Automatizacija procesa temeljena na IoT-u

Drugi po redu slučaj primjene od 33% zastupljenosti je automatizacija procesa temeljena na IoT-u, koja se odnosi na izvođenje procesa koji su nekada zahtijevali ručno upravljanje ili su pokretani zastarjelom industrijskom automatizacijom. Na ovaj način sam proces proizvodnje postaje fleksibilniji i jednostavniji, a proizvodnja ide u korak sa zahtjevima kupaca koji se sve brže mijenjaju. Primjer primjene ovog slučaja čest je u poljoprivredi, posebno u slučaju navodnjavanja.[40] Jedan od takvih je i slučaj australskog farmera koji je korištenjem IoT rješenja uštedio 149.800 galona po hektaru odnosno 20%.[42]

[11] Hindustan Coca Cola Beverages Pvt Ltd u Indiji je tvrtka koja se bavi punjenjem ambalaže. Jedan od njenih najpopularnijih brendova je Coca Cola. Hindustan Coca Cola Beverages Pvt Ltd bavi se proizvodnjom, distribucijom prodaje i opskrbom svih bezalkoholnih proizvoda.[41]

3. Daljinsko praćenje i kontrola imovine, čitanje/pisanje

Daljinsko praćenje i kontrola sredstava s mogućnošću čitanja/pisanja (eng. read/write) proširenje je daljinskog nadzora imovine samo za čitanje. Osim provjere podataka imovine, ovim slučajem se može komunicirati i povratno, odnosno imovina se može kontrolirati na daljinu. Primjena ovog slučaja također je ubrzana za vrijeme pandemije koronavirusa COVID-19 jer se većina poslova odvijala udaljenim pristupom od kuće, te su inženjeri i servisni timovi morali pronaći rješenje kako bi došli do uređaja neophodnih za rad poduzeća. Zbog dodatne složenosti i sigurnosnog rizika kontrole imovine, osim jednostavnog nadzora, ovaj slučaj korištenja dolazi sa znatno većim troškovima instalacije i održavanja. Međutim, dokazano je da se takva rješenja isplate u relativno kratkom vremenu, nekih 51% tvrtki prijavilo je amortizaciju u manje od 24 mjeseca.[40] Primjer implementacije ovog slučaja je tvrtka Schlumberger koja se bavi pružanjem usluga naftnim poljima. S ciljem optimizacije proizvodnje i povećanja sigurnosti tvrtka je usvojila rješenje za nadzor i kontrolu tvrtki Advantech i ReStream koje su razvile zajednički sustav temeljen na LTE povezivanju. Projekt je pomogao u postizanju osiguranja toka, osiguravanju integriteta imovine i optimizaciji proizvodnje i također je pomogao u povećanju sigurnosti rada. Naftne tvrtke pate od dinamičnog kemijskog okruženja koje, ako se ne kontrolira, može dovesti do preranog trošenja, gubitka produktivnosti i oslobađanja smrtonosnih otrovnih plinova.[36]

4. Upravljanje voznim parkom

Još jedan od slučajeva korištenja IoT-a za 2021. godinu je upravljanje voznim parkom (eng. Track and trace). Danas se većina rješenja za upravljanje voznim parkom oslanja na širokopojasnu povezanost, kao što je mobilna (2G, 3G, 4G), a tvrtke poput Hiber i Starlinka planiraju dodatno lansiranje satelita u svemir za još veće povezivanje s malim kašnjenjem i velikom propusnošću. Primjer implementacije ovog slučaja je Lineas[12], najveći privatni željeznički prijevoznik tereta u Europi koji je implementirao Bosch rješenje za upravljanje vozilima te na taj način povećao kapacitet svoje flote za više od 40% znajući gdje se točno koji vagon nalazi. Također moguće je pratiti vozila, rute, čvorišta te vrijeme mirovanja.[44]

5. Praćenje lokacije

Praćenje lokacije važno je za razvoj uspješnog IoT poslovnog modela. Praćenje lokacije sredstva može biti korisno i za dobavljača proizvoda (npr. razumijevanjem obrazaca upotrebe) i za korisnika (npr. pronalaženjem izgubljene stvari ili ublažavanjem krađe).[40] Jedan od primjera implementacije ovog koncepta postoji i na domaćem tržištu, a dolazi iz radionice hrvatskog poduzetnika Mate Rimca. Riječ je o pametnom električnom

[12] Lineas, sa sjedištem u Bruxellesu, Belgija šalje svoje vlakove i vagone s robom kupaca iz različitih industrija diljem Europe. U 2017. željeznički prijevoznik tereta opremio je 1100 vagona AMRA kutijama iz Boscha.[37]

biciklu tvrtke Greyp Bikes, G6 predstavljenog 2019. godine, koji je opremljen senzorima i naprednom tehnologijom povezivanja. Nastao je kao plod suradnje Greypa i Hrvatskog Telekoma koji je razvio eSIM tehnologiju temeljenu na IoT-u koja omogućava da bicikl prati preko 50 telemetrijskih podataka u vožnji. Osim što sudjeluje u vozačkim odlukama, prati nagib bicikla, snagu biciklista te otkucaje srca, može pratiti rutu i pozvati u pomoć ako detektira da je biciklist u opasnosti. S obzirom na to da je bicikli konstantno povezan na Internet, korisnik u realnom vremenu može poslati naredbu za gašenje, ako posumnja na krađu bicikla, fotografirati sliku preko kamera i objaviti na društvenim mrežama i dr.[45]

6. IoT za optimizaciju performansi imovine/postrojenja

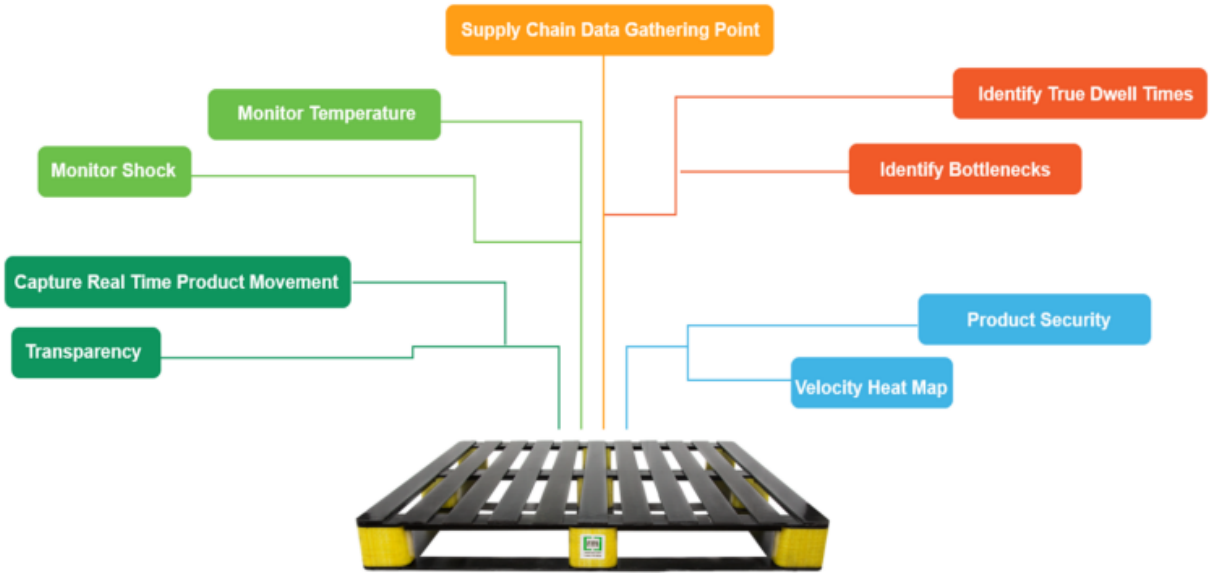
Upravljanje performansama imovine (eng. Asset performance management - APM) pojam je u proizvodnji koji opisuje metode prikupljanja i integracije podataka, njihovo vizualiziranje i analizu kako bi se poboljšala pouzdanost i dostupnost fizičke imovine. IoT za optimizaciju performansi postrojenja moderna je verzija APM-a koja integrira najsuvremenije alate za hvatanje i integraciju podataka (npr. IoT pristupnici) i softverske alate (npr. IoT platforme) za analizu kako se sredstva mogu pokretati i održavati na optimalnim razinama (npr. optimizirane postavke brzine sredstava, optimizirani materijal ulazne postavke ili optimizirani intervali održavanja).[40]

7. Kontrola i upravljanje kvalitetom temeljeno na IoT-u

Ovaj slučaj uključuje korištenje računalnog vida ili drugih podataka IoT senzora za otkrivanje problema s kvalitetom u stvarnom vremenu tijekom operacija. Od 30% tvrtki koje su implementirale ovaj slučaj korištenja IoT-a, dvije trećine izvijestilo je o amortizaciji u manje od 24 mjeseca. Tako je vodeći svjetski proizvođač automobila BMW, uz pomoć Cognizanta potpuno automatizirao testiranje elektroničke funkcionalnosti svojih automobila tijekom proizvodnog procesa.[46]

8. Praćenje stanja robe u transportu temeljeno na IoT-u

Ovaj slučaj najviše se koristi u prehrambenim i farmaceutskim industrijama. Podaci prikupljeni od temperaturnih senzora jedna su od najvažnijih vrijednosti u ovom slučaju jer određena temperaturna prekoračenja mogu bitno utjecati na kvalitetu proizvoda, a ovim konceptom omogućeno je praćenje stanja, a time se omogućuje i pravovremeno reagiranje na odstupanja. Primjer ovog slučaja primjene je korištenje pametnih paleta koje su opremljene nizom senzora koji prikupljaju brojne informacije prikazane na slici 12 za nadzor i upravljanje u realnom vremenu.



Slika 12. Pametna paleta, [47]

9. Prediktivno održavanje

Za predviđanje preostalog životnog vijeka imovine te da bi se osiguralo da se popravi prije nego što propadne, 29% tvrtki uložilo je u rješenja temeljena na umjetnoj inteligenciji i održavanju. Ovo područje primjene je trenutno "u modi", a u narednom periodu 40% ispitanih poduzeća planira investirati u ovaj koncept. Ovaj koncept je tako iskoristila kompanija Colgate-Palmolive za optimizaciju proizvodnog kapaciteta i sprječavanje zastoja ugrađujući bežične senzore u 2000 strojeva za prikupljanje podataka o strojevima. Rješenje za prediktivno održavanje detektiralo je povišene temperature i upozorilo osoblje, čime je spriječilo gotovo 200 sati zastoja i spriječilo propadanje 2,8 milijuna tuba paste za zube.[48]

10. Praćenje na licu mjesta

Dostupnost jeftinih senzora i uređaja za praćenje omogućilo je jednostavno i relativno jeftino praćenje robe i alata na gradilištima, lukama, pa čak i unutar zgrada (npr. tvornice). Od intervjuiranih stručnjaka 29% ih je implementiralo takvo rješenje. Srednja potrošnja za potpuno funkcionalno rješenje za praćenje i upravljanje na licu mjesta samo je 25 000 američkih dolara što je jedna od najnižih u skupu podataka. Međutim, troškovi se mogu povećati kako se sve više sredstava povezuje.[40]

3. Narušavanje privatnosti i sigurnosti

Svakim danom sve je veći broj uređaja spojenih na Internet. Nova tehnologija koja uključuje IoT nesumnjivo je postala neizostavan dio svakodnevnog života ljudi, tako i ne čudi da je upravo IoT postao najrašireniji tehnologija na svijetu.[49] Svaki IoT uređaj može prenijeti velike količine podataka, a neke od procjena za 2020. bile su da će „digitalni svemir" dosegnuti 44 zetabajta[13], a 10% od te količine da će dolaziti od IoT uređaja.[50] Rastom broja IoT uređaja, javlja se sve veći broj prijetnji, pa tako sigurnost postaje glavni fokus za proizvođače, poduzeća, korisnike i regulatorna tijela.[51] Tomu svjedoče i podaci sa svjetskog kongresa mobilnih uređaja (eng. Mobile World Congress - MWC) održanog u Barceloni 2022. godine na kojem je jedna od glavnih tema bila upravo sigurnost u IoT okruženju.[52]

Upravo je pitanje privatnosti i sigurnosti podataka u IoT okruženju jedan od najvećih izazova IoT-a današnjeg doba. Ova dva pojma, iako različita, uglavnom idu jedan uz drugog kao i kroz ovaj rad. Privatnost se odnosi na sva prava koja osoba ima na kontrolu svojih podataka i načina na koji se oni koriste, dok se sigurnost odnosi na to kako su ti podaci zaštićeni.[53]

Neki IoT uređaji mogu prikupljati i prenositi osobne podatke korisnika, što izaziva zabrinutost ali i postavlja pitanje koliko su ti uređaji zaštićeni, odnosno koliko su podaci u tom sustavu sigurni. Iako informacije koje prenose IoT uređaji možda neće uzrokovati probleme s privatnošću ali analizom, sastavljanjem i obuhvaćanjem svih podataka mogu dovesti do otkrivanja identiteta osobe kao i do otkrivanja osjetljivih informacija.[50] Studija provedena godine 2019. na ispitanicima iz Australije, Kanade, Japana, Francuske, SAD-a i Velike Britanije pokazuje kako je 75% ljudi nepovjerljivo prema dijeljenju podataka IoT-a, a čak trećinu pitanje sigurnosti odvraća od kupnje pametnog uređaja.[54]

IoT ima brojne prednosti, no međutim svaka medalja ima dvije strane, tako i IoT ima svoje nedostatke, a ti nedostaci su uglavnom najviše usmjereni na nedovoljnu privatnost i sigurnost. Kod privatnosti i sigurnosti kad je u pitanju pojedinac misli se na njegove osobne podatke, na njegov privatni život, zdravlje, obitelj i sve one detalje koje ne želi iznositi pred drugima. Tako primjerice nitko ne želi da treća strana ima uvid nad njegovim kamerama u domu koje koristi za nadzor djece i ulaza. Također nitko ne želi izgubiti vrijednu imovinu pa ne bi bilo dobro da se ulazna vrata doma ili vrata automobila otvaraju ikome osim njegovom vlasniku. Kad su kompanije u pitanju, niti jedna ne želi da konkurent dođe do njihovih tajnih podataka i otkrije njihovu slabost ali isto tako bi primjerice pametni zvučnik koji se nalazi u uredu kompanije mogao slati audio *stream* konkurentima s druge strane kao i skener koji bi mogao slati kopije važnih skeniranih dokumenata. Curenje ovakvih podataka može nanijeti nepopravljivu štetu kompanijama, reputaciji pojedinca ali može predstavljati i stvarnu prijetnju zdravlju i životu ljudi.[55]

[13] 1 zetabajt jednak je oko trilijun gigabajta.

Neki od sigurnosnih rizika IoT-a odnose se na veliki broj uređaja u mreži, veliki broj njihovih ranjivosti i manjak sigurnosti IoT uređaja.[56]

Jedan od izazova s kojima se IoT suočava je daljinski pristup. Za razliku od drugih tehnologija IoT uređaji imaju veliku površinu napada zbog svoje internetske povezanosti. Hakerima ova pristupačnost omogućuje komunikaciju s uređajima na daljinu i zbog toga su vrlo česte hakerske kampanje poput krađe podataka. Slična stvar je i sa sigurnosti u oblaku, jednom od komponenti IoT sustava. Također, kako kompanije nastavljaju sa svakodnevnom digitalnom transformacijom, odnosno, ugradnjom računalnih tehnologija u proizvode, procese i strategije organizacije[57], tako imaju određene industrije i svoje proizvode. Automobilska industrija i zdravstvo sve više proširuju svoj izbor IoT uređaja kako bi postale produktivnije i isplativije. Ova digitalna revolucija rezultira tehnološkom ovisnošću više nego ikad prije, pa se ovakvim oslanjanjem na tehnologiju povećava i mogućnost povrede podataka. Problem kod ove dvije industrije je taj što osim se velikih ulaganja i skupe tehnologije radi o zdravlju i životu korisnika, i takva tehnologija trebala bi biti sto posto pouzdana no međutim, većina ovakvih industrija za sada nije spremna uložiti količinu novca i resursa koji su potrebni za osiguranje IoT uređaja u njihovom opusu. Ovaj nedostatak nepotrebno je izložio brojne organizacije i potrošače povećanim prijetnjama kibernetičke sigurnosti.

Još jedan problem vezan za IoT, a s kojim se susreću digitalizirane industrije su ograničenja resursa mnogih uređaja jer nemaju svi IoT uređaji računalne snage za integraciju sofisticiranih vatrozida i antivirusnog softvera.[58] Takav primjer može se uzeti u autoindustriji gdje jedan tehnološko napredni stroj poput Tesle pokazao ranjivost BLE tehnologije. To je bio treći put da se uspješno iskoristila ranjivost Teslinog vozila iskorištavanjem privjeska za ključ. Obrnutim inženjeringom privjeska za ključeve otkriveno je da BLE sučelje omogućuje daljinsko ažuriranje softvera koji radi na BLE čipu. Korištenjem samoproizvedenog uređaja napravljenog od Raspberry Pi, modificiranog privjeska i upravljačke jedinice motora (eng. Engine control unit - ECU) iz Modela X, ispitivač je uspio uporabom modificiranog ECU na udaljenosti do pet metara, natjerati privjeske za ključeve da se ponašaju kao BLE uređaji koji se mogu povezati. Tako bi kradljivac, kako bi iskoristio ranjivost automobila, trebao se približiti žrtvinom ključu na udaljenosti od oko pet metara kako bi ga probudio, a zatim mu poslao vlastiti softver kako bi dobio potpunu kontrolu. Nakon toga, lopov bi dobio valjane naredbe koje mu omogućuju otključavanje vozila. Nakon što bi dobio pristup ugrađenom dijagnostičkom konektoru koji koriste servisni tehničari, tada bi morao upariti modificirani privjesak za ključeve s vozilom, nakon čega bi mogao pokrenuti vozilo i krenuti. Sam proces trajao bi par minuta.[59] Ovaj primjer je očigledni pokazatelj kako tehnološki razvoj kompanije u jednoj industriji, konkretno u ovom primjeru automobilskoj, ne mora podrazumijevati jednaki razvoj u drugoj vrsti tehnologije, odnosno IoT tehnologiji.

3.1. Sigurnosni propusti po razinama

Brzina kojom raste tržište IoT-a i IIoT-a na neki način šteti sigurnosti povezanih proizvoda. Sigurnost se oduvijek odnosila na standarde, smjernice i protokole koji su isprobani i testirani godinama, a proizvođači opreme povremeno mogu smanjiti to vrijeme i zanemariti određene zahtjeve kako bi ranije krenuli s isporukom proizvoda i dobili svoj dio kolača. Istodobno, sigurnosni standardi možda nisu uvijek u potpunosti usklađeni s tržištem IoT-a koje se brzo razvija. Povrh svega, korisnici su skloni zanemariti osnovna načela sigurnosti IoT-a i ostaviti svoje uređaje na zadanim postavkama i na taj način su izloženi uljezima. Svi ovi čimbenici bitno utječu na sigurnost IoT uređaja koji su danas dostupni na tržištu.[56] U narednim poglavljima objašnjeni su sigurnosni rizici po razinama IoT arhitekture.

3.1.1. Prijetnje u fizičkom sloju

Fizički sloj, još se popularno naziva i osjetilni sloj odnosno sloj percepcije jer ovaj sloj obuhvaća sve uređaje koji prikupljaju sve podražaje odnosno podatke iz okoline, a sastoji se od mreže različitih vrsta senzora.[60] Ovaj sloj je izuzetno bitan jer prikupljeni podaci od senzora šalju se dalje u mrežu.[61][62]

S obzirom na to da su senzori najmanje sigurni uređaji u arhitekturi, prijetnje temeljene na fizičkom sloju su najvažnije jer ipak, senzori mogu biti najlakši ulaz u cjelokupnu IoT arhitekturu.[8] Napadači mogu koristiti senzore za ubacivanje zlonamjernog koda te u svrhu prikupljanja osjetljivih podataka. Ako se senzori nalaze na otvorenim mjestima odnosno na mjestima koja nemaju adekvatnu fizičku zaštitu, napadači mogu izvoditi napade temeljene na elektromagnetskom zračenju, radiovalovima ili ubacivanjem šumova u signale.[63][64]

Dobar primjer prijetnji na razini fizičkog sloja su ranjivosti pronađene u popularnim Wyze Cam uređajima koji napadačima daju širok pristup *feedovima* kamere i SD karticama[65], na čijem otklanjanju se radi već dvije godine.[66] Prema izvješću stručnjaka[65] ranjivosti uključuju:

- Zaobilaženje autentifikacije (CVE-2019-9564[14])
- Greške u izvršavanju daljinskog upravljanja uzrokovanih prekoračenjem međuspremnika temeljenog na stogu (CVE-2019-12266[15])

[14] Ranjivost u logici provjere autentičnosti Wyze Cam Pan v2, Cam v2, Cam v3 omogućuje napadaču da zaobiđe prijavu i kontrolira uređaje. Ovaj problem utječe na: Wyze Cam Pan v2 verzije prije 4.49.1.47. Wyze Cam v2 verzije prije 4.9.8.1002. Wyze Cam v3 verzije prije 4.36.8.32.[68]

[15] Ranjivost *Buffer Overflow* zasnovana na stogu u Wyze Cam Pan v2, Cam v2, Cam v3 omogućuje napadaču da pokrene proizvoljni kod na zahvaćenom uređaju. Ovaj problem utječe na: Wyze Cam Pan v2 verzije prije 4.49.1.47. Wyze Cam v2 verzije prije 4.9.8.1002. Wyze Cam v3 verzije prije 4.36.8.32.[69]

- Neovlašteni pristup sadržaju SD (eng. Secure digital) kartice.[66]

Ranjivost CVE-2019-9564 omogućava zlonamjernim akterima potpunu kontrolu nad uređajem, uključujući mogućnost kontrole njegovog kretanja, onemogućavanja snimanja, uključivanja ili isključivanja kamere. Ista ne omogućava gledanje audio i video sadržaja međutim u kombinaciji s CVE-2019-12266, eksploatacija je "direktna". Ranjivost CVE-2019-12266 omogućuje hakerima da postave koje će poslužitelje koristiti za povezivanje s oblakom, a ranjivost SD kartice omogućuje napadačima pristup sadržaju kartice nakon što je umetnuta u kameru.[67] Sigurnosni istraživači analizirali su nekoliko verzija uređaja, uključujući Wyze Cam verziju 1, Wyze Cam Black verziju 2, kao i Wyze Cam verziju 3. Analiza je zaključena na način da su verzije 2 i 3 s vremenom zakrpane protiv ranjivosti dok je verzija 1 ukinuta i više ne prima sigurnosna ažuriranja. Stoga korisnici koji koriste Wyze Cam verziju 1 više nisu zaštićeni i riskiraju iskorištavanje svojih uređaja.[67] Do rujna 2019., Wyze je objavio ažuriranje za svoje Cam v2 proizvode kojima je popravljena ranjivost CVE-2019-9564, a kasnije i ažuriranje za CVE-2019-12266, a kompanija Bitdefender je u siječnju 2022. objavila ažuriranje *firmwarea* koje rješava problem SD kartice.[67] Iako su ranjivosti zakrpane, prošao je dugi vremenski period u kojem su napadači mogli pronaći nove ranjivosti i iste iskoristiti. Kamere bazirane na internet protokolu (eng. Internet Protocol - IP), uključujući Wyze Cams, ponekad su namijenjene za stvaranje video dokaza koji bi se mogli koristiti u istragama ili pravnim postupcima te bi te ranjivosti mogle poništiti korištenje videa kao dokaza zbog mogućnosti neovlaštenog mijenjanja dokaza. Također većinom ovakvih kamera upravljaju „ne-IT" organizacije koje nemaju obuku ili proračun da bi osigurale da se svi IoT uređaji drže na najsigurnijoj verziji *firmwarea,* a organizacije ih nastavljaju koristiti dok su god funkcionalne.[66]

DDoS napadi (eng. Distributed denial-of-service attack) prvi su korak u bilo kojoj neprijateljskoj kibernetičkoj (eng. cyber) operaciji.[70] Da broj DDoS napada raste, govori i izvješće kompanije Nokia[71], u kojem je analizirano 10.000 DDoS napada kroz dvije godine. Ovakvi napadi postaju kompleksniji radi rasta IoT povezanih uređaja u kombinaciji sa kibernetičkim napadima koji postaju sve sofisticiraniji i inovativniji. Ne samo da su takvi napadi postali sve kompleksniji i veći, nego ih je sve teže otkriti, jer prošlo je vrijeme DDoS napada pokrenutih s kućnih računala s ograničenom propusnošću i slabim amaterskim *shell* skriptama. Današnji DDoS napadi potječu s nekoliko stotina sofisticiranih komercijalnih web stranica za pokretanje koje prodaju niz napada po konkurentnim cijenama (otprilike 50 – 500 američkih dolara u kripto valuti). Pokretači potom iznajmljuju cikluse na *botnetima* sposobnim za napad na sustave od stotinu gigabajta, milijun paketa ili tisuća zahtjeva u sekundi. Veliki broj loše osiguranih IoT uređaja koji svakodnevno ulaze na tržište samo povećavaju broj uređaja koji se mogu iskoristiti u sljedećim napadima.[72] Na slici 13 prikazan je najveći dnevni DDoS promet izmjeren u vremenskom razdoblju od siječnja 2020. do svibnja 2021. godine, koji se u tom periodu udvostručio.[71]

Slika 13. Prikaz prometa DDoS napada u vremenu od 1/2020 - 5/2021. godine, [71]

Prijetnjama na razini fizičkog sloja nerijetko pogoduju i sami korisnici sustava koji, poradi manjka tehnološkog znanja ili nemara, ostavljaju inicijalne (eng. default) ili slabe zaporke na uređajima što predstavlja jednu od najvećih sigurnosnih prijetnji u IoT okruženju ali i samom Internetu. Procjenjuje se da 15% vlasnika IoT uređaja ne uspijeva promijeniti zadanu zaporku pa je gotovo sigurno da sve srednje i velike kompanije imaju barem jednog zaposlenika sa osjetljivim IoT uređajem. Hakeri izrađuju zlonamjerni softver koji koristi unaprijed definiran popis zadanih zaporki kojima je brže i lakše probiti obranu samog sustava (eng. Brute-force attack).[73] Takvih primjera ima svakim danom sve više, a neki od poznatih su napad na američku korporativnu mrežu preko VOIP telefona i pisača 2019. upravo zbog nedovoljno snažne zaporke[74] te iz 2020. godine kada je napadač objavio vjerodajnice za prijavu više od 515.000 poslužitelja i IoT uređaja na poznatom hakerskom forumu, te se isti događaj smatra kao najveće curenje zaporki ikad. U ovom slučaju ponovno su glavnu ulogu odigrali korisnici sa nedovoljno jakim zaporkama i Telnet protokol koji sve više kompanija zabranjuje koristiti upravo radi njegove nesigurnosti.[75]

3.1.2. Prijetnje u mrežnom sloju

Mrežni sloj zadužen je za prijenos podataka preko mreže koje prima od fizičkog sloja. Prijetnje ovog sloja sve više rastu budući da isti prima podatke sa različitih heterogenih uređaja koji povećavaju sigurnosne ugroze.[76] Princip rada IoT mrežnog sloja može se poistovjetiti sa TCP/IP slojem te njihove ugroze i prijetnje su praktički jednake.[77] Postoje različiti napadi na mrežni sloj IoT okruženja. Neke literature čak svrstavaju DDoS napade kao napade na mrežni sloj.[78]

Brzi rast IoT-a i popularnost mobilnih stanica vrlo brzo su povećali potražnju za bežičnom mrežom (eng. Wireless local area network - WLAN) poznatom kao i standard IEEE 802.11[79], odnosno Wi-Fi. S obzirom na to da je Wi-Fi široko rasprostranjen, uzet je kao primjer u ovom poglavlju. U današnje vrijeme postoji čitav niz izvješća i slučajeva povezanih napada na IoT preko Wi-Fi mreže.[80] Jedan od takvih slučajeva je i slučaj iz 2018. godine kada je napadač putem Wi-Fi mreže hakirao kamere jedne obitelji u Teksasu koja je služila za nadzor njihovog djeteta.[81] Jednu od velikih opasnosti predstavljaju i besplatne Wi-Fi mreže koje su danas posvuda oko nas, od ugostiteljskih objekata, hotela, državnih i privatnih ustanova, domova, gradova i dr. Takve mreže mogu biti zaštićene i nezaštićene. Problem kod nezaštićenih mreža je taj da ne postoji prijava ili postupak provjere za ulazak na mrežu i to bilo koja osoba ili napadač može iskoristiti, i za svo vrijeme korištenja mreže ne postoji nikakva garancija za očuvanje privatnosti i sigurnosti. Često i kućne mreže nisu sigurne zbog nedovoljnog tehnološkog znanja korisnika i kompleksnosti sučelja i pri tome kućna mreža ostaje otvorena za prisluškivanje i presretanje podataka. Postoje različite razine enkripcije koje se također mogu odabrati za mrežu usmjerivača (eng. Router) temeljene na WEP (eng. Wired Equivalent Privacy), WPA (eng. Wi-Fi Protected Access), WPA, 2 i WPA 3 sigurnosnim protokolima.[82]

WEP je prvi sigurnosni protokol za Wi-Fi mrežu razvijen 1999. godine. Razvijen je za zaštitu podataka koji kolaju bežičnom mrežom između klijenta i pristupne točke od neželjenih napadača. Ovaj protokol koristio je 64-bitnu enkripciju, a kasnije i 128 i 256-bitnu. Cilj korištenja ovog protokola bio je pružanje povjerljivosti jednake ožičenom prijenosu podataka.[84] Bio je naširoko korišten ali je bio previše ranjiv na hakiranje zaporki i stručnjaci za kibernetičku sigurnost otkrili su niz ranjivosti ovog protokola. S obzirom na njegovu nesigurnost i zastarjelost, ovaj protokol povučen je iz uporabe 2004. godine od kompanije Wi-Fi Alliance[16].[83]

WPA protokol razvijen je od Wi-Fi Alliance organizacije kao odgovor na neuspjeli WEP. Razvijen je 2003. godine i koristio je 256-bitni WPA-PSK (eng. Pre-shared key) ključ. Razvojem ovog protokola razvili su se i dodatni sigurnosni mehanizmi, a to su provjera integriteta poruke i protokol integriteta vremenskog ključa (eng. Temporal Key Integrity Protocol – TKIP) koji je kasnije zamijenio napredni enkripcijski standard (eng. Advanced Encryption Standard - AES). Ovakav mehanizam pokazao se sigurniji od prethodnog WEP-a. Uz navedeno postojala su dva načina WPA, za poduzeća odnosno poslovni način rada te za privatni način rada, od kojih je poslovni način bio puno sigurniji jer je ovom modelu bio potreban poslužitelj za autentifikaciju dok su za osobni način rada korišteni unaprijed definirani zajednički ključevi radi jednostavnije implementacije i upravljanja. Unatoč tome što se WPA pokazao kao sigurniji od WEP-a, kod njega su također otkrivene različite ranjivosti.[83]

[16] Svjetska organizacija Wi-Fi industrije koja postoji s ciljem promicanja bežičnih tehnologija i interoperabilnosti. Također certificira proizvode koji su u skladu s njegovim specifikacijama za Wi-Fi interoperabilnost, sigurnost i protokole specifične za aplikaciju.[85]

WPA2 razvijen je 2006. godine kao napredna verzija WPA koji je nudio nove mehanizme enkripcije i provjere autentičnosti kako bi se osigurala sigurnija mreža. Ti mehanizmi su bili AES i način brojača šifriranja s protokolom za provjeru autentičnosti poruke u lančanom bloku (eng. Counter Cipher Mode with Block Chaining Message Authentication Code Protocol – CCMP) koji su korišteni umjesto prethodnog TKIP-a koji je i dalje korišten u svrhu zamjene za interoperabilnost. Glavni cilj ovih protokola bio je šifriranje strogo povjerljivih informacija, ali i brojna druga poboljšanja primjerice prelazak klijenta s jedne pristupne točke na drugu bez ponovne provjere autentičnosti, a za to se koristi prethodna autentikacija ili glavni ključ u paru.[83] Godine 2017. otkrivena je velika ranjivost WPA2 protokola odnosno napad ponovne instalacije ključa (eng. Key Reinstallation Attack - KRACK), koja omogućuje zlonamjernom agentu da presretne vezu između Wi-Fi pristupne točke i uređaja. Zlonamjerni agent tada može prisiliti ponovnu instalaciju ključa za šifriranje koji se već koristi, manipulirajući i reproducirajući proces kriptografskog rukovanja koji se događa između uređaja i mreže. Nakon što se iskoristi, zlonamjerni agent može pristupiti svim nešifriranim informacijama poslanim putem te mrežne veze. Kada se korisnik pridruži Wi-Fi mreži, bilo na svom prijenosnom računalu, tabletu ili telefonu, pokreće se 4-smjerno rukovanje u kojem se pregovara o novom ključu sesije.[86] Ovom tehnikom moguće je doći do osjetljivih podataka poput brojeva kreditnih kartica, zaporki, e-mail poruka, fotografija i brojnih drugih, a napad djeluje protiv svih modernih zaštićenih Wi-Fi mreža. Ovisno o konfiguraciji mreže, također je moguće ubaciti i manipulirati podacima. Na primjer, napadač bi mogao ubaciti *ransomware* ili drugi zlonamjerni softver na web stranice.[87] Čak i uz ažuriranja WPA2 ostao je ranjiv.[88]

Napadi čovjeka u sredini (eng Man in the middle - MITM) te rječnički napadi (eng. Dictionary attacks) spriječeni su razvojem WPA3 2018. godine.[83] Poboljšanje je tehnologija razvijene za javne mreže (eng. Oportunistic wireless encryprion – OWE) pomoću koje se obavlja automatska enkripcija bez intervencije korisnika. Također koristi novi protokol za razmjenu ključeva koji osigurava simultanu provjeru autentičnosti i jednakog rukovanja što omogućuje šifriranje prometa. Iako na ovom protokolu se već počinju otkrivati određeni problemi s ranjivosti, za 2022. godinu predstavlja najsigurniji protokol.[89] Problem je što velika većina korisnika i kompanija još uvijek koristi starije i ranjive protokole jer WPA3 je relativno mlad, te na taj način postaju potencijale mete hakerskih napada kojima se ugrožava njihova privatnost, sigurnost, integritet i reputacija

Postoje ranjivosti vezane i uz Bluetooth tehnologiju, pa je uz navedeni problem s Tesla automobilima, jedna od metoda kibernetičkih napada usmjerenih na IoT uređaje je *Bluetooth* lažiranje, koje iskorištava nedostatke u povezivanju kako bi zaobišlo ključne metode provjere autentičnosti. Ranjivost iz 2020. godine poznata kao BLESA (eng. BLE spoofing attacks) prvenstveno utječe na proces ponovnog povezivanja za uređaje koji imaju *Bluetooth* funkciju, a pogodila je milijarde uređaja diljem svijeta. Uređaji spojeni na privatnu mrežu ponekad mogu izgubiti svoje uparivanje ili ispasti iz dometa. Nakon što su ponovno na mreži, automatski se ponovno povezuju na mrežu bez potrebe za prolaskom tipičnih procesa provjere autentičnosti za nove uređaje. Ovu ranjivost mogu iskoristiti kibernetički kriminalci, koji šalju lažne podatke na IoT uređaje kako bi ih prisilili na obavljanje neovlaštenih zadataka.[90] Iste

godine pojavila se i BLURtooth ranjivost koja hakerima u bežičnom dometu omogućuje da zaobiđu ključeve za provjeru autentičnosti, što znatno olakšava praćenje aktivnosti uređaja i prometa na uređajima koji koriste implementacije Bluetootha 4.0 do 5.0.[90]

3.1.3. Prijetnje u podatkovnom i aplikacijskom sloju

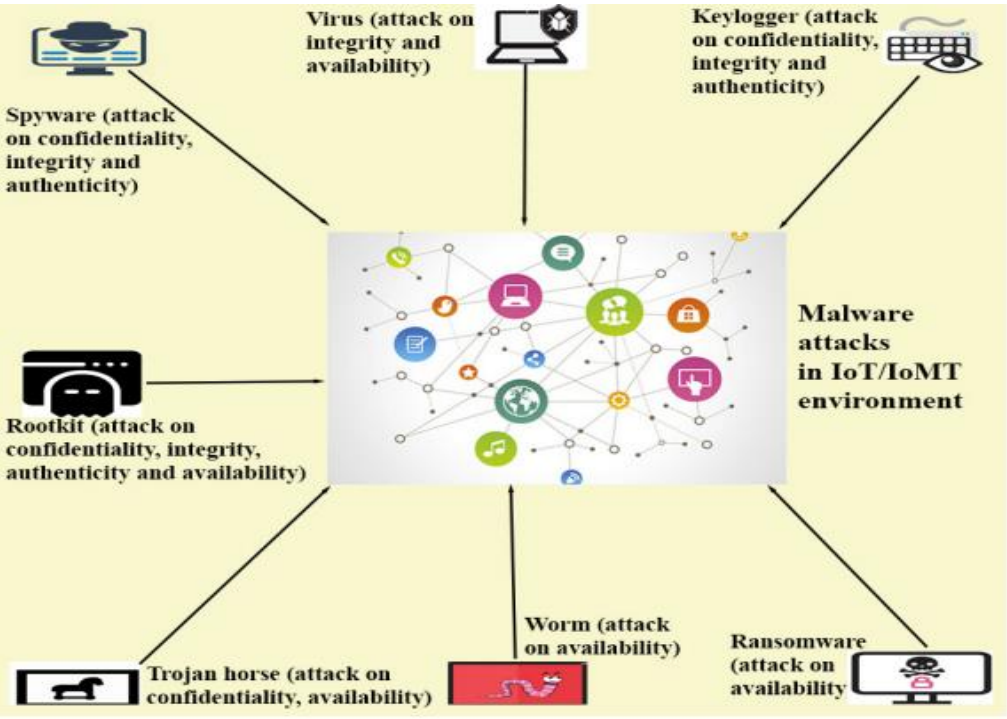
Prijetnje u podatkovnom i aplikacijskom sloju odnose se na one prijetnje koje narušavaju osnovne zahtjeve privatnosti i sigurnosti, a oni su sljedeći:

- **Autentifikacija**: mehanizam za provjeru autentičnosti identiteta ili poruka tijekom komunikacije. U IoT komunikacijskom okruženju uključuje različite entitete poput uređaja, poslužitelja, mobilnih i fiksnih korisnika, usluga u oblaku, aplikacija itd.
- **Integritet**: metoda kojom se osigurava da su podaci stvarni i točni. To znači da sadržaj primljene poruke ne smije sadržavati lažno umetanje, neovlašteno brisanje i promjene.
- **Povjerljivost**: odnosno privatnost, osigurava zaštitu informacija od bilo kakvog pristupa neovlaštenih korisnika.
- **Neporicanje**: jamči valjanost poruke, odnosno originalnost pošiljatelja i autentičnost primatelja poruke. Pruža dokaze o porijeklu poruke i integritetu podataka koje sadrži. Jedan od primjera je digitalni potpis.
- **Autorizacija**: koristi se za određivanje privilegija odnosno prava korisnika ili uređaja za određene datoteke, usluge i aplikacije. Obično mu prethodi mehanizam provjere autentičnosti za provjeru identiteta. Prava pristupa dodjeljuje administrator sustava.
- **Svježina**: osigurava svježinu informacija tako da prethodno razmijenjene poruke ne bi se trebale ponovno prenositi.
- **Dostupnost**: osigurava dostupnost informacija samo ovlaštenim korisnicima.
- **Tajnost prosljeđivanja**: ako pametni uređaj napušta IoT okruženje, ne smije dugo imati pristup budućim porukama.
- **Povratna tajnost**: kada se u IoT okruženje implementira novi uređaj, ne smije imati pristup porukama razmijenjenih u prošlosti.[91]

Zlonamjerni softver (eng. Malware) je kod ili datoteka koja se obično isporučuje preko mreže i kojom se nastoji provesti zlonamjerna aktivnost zavisno o njenoj funkcionalnosti, bilo da se radi o krađi podataka, širenju virusa ili zaraze sustava. Na slici 14. prikazani su različiti zlonamjerni softveri koji pogađaju IoT okruženje u svrhu povrede privatnosti i sigurnosti:[91]

- **Virusi**: Ovi zlonamjerni programi kopiraju se i šire na druge sustave kao dio nekog zaraženog programa, a njihovim pokretanjem dolazi do krađe podataka, oštećenja sustava i izgradnje *botneta*.
- **Trojanski konj**: maskira se kao normalan program za prevaru korisnika. Pomaže hakeru da dobije neovlašteni pristup zaraženom sustavu i pri tom mu omogućuje krađu osjetljivih podataka poput broja kreditne kartice.

- **Špijunski softver**: vrsta zlonamjernog softvera koji vrši špijuniranje korisnika i prikupljanje podataka o njima bez njihovog pristanka. Pod to spadaju podaci o bankovnim transakcijama, brojevi kreditnih kartica, vjerodajnice računa i dr.
- ***Keylogger***: zlonamjerni dio koda koji hakeri koriste za praćenje pritiska tipki na tipkovnici, odnosno sve ono što korisnik napiše uz pomoć tipkovnice (korisnička imena, zaporke). Ova vrsta softvera moćnija je od *brutte force* napada ili napada pomoću rječnika, jer u tom slučaju ni kompleksnost zaporke ne pruža dovoljnu zaštitu. Stoga je preporuka koristiti višefaktorske provjere autentičnosti odnosno kombinacije korisničkog imena, zaporke, biometrije, pametne kartice itd.
- **Crv**: zlonamjerni softver koji se širi mrežom otkrivanjem ranjivosti u operativnom sustavu. Uzrokuje štetu na mreži žrtve kroz potrošnju propusnosti i preopterećenja web poslužitelja. Koristi se za krađu podataka, brisanje datoteka ili stvaranje *botneta*. Samorepliciraju se i šire mrežom putem e-poruka koje sadrže privitke.
- ***Adware***: zlonamjerni softver oglašavanja. Očituje se automatskim prikazom reklama primjerice skočne reklame na web stranicama.
- ***Ransomware***: zlonamjerni softver koji zauzme uređaj i traži od vlasnika uređaja otkupninu. Onemogućuje korisniku pristup uređaju enkripcijom tvrdog diska ili zaključavanjem sustava. Nakon uplate traženog iznosa, vlasnik zlonamjernog programa žrtvi daje ključ za dešifriranje.
- ***Rootkit***: zlonamjerni softver koji se koristi za daljinski pristup uređaju s mogućnošću bez da ga otkrije korisnik ili sigurnosni uređaj. Vrlo ga je teško otkriti i preventivno na njega djelovati.[91]



Slika 14. Vrste zlonamjernih programa u IoT-u, [91]

Neki od poznatih zlonamjernih softvera primjerice su Silex, Mirai, Reaper, Echobot, Emotet, Gamut, Necrus i brojni drugih kojih je svakim danom sve više. Jedan od najvećih napada 2016. godine pod nazivom Mirai, a koristi se i danas, iskoristio je ranjivosti sustava konkretno vezane uz zadana korisnička imena i zaporke, zarazio ih zlonamjernim softverom i izveo najveći DDoS napad ikad pokrenut dovodeći do pada velikog dijela Interneta uključujući Twitter, Guardian, Netflix, Reddit i CNN stranice. Ponajprije su iskorišteni uređaji poput kamera i dvd uređaja.[92] Za razliku od njega, Reaper otkriven 2017. godine cilja devet različitih ranjivosti na uređajima različitih proizvođača kao što su Dlink, Netgear i Linksys te ostavlja teške posljedice na infrastrukturi.[91]

Također, 2019. godine pojavio se novi softver Silex dizajniran da trajno onesposobi hardver koji zarazi. Isti pogađa ponajviše uređaje temeljene na Linux operativnom sustavu. Pretpostavlja se da je odgovoran za određene napade stare čak 14 godina. Radi na principu da iskorištava ranjivosti Linux sustava sa zadanim administratorskim vjerodajnicama, a kada jednom pronađe takav sustav, prepisuje svu memoriju sustava nasumičnim podacima, odbacuje pravila vatrozida, uklanja mrežnu konfiguraciju i zatim ponovno pokreće sustav što ga čini potpuno beskorisnim.[93]

U ožujku 2021. skupina hakera uspjela je dobiti pristup i kontrolu nad tisućama sigurnosnih kamera koje razvija kompanija Verkada sa sjedištem u Silicijskoj dolini koja sigurnost prodaje kao uslugu. Neki od korisnika bile su državne institucije poput škola, bolnica, zatvora i brojnih ureda. Skupina hakera pronašla je vjerodajnice za prijavu javno izložene na Internetu kojima su mogli pristupiti računu administratora. Iskorištavanjem ove vjerodajnice, hakerska grupa uspjela je preuzeti kontrolu nad kamerama kako bi pokrenula buduće moguće napade i pristupila video snimkama pohranjenih u Verkadinom oblaku više od 24.000 klijenata.[94] Kompanija Verkada je za hakiranje saznala preko medija, bez ikakvih saznanja o trajanju provale ili razmjeru štete. Verkada je imala mjere kibernetičke sigurnosti, ali su bile ograničenog opsega. Ni njihove kamere ni njihove centralizirane upravljačke konzole nisu imale rješenje kibernetičke sigurnosti u stvarnom vremenu koje je dizajnirano za otkrivanje i sprječavanje napada. Ovaj incident je primjer iz stvarnog života štete koju mogu prouzročiti hakeri koji imaju pristup osjetljivim podacima.[95]

Jedan od velikih kibernetičkih napada iz 2021. godine, a ujedno i primjer da uređaji koje određena IT kompanija prestane podržavati radi nedovoljne isplativosti predstavljaju zlatnu metu hakerima je napad na uređaje kompanije koja proizvodi uređaje za pohranu podataka Western Digital.[94] Kompanija je potpuno obrisala pohranu uređaja My Book Live i My Book Live Duo iz razloga što su pronađene dvije ranjivosti, od kojih je prva bila daljinsko izvršavanje koda koja je omogućila njegovo kompromitiranje, druga, kritična sigurnosna greška koja je hakerima omogućila daljinsko vraćanje na tvorničke postavke bez lozinke. Kasnije otkrivena ranjivost uključuje lanac napada koji omogućuje neautoriziranom uljezu da izvrši *Rootkit* i instalira trajni *backdoor* na MyBook cloud mrežni uređaj za pohranu. 96]

3.2. Utjecaj Covid-19

Pandemijska kriza uzrokovana koronavirusom Covid-19 ima neviđen utjecaj na društvo i gospodarstvo. Mnoge kompanije za vrijeme krize okrenule su se novim tehnologijama budući da se za vrijeme iste prakticirao u principu rad od kuće, te postoje veliki pokazatelji kako će sve više ljudi i kompanija usmjeravati na digitalizaciju koja je postala općeprihvaćena. Kriza je također utjecala i na IoT, jer se za vrijeme krize porasla je automatizacija određenih poslova koja je prije krize bila u sporom razvoju.[97] Uz automatizaciju, također je postao važan pristup imovini na daljinu, za nadzor i upravljanje određenih procesa. Jednako kao što je poraslo korištenje konferencijskih alata poput Zooma za vrijeme krize, tako je poraslo korištenje daljinske dijagnostike, podrške i komunikacije, a neke tvrtke broje čak dvostruko povećanje korištenja alata za daljinsko upravljanje u samo mjesec dana od početka *lockdowna*.[98] Utjecaj se čak odrazio i na dronove za vrijeme krize, u kojoj su dobili potpuno novu ulogu. Tako su primjerice u Kini korišteni za dostavu medicinskih uzoraka i lijekova kao ispomoć lokalnim bolnicama u više od 300 letova. Također korišteni su za nadzor javnih prostora, emitiranje i širenje informacija te u svrhu dezinfekcije kao kod slučaja proizvođača poljoprivrednih dronova XAG Co. Ltd i Huaweia koji su osposobili 2600 pametnih robota i dronova u dezinfekcijske uređaje.[99]

Među brojnim inicijativama pametnog grada, ispalo je da je mogućnost posjedovanja sveobuhvatne podatkovne platforme i njezinog korištenja tijekom krize jedan od najvažnijih alata koji grad može imati.[97] Tako je primjerice Južna Koreja koristila svoj „Smart City Data Hub“ kako bi omogućila epidemiolozima traženje i dobivanje podataka o slučajevima koronavirusa i kontaktima zaraženih,[100] a brojni drugi gradovi poput Bostona izgradili su nove platforme kako se korona ne bi širila. U Bostonu su razvijene nadzorne ploče koje su pružale ažurirane informacije o statusu koronavirusa u Bostonu ali i cijelom SAD-u.[101] Naravno uz sve benefite koje ovakav sustav pruža, postavlja se ponovno pitanje jesu li prednosti koje ova tehnologija pruža veće od nedostataka koje ima, i koliko su podaci ali i sami korisnici u takvom sustavu zaštićeni.

3.2.1. Porast IoT zdravstvenih aplikacija

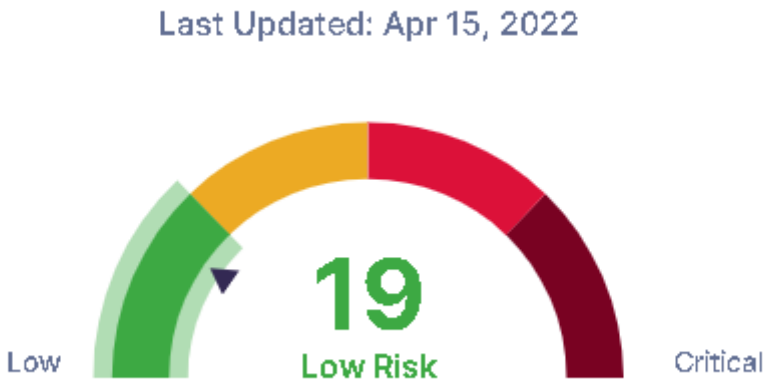
Za svo vrijeme trajanja pandemijske krize, zdravstveni sustavi bili su u središtu pozornosti. Za vrijeme pandemije poraslo je korištenje IoT aplikacija i određenih IoT rješenja koja se odnose na:

- **Telezdravstvene konferencije** – odnosno telezdravstvo, prilikom kojih liječnik putem videokonferencije razgovara s pacijentom nudeći mu pri tom brojne savjete i upute.

- **Digitalna dijagnostika** – još uvijek je u eksperimentalnoj fazi. Dobar primjer su pametni termometri kompanije Kinsa kojima se putem web stranice predviđa buduća

epidemija i razina rizika te koja daje broj slučajeva gripe i koronavirusa. Službene stranice kompanije sadrže podatke o saveznim državama SAD-a, najugroženije i najsigurnije zemlje po pitanju raširenosti virusa gripe i korona virusa prikazano na slici 15, te razina rizika za svaku pojedinu članicu na slici 16.

Slika 15. Prikaz najsigurnijih i najugroženijih virusom saveznih država, [102]



Slika 16. Razina rizika ugroženosti virusom pojedine savezne države, [102]

- **Daljinsko praćenje** - također je poraslo za vrijeme pandemije, posebice starijih osoba. Nude se razna rješenja za praćenje kroničnih bolesti koje povećavaju rizik od umiranja od Covid-19. Primjer takve kompanije je Livongo Health.[103]

- **Korištenje robota i dronova** – kao što je prethodno navedeno, brojni roboti i poljoprivredni dronovi korišteni su u svrhu dezinfekcije, čišćenja ali i dostave lijekova i uzoraka kao pomoć zdravstvenim ustanovama.[97]

3.2.2. Utjecaj na privatnost i sigurnost

Pandemija koronavirusa donijela je najbržu promjenu raznih obrazaca diljem svijeta. Dok su se radnici u zdravstvu, policiji, maloprodaji, dostavi i nizu drugih usluga borili sa znatno povećanom potražnjom i izazovnim radnim uvjetima, većina uredskog osoblja prešla je na rad od kuće, što je predstavljalo veliki izazov za IT stručnjake u pružanju sigurnog daljinskog povezivanja. Prema kampanji Check Point broj napada na sustave se drastično povećao za vrijeme pandemije. Čak 71% sigurnosnih stručnjaka primijetilo je porast sigurnosnih prijetnji ili napada, a vodeća prijetnja bila je phishing (55%), a zatim zlonamjerne stranice koje nude informacije i savjete o pandemiji (32%) te je primijećeno povećanje broja zlonamjernih programa (28%) te *ransomware* napada (19%). Tri vodeća izazova za stručnjake bila su osiguravanje sigurnog daljinskog pristupa, potreba za skalabilnim rješenjima za daljinski pristup te korištenje nepovjerljivih softvera, alata i usluga od strane korisnika.[104] Jedan od velikih *ransomware* napada bio je napad na kompaniju davatelja IT usluga iz New Jerseya Cognizant. Napad na sustave ove kompanije bio je potencijalno ozbiljan jer ista pruža usluge u oblaku i sadrži podatke iz područja bankarstva, zdravstva, zaštite i proizvodnje. Maze, *ransomware* korišten u napadu specifičan je po tome što ne samo da šifrira podatke na zaraženim Windows sustavima već i izvlači kopije originala. Pretpostavlja se da je isti ukrao dokumente klijenata, što je samo jedan u nizu napada na sustave IoT-a za vrijeme pandemijske krize.[105]

Nadalje već spomenuta aplikacija koju su morali preuzimati zaraženi koronavirusom u Južnoj Koreji i Kini pokrenula je pitanja o privatnosti osoba. Ista se nije razvijala i primjenjivala na razini Europske Unije jer bi se smatrala kršenjem pravila o privatnosti. Tako su rasprava i transparentnost dosegli novi vrhunac.[106] Diljem svijeta koristile su se aplikacije i platforme koje su prikupljale brojeve telefona, lokaciju, rute kretanja i putovanja, kontakte oboljelih, simptome i osobne podatke koje uključuju velike tehnološke kompanije poput Facebooka, Googlea, Applea, Amazona, IBM-a koje se nisu posebno oglasile vezano za korištenje podataka potrošača u komercijalne svrhe. Jedan od uređaja korištenih u svrhu prikupljanja podataka su i pametne narukvice primjerice kompanije Accent.[107] Poteglo se pitanje morala i prava svakog pojedinca, no međutim također se nije dobio konkretan odgovor. Također jedno od važnih pitanja je i to, kako će te aplikacije i kompanije funkcionirati nakon pandemije i koristiti podatke u nelegalne svrhe što dalje predstavlja i problem za zakonodavstvo.[108]

Jedno od velikih pitanja za vrijeme pandemijske krize, bilo je upravo pitanje sigurnosti. Uzme li se samo primjer Zoom platforme za videokonferencije koji su koristili poslovni korisnici i škole diljem svijeta, i čija je upotreba s deset milijuna korisnika iz 2019. narasla na čak 300 milijuna dnevnih korisnika na početku 2020., a čija enkripcija nije bila u potpunosti s kraja na kraj (eng. end-to-end). Otkriveno je također da Zoomova politika privatnosti daje pravo kompaniji da radi što god poželi s podacima korisnika. Većina tih nedostataka je ispravljena no ne u potpunosti.[109]

Implementacija IoT-a u zdravstveno okruženje donijela je određene prednosti i mane. Pacijenti raznih zdravstvenih ustanova uvidjeli su velika poboljšanja zahvaljujući uvidu u podatke i pravovremenost koje takvi uređaji omogućavaju. Broj medicinskih uređaja u IoT okruženju raste, ali kao i kod brojnih drugih tehnologija i okruženja, sigurnost uređaja je jako zapostavljena što je dovelo do povećanih napada *ransomwareom* na zdravstveni sustav. Osim sigurnosnih izazova pojedinih uređaja, zdravstveni sustavi susreli su se s izazovom zaštite mreža, nedostatka sigurnosnih zakrpa različitih operativnih sustava i brojnih drugih. Tako da unatoč tome što je IoT znatno pružio broj olakšanja, uveo je i brojne rizike i nedostatke takvom sustavu. Društveni kontekst napada na IoT sustav za vrijeme pandemijske krize uzrokovane COVID-19 virusom imao je gori učinak od financijskog jer su napadi predstavljali dodatno opterećenje na već ionako preopterećeni sustav.[110]

Kibernetički napadi na zdravstvene sustave diljem svijeta već treću godinu za redom obaraju rekordne vrijednosti. U SAD-u više od 500 organizacija za pružanje zdravstvene skrbi u 2021. godini doživjelo je neku vrstu kršenja privatnosti razotkrivanjem 40 milijuna kartona pacijenata, a u Izraelu je također porastao broj napada nakon uspješnog napada na medicinski centar Hillel Yaffe u Haderi u listopadu 2021. godine.[110] Prema izvješću kompanije za kiberntičku sigurnost, napadi *ransomwarea* na Izraelski zdravstveni sustav između siječnja 2020. do rujna 2021. godine porastao je za 600%. Prema izvješću Izrael je na prvom mjestu liste najciljanijih zemalja prema broju podnesaka izvješća o napadu, a slijede Južna Koreja, Vijetnam, Kina, Indija, Kazahstan, Filipini, Iran i Ujedinjeno Kraljevstvo.[111]

Za vrijeme pandemije također je poraslo i nepovjerenje korisnika i zabrinutost za sigurnost vezano za tehnologiju i IoT uređaje. Trenutni problemi trebali bi staviti fokus na dovođenje novih standardizacijskih i pravnih propisa koje bi mogle dovesti do povećanja kibernetičke sigurnosti u dugoročnom razdoblju. Također, u prošlosti su ekstremni događaji koji su uključivali ekstremne povrede sigurnosti dovodili do novih sigurnosnih standarda pa možda upravo slučaj Covid-19 bude razlog za pokretanje novih standarda i zakona o kojima se više bavi peto poglavlje ovoga rada.[106]

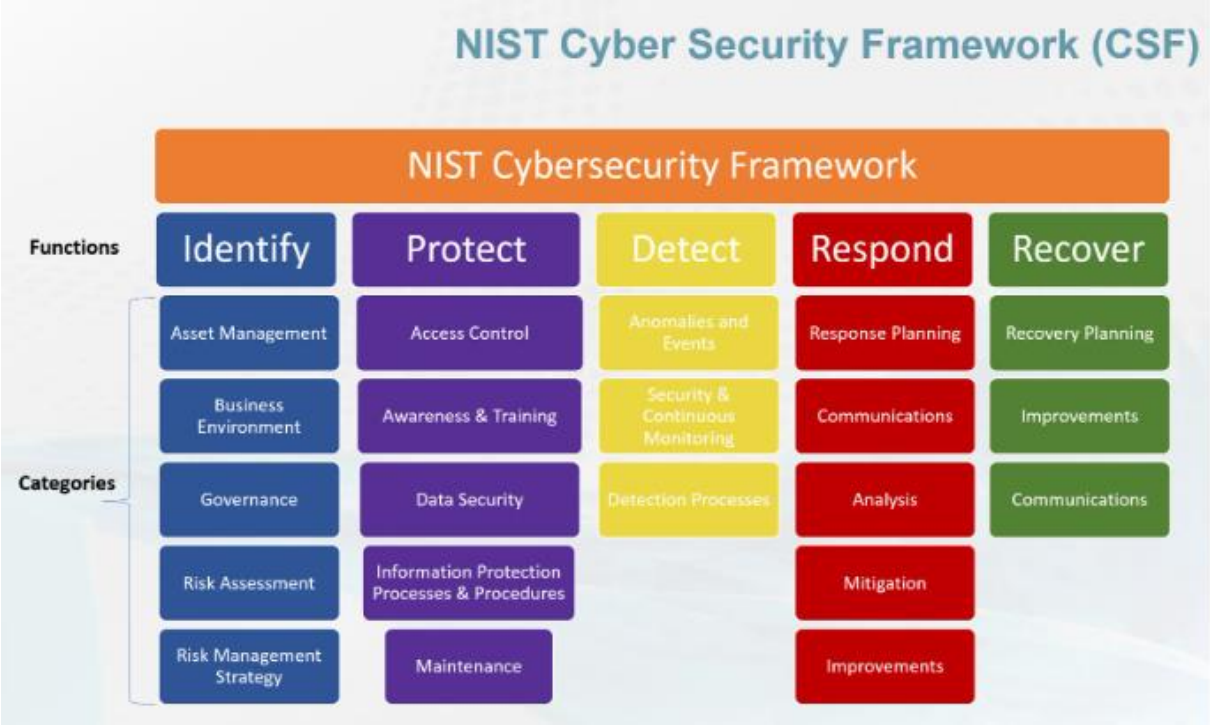
4. Sigurnost u Internetu stvari

IoT sigurnost odnosi se na metode zaštite koje se koriste za osiguranje uređaja povezanih u sustavu IoT. IoT sigurnost jedan je od najvećih izazova današnjeg IoT-a i tehnoloških stručnjaka. Danas postoje razne tehnike, metode i alati kojima se nastoji poboljšati sigurnost i osigurati povjerenje korisnika IoT sustava, a neke od metodologija koje spadaju pod okrilje sigurnosti IoT-a su sigurnost sučelja aplikacijskog programa (eng. Application programming interface - API) , provjera autentičnosti infrastrukturom javnog ključa (eng. Public key infrastructure - PKI) i mrežna sigurnost, koje se mogu koristiti u borbi protiv rastuće prijetnje kibernetičkog kriminala. IoT sigurnost trebala bi se primjenjivati i implementirati od pripreme, tijekom procesa istraživanja, razvoja bilo potrošačkog, poslovnog ili industrijskog, a ne samo u fazi dizajna i kroz sve slojeve referentne arhitekture IoT sustava. PKI i digitalni certifikati idealan su način osiguravanja sigurne veze između više umreženih uređaja. Koristeći asimetrični kriptografski sustav s dva ključa, PKI olakšava šifriranje, dešifriranje privatnih poruka i interakcije pomoću digitalnih certifikata te zaštite podataka koje se unose u običnom (eng. Plain) tekstu primjerice za dovršavanje transakcija u kupovini na Internetu. Zaštita IoT-a također uključuje osiguranje sigurnosti mrežnih *portova,* zaštitu mreže, blokiranje neovlaštenih IP adresa, osiguravanje ažuriranosti sustava, uključivanje vatrozida ali i kompleksne zaporke i primjene definiranih sigurnosnih politika.[112]

Nadalje, uz pojam IoT sigurnosti, sve više se veže pojam povjerenja odnosno nepovjerenja korisnika jer je kako je prethodno u radu navedeno, nepovjerenje upravo jedan od razloga nekorištenja IoT sustava, a sigurnost upravo razlog tog nepovjerenja. Brojne kampanje i sigurnosni skandali koji su potresali brojne IT kompanije, IoT kampanje i nedostaci, svakodnevno otkrivanje novih situacija koje bi mogle narušiti njihovu privatnost primjerice kao kod ugradnje pametnih brojila električne energije uvedenih od HEP-a koji mjere stvarnu potrošnu pojedinih uređaja[113] ali i narušavaju privatnost korisnika jer pružaju uvide u to koliko je koji uređaj u kojem vremenu potrošio određeni iznos električne energije[114], a da pri tom potrošače nije tražena dozvola za ugradnju istih. Načini poboljšanja povjerenja korisnika je uvođenje konkretnih standarda i zakonskih okvira za regulaciju cjelokupnog IoT-a, ali i transparentnost proizvođača. Jedan od takvih primjera je veliki tehnološki div Xiaomi. Xiaomi je objavio novi skup predloženih globalnih standarda usmjerenih na jačanje sigurnosti svojih potrošačkih IoT proizvoda kojima se zadovoljavaju potrebe potrošačke IoT industrije jer ne postoji opći standard koji bi se mogao implementirati. Dokument[115] također navodi zahtjeve za sigurnost i privatnost podataka, koji između ostalog uključuju sigurnost komunikacije, autentifikaciju i kontrolu pristupa, sigurno pokretanje i brisanje podataka. Već su neki Xiaomi proizvodi dobili međunarodnu sigurnosnu akreditaciju, BSI (eng. The British Standards Institution) certifikat.[116]

4.1. Okvir kibernetičke sigurnosti prema NIST-u

NIST-ov (eng. National Institute of Standards and Technology) okvirni dokument kibernetičke sigurnosti prikazan na slici 17, pokriva sva područja kibernetičke sigurnosti u obliku sigurnosnih funkcija, kategorija, potkategorija i standarda koji su s njima povezani.



Slika 17. NIST-ov okvir kibernetičke sigurnosti, [117]

NIST CSF (eng. NIST Cyber security framework) organiziran je u pet osnovnih funkcija. Funkcije su organizirane istodobno jedna s drugom kako bi predstavljale životni ciklus sigurnosti. Svaka je funkcija ključna za dobro funkcioniranje cijelog sustava i uspješno upravljanje rizikom kibernetičke sigurnosti. Identificiranje se odnosi na razumijevanje upravljanja rizikom kibernetičke sigurnosti, zaštita na poduzimanje mjera zaštite za zaštitu kritičnih infrastrukturnih usluga, otkrivanje na metode detekcije neželjenih aktivnosti u sustavu, odgovor aktivnost pri suočavanju s neželjenim događajem, te oporavak se odnosi na otpornost i vraćanje svih sposobnosti narušenih neželjenim događajem.[117]

NIST CSF razine predstavljaju koliko dobro organizacija sagledava rizik kibernetičke sigurnosti i procese koji postoje za ublažavanje rizika. To pomaže organizacijama pružiti referentnu vrijednost za njihovo trenutno poslovanje.

- Razina 1 – Djelomična: Organizacijski rizik kibernetičke sigurnosti nije formaliziran i njime se ne upravlja brzo već postupno. Također postoji ograničena svijest o upravljanju rizikom kibernetičke sigurnosti.

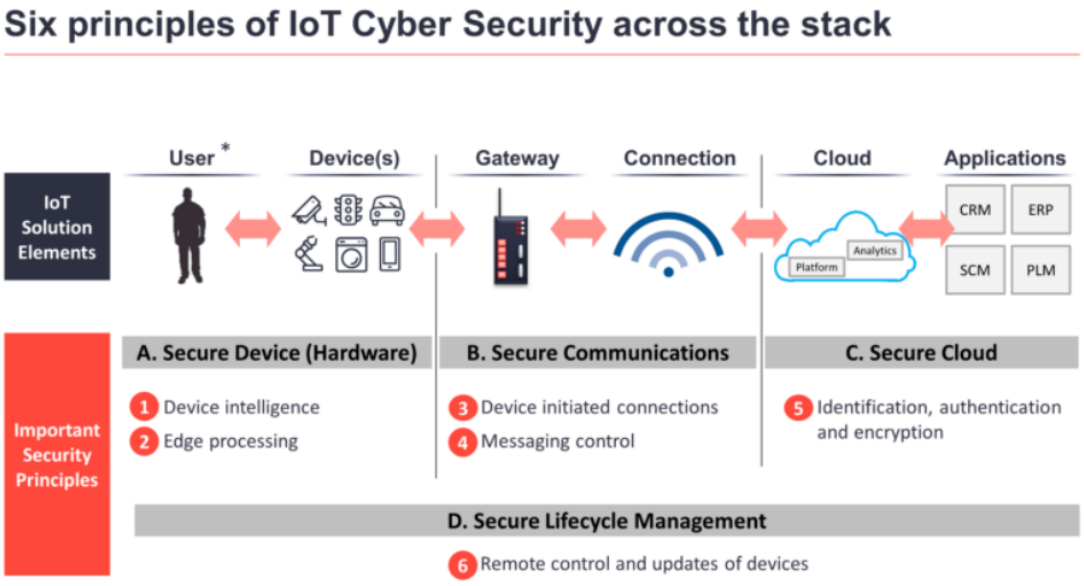
- Razina 2 – Informirani o riziku: Ne postoji politika upravljanja sigurnosnim rizicima na razini cijele organizacije. Uprava upravlja rizikom kibernetičke sigurnosti na temelju rizika kada se dogode.

- Razina 3 – Ponovljivo: Formalni proces upravljanja organizacijskim rizikom prati definirana sigurnosna politika.

- Razina 4 – Prilagodljivo: Organizacija će u ovoj fazi prilagoditi svoje politike kibernetičke sigurnosti temeljene na naučenim lekcijama i na temelju analitike kako bi pružila uvid i najbolje prakse. Organizacija stalno uči iz sigurnosnih događaja koji se događaju u organizaciji i dijelit će te informacije s većom mrežom.[117]

4.2. Sigurnost prema arhitekturi IoT-a

Prema glavnom izvršnom direktoru Ardexe, sigurnost IoT sustava može se sagledati kroz arhitekturu IoT-a i to kroz šest točaka prikazanih na slici 18.



Slika 18. Šest načela IoT sigurnosti kroz slojeve, [118]

Što se tiče fizičkog sloja, proizvođači originalne opreme (eng. Original Equipment Manufacturer - OEM) i dizajna (eng. Original Design Manufacturer - ODM) sve više integriraju sigurnosne značajke u hardver i softver kako bi poboljšali sigurnost istih, a neke od njih uključuju sigurnost čipa u obliku TPM (eng. Trusted platform modules) koji djeluju kao temeljno povjerenje štiteći informacije i vjerodajnice, sigurnosno pokretanje odnosno osiguranje pokretanja samo provjerenog softvera na uređaju, te fizičku zaštitu odnosno zaštitu od neovlaštenog fizičkog pristupa uređaju. Načela ovog sloja uključuju inteligenciju uređaja u kontekstu upravljanja sa sigurnošću, enkripcijom, autentifikacijom, vatrozidom i dr. te obradu na rubu (eng. Edge) koja se odnosi na lokalnu obradu podataka prije prenošenja na oblak što omogućuje poboljšanje sigurnosti.[118]

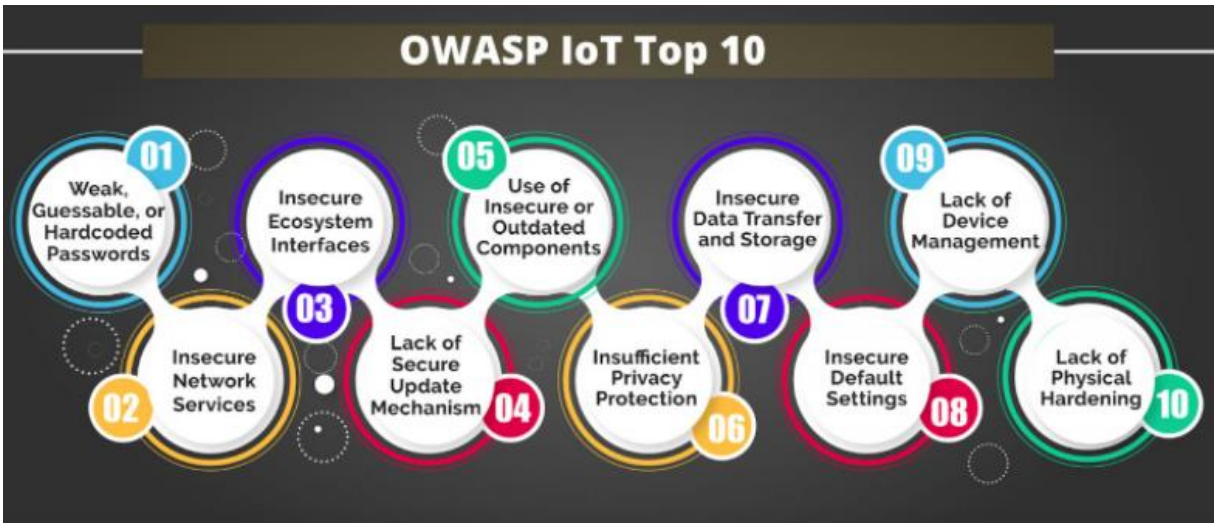
Komunikacijski sloj je bitan jer povezuje sve uređaje u sustavu, a rješenja koja se na njega odnose usmjerena su na sigurno šifriranje podataka u fazi mirovanja i prijenosa te vatrozida i sustava za sprječavanje neželjenih upada. Načela ovog sloja odnose se na pokretanje veze s oblakom, ne obrnuto što se prvenstveno odnosi na otvaranje određenih *portova* vatrozida jer je u tom smjeru manji sigurnosni rizik te kontrola poruka korištenjem protokola koji uključuju dvostruku enkripciju, filtriranje i dr. Ispravno označavanje poruka omogućuje primjenu određenih sigurnosnih politika na iste, što omogućuje bolju kontrolu i sigurnosnu razmjenu.

Sloj oblaka odnosi se na softversku pozadinu rješenja IoT-a, gdje se unose svi prikupljeni podaci koji se analiziraju kako bi se izvele određene radnje, a sigurnost oblaka oduvijek je bila tema rasprava stručnjaka. Važne značajke kibernetičke sigurnosti uključuju šifriranje osjetljivih podataka pohranjenih u oblaku, provjeru integriteta drugih platformi i aplikacija te korištenje digitalnih certifikata za identifikaciju i provjeru autentičnosti. Sigurno upravljanje životnim ciklusom odnosi se na sveobuhvatni sloj s kontinuiranim procesima potrebnim za održavanje sigurnosti IoT-a odnosno osiguravanje dovoljnih razina sigurnosti od proizvodnje uređaja, početne instalacije do uporabe. Za ovaj sloj važno je praćenje aktivnosti i evidencija sumnjivih aktivnosti. Također podrazumijeva redovna ažuriranja i sigurnosne zakrpe uređaja kako bi isti bili što otporniji na ugroze i popravile se moguće ranjivosti te sigurno daljinsko upravljanje.[119]

4.3. Sigurnosne prakse

Nedostatak sigurnosti narušava cjelokupnu svrhu posjedovanja naprednog sustava za prijenos i upravljanje podacima i dovodi do operativnih rizika i financijskih gubitaka. Napad na bilo koji od povezanih IoT uređaja može ugroziti sigurnost cijele mreže. Stoga proizvođači Interneta stvari moraju usvojiti pristup usmjeren na sigurnost kako bi spriječili napade i maksimalno iskoristili njegov puni potencijal. Široko cijenjeni projekt sigurnosti otvorenih web aplikacija (eng. Open Web Application Security Project - OWASP) s ciljem promicanja sigurnog digitalnog ekosustava odredio je OWASP IoT top 10 ranjivosti kako bi pomogao

proizvođačima, poduzećima i potrošačima da bolje razumiju sigurnosne prijetnje koje vrebaju unutar internetskog svijeta.[120] Na slici 19. prikazane su ranjivosti, a kroz poglavlje je opisano kako bi se na iste moglo preventivno djelovati u svrhu bolje zaštite i sigurnosti.



Slika 19. Deset ranjivosti prema OWASP-u, [120]

IoT uređaji sa slabim ili zadanim zaporkama, kako je i pokazano kroz rad imaju veliki potencijal postati meta kibernetičkog napada. Uspješan pokušaj neovlaštenog pristupa jednom uređaju ostavlja druge u sustavu ranjivim jer IoT uređaji često dijele iste zadane lozinke. Prema OWSAP-u svaki uređaj mora imati jedinstveni skup vjerodajnica, imati onemogućeno korištenje inicijalnih odnosno zadanih zaporki, te uklonjena stražnja vrata (eng. Backdoor) stvorena tijekom otklanjanja pogrešaka. Mrežne usluge unutar uređaja mogu predstavljati ozbiljnu prijetnju sigurnosti i integritetu sustava i napadači mogu uspješno ugroziti sigurnost IoT krajnje točke iskorištavanjem slabosti prisutnih u modelu mrežne komunikacije pa sukladno tome OWSAP predlaže korištenje sigurnosnih protokola, onemogućavanje nepotrebnih *portova* i usluga pružanja daljinskog pristupa, držanje IoT uređaja u zasebnoj mreži i instaliranje redovnih ažuriranja. Sučeljima poput pozadinskog API-ja, oblaka i mobilnog sučelja obično nedostaje pravilne autentifikacije, enkripcije i filtriranja podataka što može negativno utjecati na sigurnost IoT uređaja pa je preporuka držati se načela najmanje privilegija i jake provjere autentičnosti na IoT uređajima.

Korištenje nesigurnih ili zastarjelih komponenti predstavlja veliku manu sustava koja olakšava neželjenom akteru napad na sustav stoga su vrlo važna redovna ažuriranja sustava i sigurnosnih zakrpa kojima se ispravljaju ranjivosti i propusti na sustavu. IoT uređaji možda moraju pohraniti i zadržati osjetljive podatke korisnika da bi ispravno funkcionirali. Međutim, ovi uređaji često ne nude sigurnu pohranu što dovodi do curenja kritičnih podataka kada ih hakiraju cyber kriminalci. Stoga je nužno ograničiti pohranu osobnih podataka na uređajima, definiranje sigurnosne politike i kreiranje plana aktivnosti na prijetnje.

Nedostatak enkripcije tijekom rukovanja osjetljivim podacima, bilo tijekom prijenosa, obrade ili u mirovanju, prilika je za hakere da ukradu i razotkriju podatke. Siguran prijenos osiguran je šifriranjem po svim razinama, korištenjem sigurnosnih protokola te korištenjem jednokratnih ključeva koji nisu pohranjeni u uređaju. Nedostatak upravljanja uređajem se odnosi na nemogućnost učinkovitog osiguranja svih uređaja na mreži. Preporuka je izolirati nesigurne uređaje na mreži, integrirati uređaje sa sustavima zaprečenjem nedostataka i uređaja za ažuriranja. Za ostale nedostatke proizvođači bi se trebali bazirati na tome da korisničko sučelje ne bude kompleksno i da korisnici s lakoćom mogu postaviti sigurnosne postavke i zaporke, te da hardver bude u skladu s potrebama korisnika i namjeni uređaja.[120]

4.4. Sigurnosne prakse nakon Covid-19

Privatnost i sigurnost IoT-a postalo je krucijalno pitanje i fokus kompanija, potrošača i regulatora. To je ponajviše posljedica sve većeg broja uređaja na mreži ali i broja napada i prijetnji koji se javljaju na dnevnoj bazi. S pojavom Covida-19 i pandemijskom krizom, broj kibernetičkih napada se povećao, a samim time se povećala i briga za sigurnost u IoT-u. Prema Iot Analytics-u[121], jedna od četiri sigurnosne prakse koje bi kompanije trebale primjenjivati, pogotovo nakon pandemijske krize je pregled inventara koje posjeduje, odnosno uvid u uređaje koji se koriste sa njihovim hardverskim i softverskim specifikacijama, analiza mrežnog prometa između uređaja, koliko je imovina i sustav ažuriran i koje su metode i brzina odgovora na potencijalne napade. Nadalje, kompanije bi trebale poduzeti određene korake pri detekciji i rješavanju problema *shadow*, odnosno privatnih i neovlaštenih uređaja kojima se zaposlenici spajaju na unutarnju poslovnu mrežu, a koji obično imaju nedovoljno ili nimalo zaštite, što se posebno pokazalo kao problem za vrijeme pandemije. U veljači 2020. godine, Zscaler, vodeći pružatelj sigurnosti u oblaku, objavio je analizu povećanja uporabe takvih uređaja u kompanijama za čak 1500%.[122] Stoga je vrlo važno poznavati imovinu organizacije, ovlaštene uređaje ali nadzirati i poboljšavati navike zaposlenika edukacijom i kroz svakodnevni rad.

Jedna od sigurnosnih praksi je također razmatranje koje aplikacije bi se trebale nalaziti u oblaku jer oblak i nije najsigurnija opcija za korištenje. Sigurnosni softverski alati koji se koriste za oblak uključuju sustave za otkrivanje i prevenciju upada (eng. Intrusion Detection Systems/Intrusion Prevention Systems - IDS/IPS), upravljanje sigurnosnim informacijama i događajima (eng. Security information and event management - SIEM) te virtualne vatrozide. Do nedavno su sigurnost i razvoj softvera bili dva različita područja prakse. Pokazalo se da ovakvi vremenski odmaci za vrijeme korone znatno dovode do povećanja sigurnosnih ranjivosti. U zadnjih pet godina, pristup „*shift left"* odnsno pomak u lijevo stekao je veliku popularnost, a isti se odnosi na praksu pomicanja sigurnosti na najraniju moguću točku u procesu razvoja. To dovodi do transformacije DevOps (eng. Development and operations) u DevSecops (eng. Development, security and operations) u kojem ključnu ulogu igra suradnja sigurnosnih stručnjaka s DevOps timom kako bi se potencijalne opasnosti svele na najmanju moguću mjeru. Pristup pomaka u lijevo uz to što se

sve više pokazuje kao najbolja sigurnosna praksa, također dovodi i do velikih ušteda. Primjerice jedan institut iz IBM-a otkrio je da je rješavanje sigurnosnih problema u fazi dizajna šest puta jeftinije nego za vrijeme implementacije.[123]

Uz stalni i sve veći razvoj umjetne inteligencije, neka tradicionalna sigurnosna rješenja nadopunjuju se sve više mogućnostima strojnog učenja kako bi se postigli bolji i brži rezultati. Mnoge sigurnosne prakse u zadnje vrijeme se odnose ponajprije na sigurnosne alate temeljene na umjetnoj inteligenciji (eng. Artificial intelligence - AI), a jedan od takvih primjera je Ciscovo uvođenje mrežne analitike temeljeno na umjetnoj inteligenciji.[123] Jedan od ciljeva ovakvih tehnologija je otkrivanje ranjivosti i anomalija u sustavu korištenjem strojnog učenja. Algoritmi pretražuju podatke o prometu IoT uređaja kako bi detektirali anomaliju. U slučaju pronalaska generira se poruka, a sustav automatski izvršava sve potrebne radnje zavisno o situaciji. Jedno od takvih tradicionalnih rješenja koja se nadopunjuju je spomenuti SIEM, a primjer takvog rješenja je IBM Qradar.[121]

5. Zakonski i standardizacijski okvir

Korištenjem uređaja Interneta stvari javlja se niz pitanja i izazova vezanih uz pravne aspekte. U nekim situacijama, uređaji IoT-a stvaraju nove regulatorne situacije koje nisu prethodno postojale, a tehnologija napreduje mnogo brže nego regulatorna okruženja. Odgovornost prilikom upravljanja sigurnošću u informacijskim sustavima, ulaganje u stručnost i konkretne sigurnosne tehnologije, trebala bi biti na najvišoj mogućoj razini, no međutim često je zanemarena. Tako da se redovne provjere i mjere zaštite podataka, što zbog manjka znanja, što zbog nedostatka regulative vezane uz sigurnost podataka, provode u minimalnim mjerama. Sve većim razvojem uređaja, aplikacija i usluga koji umreženi čine okruženje Internet stvari, javljaju se sve veće mogućnosti i beneficije od takvog okruženja. Međutim, sve većim korištenjem IoT okruženja dovodi se u pitanje privatnost i sigurnost podataka pojedinca što povlači regulatorna i pravna pitanja.

Uređaji Interneta stvari prikupljaju velike količine podataka o ljudima te su u mogućnosti te podatke prenositi do neželjenih lokacija uz malo ili nimalo tehničkih zapreka što može predstavljati veliki problem ako se radi o povjerljivim podacima. I unatoč tome što takvo okruženje omogućava niz prednosti za svakodnevne aktivnosti, ono također i donosi veliki rizik koji se najviše odnosi na zlonamjerni pristup uređajima unutar okruženja. Posljedice neovlaštenog pristupa podrazumijevaju gubitak nadzora nad uređajima, krađu osobnih podataka, dobivanje iskrivljenih podataka, krađu identiteta, prekid poslovanja, ugrožavanje potrošača, kompromitacije podataka, bankrot, troškove i brojne druge, kakvih je danas sve više. Što više pojedinci ovise o Internetu stvari, to više trebaju brinuti, jer u konačnici nitko ne želi da se brava od vrata otvara nikome osim vlasniku kuće, kao ni da uređaji za mjerenje krvnog tlaka ili primjerice šećera u krvi daju krive informacije, ili da se unutar kuće uključi grijanje umjesto hlađenja. Stoga se može zaključiti kako bi zlonamjerni upad i nadzor nad uređajima u kući od traće strane mogli biti pogubni za život pojedinca.[124]

Bilo da je riječ o jeftinim uređajima koje je danas sve lakše za nabaviti, nedovoljno razvijenim sigurnosnim softverima ili nedostatku legislative, sve je veći broj propusta i problema koje takav sustav donosi ali jednako tako i svijest čovjeka o potencijalnim rizicima svakim danom je sve veća. Iako se razvijanjem uređaja i softvera za okruženje Internet stvari, sve više razvijaju zlonamjerni softveri kojima je cilj neovlašteni upad u iste, mnoge ranjivosti i propusti IoT okruženja ublažile bi se priznatim i propisanim sigurnosnim politikama i zakonima. U dosadašnjim sustavima, prilikom incidenta, dosta je teško prebaciti odgovornost na pojedinca iz razloga što cjelokupno okruženje podijeljeno je na način da jedna tvrtka proizvodi uređaje, druga administrira, treća proizvodi sigurnosni softver, četvrta upravlja mrežom, a pojedinac na kraju koristi uređaje. S povećanim brojem incidenata u zadnje vrijeme, društvo je postalo svjesno rizika i propusta IoT okruženja, a neke države su čak počele donositi prve zakone glede zaštite pojedinaca u takvom sustavu.[125]

Do sada tehnologija okruženja Internet stvari, nije bila pokrivena zakonskim okvirom no međutim stvari su se počele sve više mijenjati, a velike promjene na tom području donijela opća uredba o zaštiti podataka (eng. The General Data Protection Regulation - GDPR) kojom je Europska Unija (eng. European Union - EU) postrožila regulativu vezanu uz osobne podatke, a mnoge zemlje diljem svijeta započele su usvajanje zakona o okruženju Internet stvari poput SAD-a, Velike Britanije i EU kako bi na taj način potakle razvoj i inovacije IoT-a.[126]

5.1. Sjedinjene Američke Države

SAD, jedna od najvećih svjetskih velesila po pitanju razvoja industrije i tehnologije, te je jedna od vodećih zemalja po pitanju implementacije IoT-a. Nerijetko je uzor ostalim zemljama koje nastoje slijediti njen primjer i upravo iz tog razloga, za primjer je navedeno zakonodavstvo na razini SAD-a po pitanju IoTa. U Sjedinjenim Američkim državama centralni nositelj vlasti je Federalna vlada Sjedinjenih Američkih država.[127] Savezne države SAD-a, također imaju vlastite ustave i dvodomne parlamente (osim Nebraske, koja ima jednodomni) koji imaju zakonodavnu vlast.[128] Tako je primjerice 2018. godine savezna država Kalifornija donijela zakon SB327[17] [129]o IoT-u i tako postala prva država koja je donijela takav zakon na snagu. Stupio je na snagu u siječnju 2020. godine, a još se naziva i „zakon o *passwordima*“ jer nalaže proizvođačima da svakom uređaju dodjeljuju jedinstvenu zaporku za svaki uređaj, koju korisnici moraju promijeniti prije prvog pristupa uređaju. Iste godine stupio je na snagu Kalifornijski zakon o privatnosti potrošača (eng. California Consumer Privacy Act - CCPA) [130] koji nalaže zaštitu prikupljenih podataka o potrošačima tvrtkama. Podaci iz 2021. godine govore kako je do tada nekoliko saveznih država uvelo određene zakonske okvire koji nalikuju kalifornijskom CCPA primjeru, a isti su vidljivi na Slici 20.

[17] Senate Bill No. 327

Slika 20. Savezne države koje uvode zakonski okvir za IoT, [131]

Zakon o poboljšanju kibernetičke sigurnosti IoT-a[132] iz 2020., donesen od strane američkog Kongresa imao je za cilj ograničiti ranjivosti na uređajima koje koriste savezne agencije. Zakon poziva Nacionalni institut za standarde i tehnologiju (eng. National Institute of Standards and Technology - NIST) da uspostavi smjernice kako bi se osigurao siguran razvoj, konfiguracija i upravljanje IoT uređajima. Interno izvješće NIST-a (eng. National Institute of Standards and Technology Interagency/Internal Report - NISTIR) 8259D[18] [133] dalo je 270 zahtjeva za Zakon o poboljšanju kibernetičke sigurnosti IoT-a, dok se NISTIR 8259A [134] izravno bavi identifikacijom uređaja u potrošačkim proizvodima. Prema njemu svi uređaji koji se nalaze unutar okruženja IoT trebaju imati jedinstvene identifikatore u siliciju, a konfiguraciju uređaja mogu promijeniti samo ovlašteni subjekti, pristup samom uređaju je zaštićen, dok se također sigurnosna ažuriranja i certifikati izdaju samo od provjerenih i odobrenih organizacija.[131]

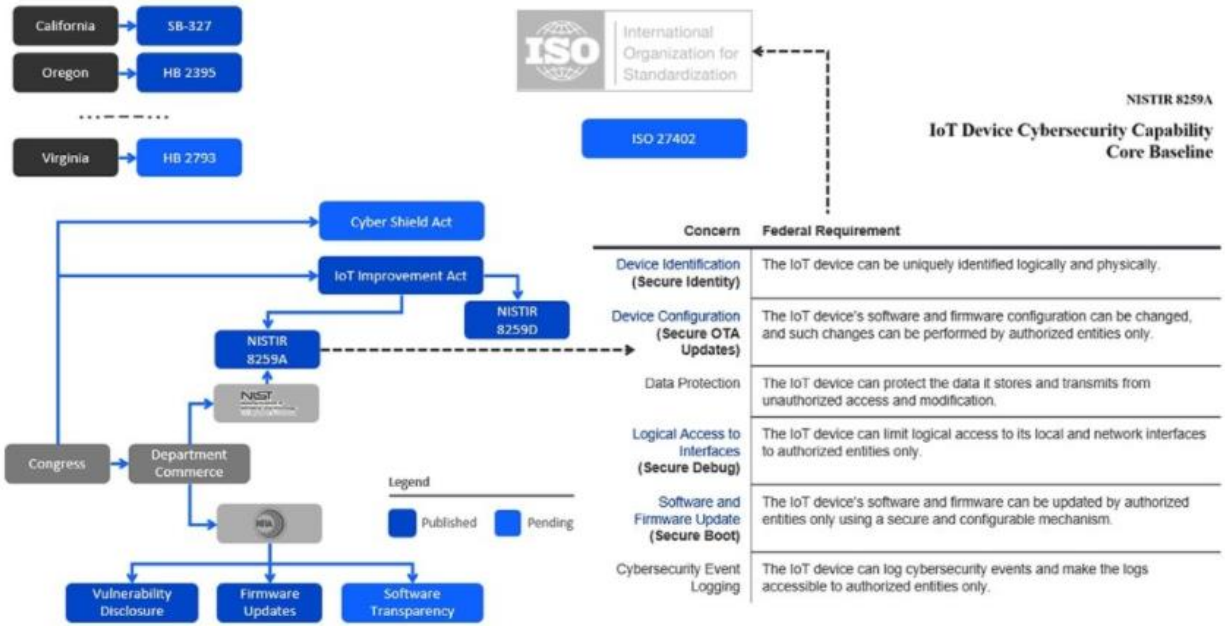
Godine 2021., na razini američkog Kongresa ponovno je predložen zakon o cyber štitu (eng. Cyber Shield Act).[135] Isti je prethodno predlagan godine 2017.[136] i 2019.[137] međutim, prijedlog zakona nikada nije stigao na glasovanje. Isti poziva na stvaranje dobrovoljnog programa certificiranja kibernetičke sigurnosti za uređaje IoT-a. Predloženim zakonom bi se uspostavio savjetodavni odbor za kibernetičku sigurnost sastavljen od stručnjaka iz različitih područja, uključujući akademsku zajednicu, vladu, industriju, grupe potrošača i javnost koji bi imao zadatak stvoriti određena mjerila kibernetičke sigurnosti. Ako IoT proizvodi zadovoljavaju ove standarde, proizvođači bi ih mogli certificirati oznakom "Cyber Shield", omogućujući potrošačima da se odluče za certificirane proizvode.[138]

[18] Nacrt NISTIR 8259D premješten je u dodatak NIST-ove publikacije SP 800-213A.[142]

Većina nacionalnih propisa u SAD-u utječe na organizacije koje surađuju izravno sa saveznom vladom, ali mnogi od tih propisa imat će učinke koji se prenose na potrošačka tržišta. One organizacije koje planiraju ponuditi svoje IoT proizvode tržištu izvan SAD-a, morat će poštovati i prilagoditi se određenim standardima koji su za ovo područje još u razvoju. Međunarodna organizacija za standardizaciju (eng. International Organization for Standardization – ISO) stvorila je ISO 27402[139], dokument koji organizacijama daje osnovne IoT sigurnosne prakse koje mogu koristiti kao osnovu. Michael Dow, viši menadžer za IoT sigurnost u Silicone Labsu smatra kako bi ISO 27402 s vremenom mogao zamijeniti NIST, jer se ima priliku sinkronizirati sa Europskom Unijom te napraviti popis priznatih zahtjeva za IoT proizvode.[131]

Američki predsjednik Joe Biden, izdao je u svibnju 2021. godine izvršnu naredbu o poboljšanju nacionalne kibernetičke sigurnosti kako bi potaknuo javne i privatne sektore u prepoznavanju, otkrivanju, zaštiti od sve većih kibernetičkih napada.[140] Rezultat je to sve češćih i sofisticiranijih zlonamjernih kibernetičkih kampanja te kao odgovor na incidente SolarWinds i Microsoft Exchange.[141]

Na slici 21 prikazana je shema državne regulative SAD-a koja shematski prikazuje sve što je opisano kroz ovo poglavlje.



Slika 21. Shema državne regulative SAD-a, [131]

5.2. Europska Unija

Europska Unija započela je sa pripremama za doba Interneta stvari još davne 2005. godine sa pravilnikom o Europskom informacijskom društvu za rast i zapošljavanje[19][143]. Obuhvaćao je strategije za vođenje informacijskog društva i medijskih politika i predstavljao je temelj politike za regulaciju, ulaganje, istraživanje, razvoj, inovacije te korištenje informacijsko komunikacijskih tehnologija u gospodarstvu i društvu.[144] Nakon toga, područje regulacije postupno se povećavalo različitim direktivama koje se odnose na standardizaciju, privatnost, zaštitu podataka, kibernetičku sigurnost i kriminal. Uredbe za okruženje Internet stvari zahtijevaju da se odluke odnose kako na uređaje tako i na mrežu te podatke koji se prenose njom.[145]

U području standardizacije, godine 2014. donesena je direktiva 2014/53/EU[146] o usklađivanju zakonodavstva država članica, a ona se odnosi na tržište radio opreme koje je od bitnog značaja za budući zajednički i usklađeni razvoj tehnologije. Ova direktiva EU definira pravila vezana za stavljanje radijske opreme na unutarnje tržište, a zahtjevi navedeni u članku 3. odnose se na zaštitu osobnih podataka i privatnosti i zaštitu od prijevare.[147]

Od 2018. godine na snazi je GDPR uredba koja sadrži jedinstven set pravila i odredbi koja se izravno primjenjuju unutar EU. Još 1995. godine EU je donijela prvu Uredbu o zaštiti podataka unutar koje se nalazio minimalan set pravila za zaštitu istih. Kako tehnologija svakim danom sve više napreduje, javila se potreba za unaprjeđenjem iste. Godine 2016. Europski parlament i Vijeće donijeli su Uredbu (EU 2016/679)[148] koja predstavlja usklađeno zakonodavstvo u svim članicama EU, štiti privatnost građana Unije te mijenja način na koji razne organizacije postupaju sa podacima građana. Donošenjem ove uredbe, građani imaju veću kontrolu nad svojim osobnim podacima. Na neki način, uredba koja je donesena, prilagođena je vremenu i tehnologiji u kojoj živimo. S obzirom na to da smo u današnjem svijetu obavezni ostavljati podatke u različitim ustanovama, bilo akademskim, zdravstvenim, financijskim, telekomunikacijskim veoma je teško te podatke očuvati i zaštiti, međutim po GDPR-u sve kompanije moraju legalno prikupljati podatke s konkretnim razlogom te da su isti zbrinuti, zaštićeni i dobro pohranjeni. Obrada osobnih podataka dopuštena je prema članku 6. ove uredbe ako se isti prikupljaju temeljem dopuštenih osnova, a jedna od takvih je i legitimni interes voditelja obrade, iznimno ako su temeljna ljudska prava jača od tih interesa. Brojne industrije smatraju da GDPR omogućava dovoljno sigurnosti vezano uz primjenu pravnih osnova legitimnog interesa, jer isti nije dovoljan da takva obrada podataka bude legitimna. Brojni smatraju kako GDPR uredba u kombinaciji s direktivom o e-privatnosti (2002/58/EC)[149] donose brojne prepreke koje bi na neki način mogle usporiti razvoj usluga IoT-a ili u krajnjem slučaju poskupiti i zakomplicirati njegovu implementaciju.[150]

[19] i2010 – A European Information Society for growth and employment.

Godine 2017. donesena je Uredba o e-privatnosti[151] koja je zamijenila Direktivu o e-privatnosti iz 2002. godine. Ova uredba namijenjena je zaštiti osobnih podataka u elektroničkim komunikacijama što obuhvaća niz usluga poput poziva, poruka, maila, aplikacija, video poziva, i brojnih drugih. To uključuje telekomunikacijske operatere, razvijatelje mobilnih aplikacija ali i IoT okruženje. Uredba za razliku od direktive iz 2002. godine koja je omogućavala državama članicama da donose vlastite mogućnosti zaštite pod okvirom izvorne direktive, vrijedi za sve članice jednako. Ista se još naziva i „*cookie law*“ iz razloga što se kasnijim unaprjeđenjem odnosila i na dio web-a gdje korisnici daju suglasnost za prikupljanje podataka vezanog za kolačiće.

Hrvatska je donijela Zakon o elektroničkim komunikacijama, opisan u narednom poglavlju, koji je bio u duhu direktive o e-privatnosti. Uredba o e-privatnosti ima cilj regulirati sva pitanja vezana za podatke unutar elektroničkih komunikacija, te na neki način je nadopuna na GDPR. Obuhvaća marketing i niz tehnologija koji se koriste za praćenje komunikacija kako bi se što više smanjili problemi poput neželjenih poruka, automatiziranih poziva i reklama te profiliranja, a zahtjeva pristanak korisnika. Korisnici na ovaj način imaju veću kontrolu nad svojim podacima kao i izbor kojim lokacijama će omogućiti prikupljanje osobnih podataka. Metapodaci su anonimni i privatni te izbrisani ako korisnici ne daju svoj pristanak za prikupljanje istih. Međutim, brojne industrije smatraju Uredbu ograničenjem za razvoj usluga koji su temeljeni na analizi velikih podataka iz razloga što ona ne predviđa legitimni interes voditelja obrade kao jednu od dopuštenih osnova te prema njoj se obrada podataka, čak uz privolu osobe, treba obavljati anonimno.[152]

Zakonski okvir vezan uz kibernetički kriminal, donesen je Direktivom 2013/40/EU o napadima na informacijske sustave[153], prema kojoj se uvodi minimalan set pravila, koja opisuju definicije kaznenih djela kao i određenih sankcija vezanih za napade na informacijske sustave, a kibernetička sigurnost definirana je nedavno usvojenom Direktivom o mrežnoj i informacijskoj sigurnosti (Network and Information Security Directive - NIS)[154]. Osnovni cilj ove direktive sastoji se u osiguranju velike razine mrežne i informacijske sigurnosti u Uniji povećavajući koordinaciju između svih država članica.[155]

Kako bi se osigurao integritet i kontinuitet poslovanja operatera ključnih i digitalnih usluga, NIS direktiva propisuje da tvrtke iz sektora kao što su: digitalnih usluge, energetika, prijevoz, bankarstvo, zdravstvo, vodo-opskrba i koje odgovaraju kriterijima propisanim zakonom, moraju implementirati tehničke i organizacijske mjere za upravljanje rizikom, ali da se prilikom toga vodi računa o novijim tehničkim dostignućima koja se koriste u okviru najbolje sigurnosne prakse u dijelu kibernetičke sigurnosti te mjere za suzbijanje i olakšavanje djelovanja incidenata na sigurnost mrežnih i informacijskih sustava. Vrlo je pozitivno to što prilikom odabira i implementacije tehničke mjere moraju uzeti u obzir najnovija tehnička dostignuća i najbolje sigurnosne prakse jer takva definicija praktički onemogućava da se, na primjer, klasični antivirusni sustavi koji se temelje na starom načinu zaštite od zloćudnog koda, smatraju adekvatnom zaštitom sustava.[156]

Godine 2019. donesena je nova uredba o EU kibernetičkoj sigurnosti[157]. Njome se prvi put uvode pravila za certificiranje kibernetičke sigurnosti na razini cijele EU. Tvrtke u

EU imat će koristi od toga da moraju certificirati svoje proizvode, procese i usluge samo jednom i vidjeti njihove certifikate priznate širom Unije. U okviru će se stvoriti više shema za različite kategorije informacijsko komunikacijskih tehnologija (eng. Information and communications technology - ICT) proizvoda, procesa i usluga. Svaka će shema, između ostalog, navesti vrstu ili kategorije ICT proizvoda, usluga i procesa koji su obuhvaćeni, svrhu, sigurnosne standarde koji moraju biti ispunjeni i metode ocjene.[158]

Ova uredba jača agenciju za kibernetičku sigurnost Europske unije (eng. The European Union Agency for Cybersecurity - ENISA) koja je posvećena postizanju visoke zajedničke razine kibernetičke sigurnosti u Europi. Osnovana je 2004. te doprinosi kibernetičkoj politici EU, povećava pouzdanost ICT proizvoda, usluga i procesa sa shemama certificiranja kibernetičke sigurnosti, surađuje s državama članicama i tijelima EU i pomaže Europi u pripremi za kibernetičke izazove sutrašnjice. Kroz razmjenu znanja, izgradnju kapaciteta i podizanje svijesti, Agencija djeluje zajedno sa svojim ključnim dionicima na jačanju povjerenja u povezano gospodarstvo, povećanju otpornosti infrastrukture Unije i, naposljetku, za održavanje digitalnog osiguranja europskog društva i građana.[159]

Područje sigurnosti Interneta stvari na razini EU za sada je dosta dobro pokriveno navedenim direktivama i uredbama. Međutim, u budućnosti, kako se razvija tehnologija, sustavi, ali i pojavljuju različiti oblici računalnog kriminala, zasigurno će biti potrebne dopune i izmjene postojećih ali i stvaranje novih zakonskih okvira.

5.3. Republika Hrvatska

S obzirom na to da je Republika Hrvatska punopravna članica Europske Unije, na nju se izravno primjenjuju Uredbe donesene u Uniji budući da su one obvezujuće za sve države članice[160], tako da su prethodno navedene uredbe uvedene u pravni okvir Republike Hrvatske. Hrvatska kao ni EU, nema definiran zakon vezan za sigurnost Interneta stvari, ali zakonima EU, jednako kao i svojim vlastitima, za sada pokriva to područje.

Godine 2001. Vijeće Europe donijelo je Konvenciju o kibernetičkom kriminalu[161], koja je stupila na snagu 2004. godine. Republika Hrvatska uz brojne druge zemlje tada je bila jedna od zemalja koja je ratificirala ovu konvenciju. Iste godine na snagu su stupile izmjene i dopune Kaznenog zakona RH[162]budući da su u pravni sustav RH usvojene odluke Konvencije o kibernetičkom kriminalu i Dodatnog protokola te Konvencije 2004. godine[163]. Na taj način Republika Hrvatska postavila je okvire za društveno neprihvatljivo ponašanje, te uvela sankcije za isto, a vezano uz računalne sustave, a opisi kaznenih djela vezanih uz računalne sustave koja su do tada već postojala nadopunjeni su i usavršeni. Ova konvencija predstavlja oblik međunarodnog ugovora, što je vrlo bitno jer se njime uređuju međunarodni odnosi između subjekata međunarodnog prava.[164]

Sabor Republike Hrvatske, u lipnju 2008. godine, donio je Zakon o elektroničkim komunikacijama[165]. Njime se uredilo područje elektroničkih komunikacija, koje se najviše odnosi na pružanje elektroničkih usluga, zaštitu podataka i sigurnost komunikacija, kao i korištenje komunikacijske mreže. Također, uredilo se područje vezano uz adresiranje i upravljanje radiofrekvencijskim spektrom, gradnjom i korištenjem elektroničke infrastrukture, radio i televizije, davanje univerzalnih usluga, zaštite prava korisnika i brojna druga pitanja vezana za elektroničke komunikacije.[166] Ovaj zakon više puta je dopunjen i izmijenjen, a posljednja izmjena je iz 2017. godine[167]. Usklađen je sa brojnim propisima iz EU, a njime se u pravni poredak Republike Hrvatske donose uredbe, direktive i odluke Europske Unije navedne u članku 1.a.

Godine 2018. Hrvatski sabor je na sjednici donio Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga.[168] Cilj ovog zakona je omogućavanje velike razine sigurnosti prilikom pružanja usluga koje su bitne za ključne aktivnosti u gospodarskom i društvenom sektoru. Njime se uređuju postupanja i mjere za dosezanje navedenog cilja, ovlast nadležnih tijela te tijela koja su nadležna za prevenciju i zaštitu od incidenata te tijela za nadzor provedbe. Ovim zakonom obuhvaćen je sektor energetike vezan uz električnu energiju, plin i naftu, transportni sektor unutar kojeg spada zračni, vodni, željeznički i cestovni promet, sektor financija i zdravstva, digitalna infrastruktura i usluge te poslovne usluge za državna tijela.[169]

Sukladno ovom zakonu , Vlada RH 2018. godine, donijela je Uredbu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga[170] kojom se utvrđuju određene mjere kojima bi se postigla visoka razine kibernetičke sigurnosti operatora ključnih usluga, način provedbe, kriteriji za određivanje incidenata koji imaju velik utjecaj na pružanje bitnih usluga, te druga bitna pitanja za obavješćivanje o incidentima.[171]

Vidljivo je kako se iz godine u godinu, zakoni vezani uz elektroničku i kibernetičku sigurnost sve više nadopunjuju i mijenjaju. Kako se mijenjaju tehnologije, uvode različiti sustavi, pojavljuju novi uređaji, pravni organ sve više nastoji slijediti tehnički razvoj i novonastale situacije. Primjer takve situacije je konkretno prijedlog dopune zakona o elektroničkim komunikacijama za vrijeme pandemije korona virusa COVID-19.[172] Naime, kako su mjere zaštite javnog zdravlja i mjere za suzbijanje širenja korona virusa poprimile velike razmjere, a ljudi su se počeli nadzirati kao nikad prije, javili su se prijedlozi da se nekim tehnologijama za nadzor ljudi ograniče neka temeljna ljudska prava i slobode. Tako je i Vlada Republike Hrvatske predložila donošenje dopuna Zakona o elektroničkim komunikacijama kako bi pravno omogućila lociranje putem mobilnog uređaja u svrhe provođenja mjera sprječavanja širenja korona virusa. Do sada je člankom 104. Zakona o elektroničkim komunikacijama bilo propisano da se podaci o lokaciji bez prometnih podataka, koji se odnose na pretplatnike ili korisnike javnih komunikacijskih mreža ili usluga, mogu obrađivati samo onda kada su učinjeni neimenovanima, ili na temelju prethodne privole pretplatnika ili korisnika usluga, na način i u razdoblju potrebnom za pružanje usluge s posebnom tarifom.[173]

Ovom dopunom člankom 104. ugradila bi se iznimka prema kojoj je dopuštena obrada podataka o lokaciji bez prometnih podataka u cilju zaštite nacionalne sigurnosti u situacijama proglašenja prirodne katastrofe ili epidemije zarazne bolesti. Tomu je pridodan uvjet prema kojem se u tim situacijama zdravlje i život građana bez te obrade ne bi mogli adekvatno zaštititi. Ovom izmjenom se također želi nametnuti obveza telekomunikacijskim operaterima da temeljem zahtjeva ministra nadležnog za proglašenu katastrofu ili epidemiju, tijelu državne uprave nadležnom za poslove civilne zaštite osiguraju podaci o lokaciji bez prometnih podataka.[174]

5.4. Tijela zadužena za informacijsku sigurnost u RH

U Republici Hrvatskoj, postoji niz organa odnosno državnih tijela koja su zadužena za informacijsku sigurnost u elektroničkim komunikacijskim sustavima. Zavisno o djelokrugu poslova tih tijela, neka su zadužena za akreditaciju, neka za reagiranje na računalno sigurnosne incidente, određena tijela djeluju samo unutar javnog sektora, a neka unutar državnog i sva se razlikuju po misijama i zadaćama koje obavljaju. Međutim, svi imaju samo jedan cilj, a to je zaštita podataka, osiguravanje informacijske sigurnosti, sprječavanje nastanka incidenta i provođenje standarda i mjera sukladno zakonskim okvirima. Neka od važnijih tijela za provođenje navedenog, opisana su u ovom poglavlju.

Središnje državno tijelo za informacijsku sigurnost u Hrvatskoj je Ured Vijeća za nacionalnu sigurnost (eng. National Security Authority - NSA). Zadaća ovog organa je koordinacija i usklađivanje donošenja mjera i standarda informacijske sigurnosti kao i nadziranje primjene istog, a vezanih za sigurnost informacijskih sustava i podataka unutar njih. Također, zadaća mu je i izdavanje certifikata pravnim i fizičkim osobama koje na taj način imaju pravo pristupa klasificiranim podacima bilo na nacionalnoj razini, Sjeveroatlantskog saveza (The North Atlantic Treaty Organization – NATO**)** ili EU. Jednako tako koordinira međunarodnom suradnjom u okviru informacijske sigurnosti, a odlukom Vlade u ime Republike Hrvatske zaključuje međunarodne sigurnosne ugovore vezanih uz zaštitu klasificiranih podataka.[175]

Drugo bitno nacionalno tijelo koje je zaduženo za prevenciju i zaštitu od računalnih ugroza javnih informacijskih sustava u RH je nacionalni CERT (eng. Computer emergency response team). Ono predstavlja odjel unutar Hrvatske akademske i istraživačke mreže (Croatian academic and research network - CARNET) osnovano 2007. godine prema Zakonu o informacijskoj sigurnosti RH. Primarna zadaća mu je osiguranje kibernetičke sigurnosti na nacionalnoj razini na način da obrađuje računalno-sigurnosne incidente prilikom prijave istih. Područje djelovanja mu je unutar domene .hr ili unutar hrvatskog ip adresnog prostora, odnosno barem jedna strana prilikom nastanka incidenta mora biti u tom okviru. Nacionalni

CERT bavi se javnim informacijskim sustavima koja uključuju sektor bankarstva, financija, digitalne infrastrukture, dok se Zavod za sigurnost informacijskih sustava (ZSIS) bavi tijelima državne uprave poput vojske, policije, vlade i dr. Bitno je napomenuti kako se ovo tijelo bavi incidentima sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga.[176]

Prethodno spomenuti ZSIS, predstavlja središnje državno tijelo koje se bavi tehničkim poslovima vezanih za informacijsku sigurnost. To se odnosi na određene standarde, akreditaciju sustava, upravljanje kripto uređajima koji se koriste u razmjeni klasificiranih podataka, ali također i koordinacijom za odgovor i prevenciju računalno-sigurnosnih incidenata. Područje djelovanja zavoda kao i njegove propisano je Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske[177], Zakonom o informacijskoj sigurnosti[178] te Uredbom Vlade Republike Hrvatske o mjerama informacijske sigurnosti[179]. Uz navedeno, ZSIS se još bavi i ispitivanjem tehnologija koje su određene za zaštitu klasificiranih podataka tzv. tempest zoniranje opreme, instalacija i prostora te izdavanja certifikata za isto. Jedna od zadaća zavoda je također da regulira standarde informacijske sigurnosti iz tehničkog pogleda te da iste usklađuje s međunarodnim standardima i preporukama. Uz to, pruža potporu Uredu vijeća za nacionalnu sigurnost u poslovima akreditacija, te nacionalnom CERT-u u poslovima prevencije i zaštite od računalnih ugroza.[180]

Nacionalno regulatorno tijelo koje se bavi regulatornim poslovima vezanih za elektroničke komunikacije, poštanske te željezničke usluge je Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM). Ovo tijelo svojim radom odgovorno je Hrvatskom saboru, a godišnje Hrvatskom saboru i Vladi podnosi izvješće o radu, a zakonitost njegovih odluka podliježe sudskoj kontroli. Regulatorne ali i ostale poslove, HAKOM obavlja sukladno zakonima za čiju je provedbu i sam nadležan. U djelokrugu rada su primarno Zakon o elektroničkim komunikacijama, Zakon o mjerama za smanjenje troškova postavljanja elektroničkih komunikacijskih mreža velikih brzina[181], Zakon o poštanskim uslugama[182], Zakon o regulaciji tržišta željezničkih usluga i zaštiti prava putnika u željezničkom prometu[183] te Zakon o željeznici[184], a uz to sudjeluje u provedbi i brojnih drugih zakona. Ovo je tijelo koje također ima i inspekcijske ovlasti i ovlašteno je za rješavanje sporova između davatelja usluga i krajnjih korisnika. Jedna od važnijih zadaća mu je regulacija tržišta kako na području elektroničkih komunikacija tako i u poštanskom i željezničkim uslugama, a posebna pozornost posvećena je pružanju univerzalnih usluga koje bi po pristupačnim cijenama morale biti dostupne svim korisnicima na području Republike Hrvatske.[185]

Uz navedene bitno je još spomenuti i agenciju za zaštitu osobnih podataka (AZOP). Ona je jedino neovisno javno nadzorno tijelo u Republici Hrvatskoj neovisna pravna osoba koja obavlja poslove u okviru djelokruga i nadležnosti utvrđenih Zakonom o provedbi Opće uredbe o zaštiti podataka[186] kojim se osigurava provedba Opće uredbe o zaštiti podataka. Neovisnost tijela za zaštitu osobnih podataka propisuje osim toga i Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog

protokola uz istu u vezi nadzornih tijela i međunarodne razmjene podataka, a koji su u Republici Hrvatskoj potvrđeni zakonom.[187] Jedna od glavnih zadaća joj je praćenje i provođenje primjene GDPR, a s obzirom na to da je Republika Hrvatska punopravna članica Europske unije i Vijeća Europe, jedan od važnijih zadataka joj je ispunjavanje prava i dužnosti u području zaštite podataka, ali i povećanje odgovornosti i svijesti građana o važnosti zaštite osobnih podataka te sudionika u procesu obrade podataka.[188]

6. Analiza istraživanja

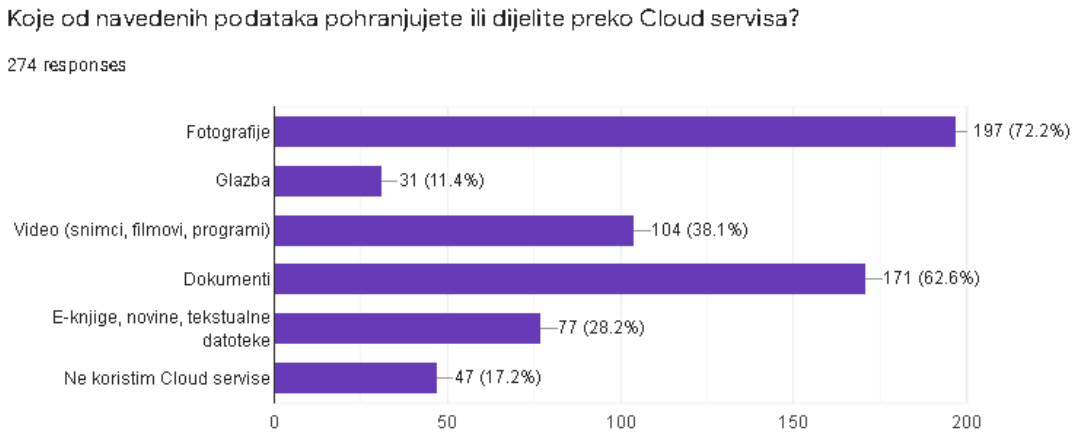
Korisnici imaju važnu ulogu u zaštiti podataka u IoT sustavu svojim ponašanjem, navikama i praksom kao što je prikazano kroz ovaj rad. Činjenica je da se od tehnologije ne može pobjeći i da nam ona postaje sastavni dio života. U jednu ruku korisnici su prisiljeni koristiti tehnologiju po cijenu da ista prati njihovo kretanje i prikuplja podatke o njima, ali s druge strane ista se može ograničiti te neki podaci mogu ostati tajni i sigurni. Prvenstveno se to odnosi na prihvaćanja uvjeta korištenja određenih aplikacija, instaliranje sumnjivih aplikacija, korištenje *cloud* platformi za pohranu podataka i brojne druge. Isto kao što u stvarnome svijetu nećemo ispred bilo koga iznijeti važne i privatne informacije, jednako tako takvi podaci ne bi se trebali nalaziti na Internetu. No i ako se nalaze, sustave je potrebno štiti jakim zaporkama, redovitim ažuriranjima i sigurnosnim zakrpama, te koristiti certificiranu i provjerenu tehnologiju.

Za potrebe izrade ovog rada, provedeno je anketno istraživanje sa svrhom ispitivanja navika i svijesti potrošača o okruženju Interneta stvari s aspekta sigurnosti kojim se nastojalo utvrditi koje su to svakodnevne navike korisnika i koliko su svjesni pametnog okruženja oko sebe i što to za njih predstavlja, a s ciljem buđenja svijesti o podacima koji se o njima prikupljaju i o svijetu u kojem živimo.

Anketa je provedena putem Google Forms obrasca, te se kroz 17 pitanja, koja se nalaze u Prilogu 1, nastojalo ispitati stavove 274 ispitanika. Ispitanici su podijeljeni po spolu, dobi i stupnju obrazovanja. U anketnom ispitivanju sudjelovao je jednak broj muškaraca i žena. Nadalje, od ukupnog broja ispitanika sudjelovalo je 1,8% ispitanika dobi do 17 godina u koju spadaju djeca i adolescenti, 21,9% ispitanika dobi u rasponu 18-30 godina odnosno mlade osobe i studenti, 45,3% ispitanika u rasponu između 31 i 45 godina odnosno osobe zrele životne dobi kojih je ujedno u ovom istraživanju najviše sudjelovalo, 27,4 % ispitanika srednje životne dobi u rasponu od 46 do 60 godina starosti te 3,6% ispitanika preko 60 godina životne dobi odnosno starije osobe i umirovljenici. Prema stupnju obrazovanja sudjelovalo je 1,8% ispitanika sa završenim osnovnoškolskim obrazovanjem, 27,4% ispitanika sa završenom srednjom školom, 17,2% ispitanika sa završenim preddiplomskim studijom, 43,1% ispitanika sa završenim diplomskim studijom kojih je ujedno najviše u istraživanju, te 10,6% ispitanika sa završenim poslijediplomskim studijom. Ostalih 14 pitanja odnose se na ponašanje korisnika na Internetu, njihovo korištenje IoT-a i ispitivanje njihovih stavova.

S obzirom na to da je *Cloud* jedna od komponenti sustava IoT, ispitanicima su postavljena tri pitanja vezana za isti. Prema rezultatima ankete velika većina ispitanika, čak 84,5% koristi neke od *Cloud* servisa za pohranu i razmjenu podataka poput OneDrive, Google Drive, Dropbox, iCloud, AmazonDrive i sl. što je potpuno očekivani rezultat iz razloga što takve platforme nude brojne mogućnosti za pohranu i razmjenu podataka većeg kapaciteta bez potrebe korištenja vanjskog medija za pohranu podataka i mogućnost dijeljenja podataka s velikim brojem ljudi istovremeno. Podaci koji se najviše pohranjuju odnosno razmjenjuju preko *Clouda* su fotografije, što je vidljivo na Grafikonu 1. Pretpostavlja se da tomu najviše

pridonosi sigurnosna pohrana fotografija s mobilnih uređaja u svrhu praktičnosti i zaštite fotografija i podataka u slučaju oštećenja ili gubitka mobilnog uređaja. Uz to se također može uključiti i video sadržaj kojeg 38,1% korisnika pohranjuje na *Cloud.* Tomu pogoduje i činjenica da je trend izrade fotografija znatno smanjen te da se fotografije sa velikih životnih događaja poput vjenčanja, krštenja, proslava rođendana ili jednostavno s izleta, uglavnom dijele preko ovakvih platformi. Zanimljiv podatak je kako svi ispitanici do 17 godina starosne dobi te više od pola ispitanika osoba starijih od 60 godina koriste *Cloud*. Druga po redu vrsta datoteke prema Grafikonu 1, koju ispitanici pohranjuju i razmjenjuju preko ovog servisa su dokumenti, čak 62,6%, što je najvjerojatnije rezultat razmjene, jer je većina ljudi za vrijeme pandemije koronavirusom COVID-19 radila od kuće te je *Cloud* bio jedan od načina razmjene dokumenata i literature između skupina i timova ljudi. Glazba je najmanje zastupljena na grafu, što je i očekivano, jer nije neophodna za posao, a u slučaju gubitka podataka s mobilnog uređaja u kontekstu sigurnosne pohrane, vrlo je jednostavno ponovno pronaći na YouTube-u.



Grafikon 1. Vrste podataka koji su dijeljeni preko *Cloud* servisa

Čak svi ispitanici koji smatraju da su podaci koji se nalaze na *Cloudu* sigurni i zaštićeni te da njima ne može pristupiti nitko osim njih koristi *Cloud*, a to je 47,8% ispitanika. Također analizom podataka utvrđeno je kako više od 40% ispitanika koji koriste navedene platforme, smatra kako su iste nesigurne ali ih i dalje koriste za razmjenu svih vrsta podataka pretpostavlja se radi praktičnosti korištenja, jednostavnosti pohrane i razmjene. To je ipak ona cijena koju korisnici tehnologije plaćaju za sve prednosti koje nam ona pruža počevši od pojednostavljenja svakodnevnih zadaća, a to je može se reći cijena plaćena privatnošću i uvidom u privatni život, ne tehnologiji, već pojedincima u čijem je ona posjedu. Iznenađuje podatak o skoro izjednačenim mišljenjima vezanih za ovo pitanje jer *Cloud* platforme nisu stara stvar i dobro je poznat problem sigurnosti i privatnosti, no međutim očigledno je

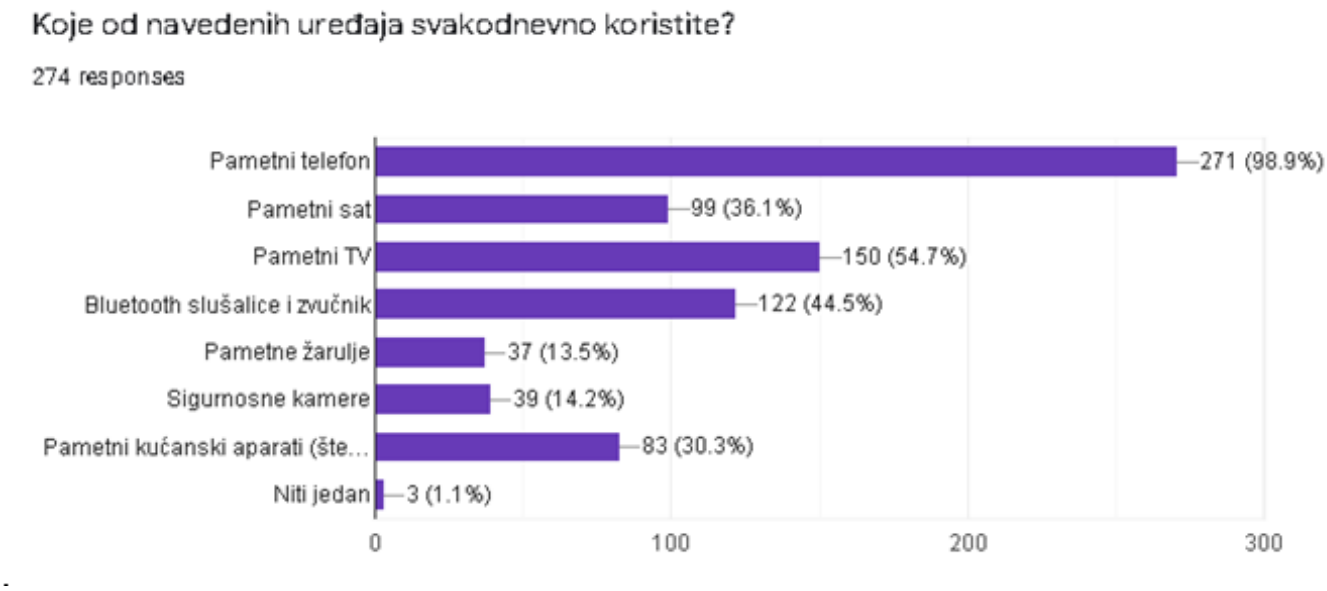
nedovoljno svijesti i brige za ovaj problem među ispitanicima svih razina obrazovanja, spolova i dobi.

Još jedan iznenađujući podatak vezan je uz pitanje zaporki servisa i aplikacija, konkretno koriste li ispitanici zaporke koje su vezane za imena, prezimena njih, njihovih bližnjih, kućnih ljubimaca ili mjesta rođenja, datume i godine, na koje je preko 70% ispitanika odgovorilo sa „ne“. Kroz ovaj rad spomenuto je u više navrata upravo problem inicijalnih i slabih zaporki. Jedan od problema također je i korištenje zaporki koje su vezane za navedene informacije. To je pogotovo problem kada je napadač pozna vaš privatni život u onolikoj mjeri da zna navedene podatke i može ih iskoristiti u nelegalne svrhe. To može biti i poznata osoba bliska žrtvi ili osoba koja je prikupila podatke o njoj putem različitih izvora (ljudi, mediji, *e-mail*, poruke, prisluškivanje i dr.). Na grafikonu 2 prikazano je također, kako 29 % ispitanika koristi zaporke sa navedenim podacima.

Grafikon 2. Zaporke temeljene na privatnim podacima

Analizom podataka utvrđeno je kako od 29% ispitanika čije su zaporke bazirane na privatnim podacima, podjednak broj žena i muškaraca. Iznenađuje činjenica da niti jedna osoba dobi do 17 godina ne koristi se ovakvim zaporkama što je veoma dobar podatak jer to znači da mladi ipak imaju svijesti da bi neželjena osoba mogla pristupiti njihovim korisničkim računima. Također iznenađuje činjenica da preko 70% ukupnih ispitanika koja se koristi ovakvim zaporka su upravo visokoškolovani ljudi, od kojih je preko 10% osoba sa poslijediplomskim studijem u dobi od 46 do 60 godina jer za takve osobe se smatra da su kroz život i školovanje stekli osobno iskustvo ili se susreli s iskustvima drugih ljudi vezanih za problem neželjenog upada na korisničke račune. Od ukupnog broja ispitanika dobi starije od 60 godina, samo 30 % koristi se zaporkama s podacima iz privatnog života što je također dobar podatak jer za starije osobe bi se smatralo da će taj postotak biti veći iz razloga da lakše zapamte zaporku povezujući je sa poznatim podatkom.

U sljedećem pitanju od ispitanika je traženo da od ponuđenih mogućnosti izaberu pametne uređaje koje svakodnevno koriste, što je prikazano na Grafikonu 3. Odgovor je očekivan jer pametni mobilni uređaj danas praktički ima svatko, iznimka u ispitivanju su dvije osobe u dobi preko 60 godina. Zatim slijede redom pametni tv, bluetooth slušalice i zvučnik te pametni sat koji danas sve više postaju trend. Također sve više raste trend pametnih kućanskih uređaja, počevši od robot usisavača čija je uporaba porasla u zadnje vrijeme, ali i ostalih poput perilica, sušilica, frižidera, štednjaka, klima kojih je sve više u ponudi na tržištu. Stoga i ne čudi da upravo kućanski aparati, čak preko 30% koriste se najviše nakon nosivih pametnih uređaja. Najmanje se koriste pametne žarulje i kamere, ali njihova će uporaba s vremenom sve više rasti, poradi fizičke sigurnosti ali i radi trenda emigracije iz Republike Hrvatske gdje imanja i kuće ostaju prazne i laka meta za provalnike.



Grafikon 3. Najkorišteniji pametni uređaji

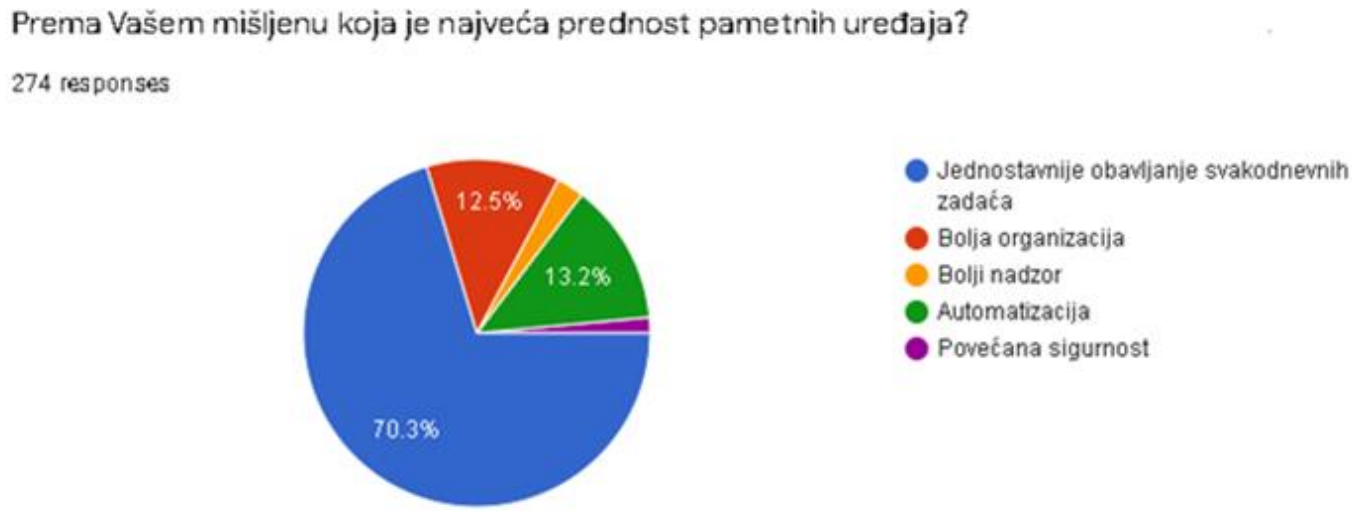
Od ukupnog broja ispitanika koji koriste pametni sat, preko 70 % koristi ga za sport odnosno za mjerenje pulsa, količine kisika u krvi, mjerenje vremena, prijeđenog puta, potrošnje kalorija, praćenja lokacije kretanja te za statistike za uspoređivanje s podacima prethodnih treninga. Od ostatka ispitanika, koji koriste pametni sat, 16% ga koristi za komunikaciju odnosno poruke i pozive, te 3% koji ga koristi za zabavu. Preostalih 3% ispitanika, pametni sat posjeduje samo iz razloga što je u trendu i jer je „in“.

Ispitanicima je također postavljeno pitanje brine li ih to da bi neželjena osoba mogla doći do podataka prikupljenih s pametnog sata i iskoristiti ih, gdje je velika većina, odnosno preko 80% ne brine, dok ostatak ispitanika brine. Preko 70% ispitanika koji smatraju da prethodno pitanje treba zabrinjavati, ne koristi pametni sat, što govori da je jedan od razloga

nekorištenja pametnog sata pitanje sigurnosti i zaštite osobnih podataka i tjelesnog stanja osobe. U tih 70 % spadaju osobe od 18 do 60 godina. Sve osobe ispod 17 i preko 60 godina smatraju da navedeno pitanje nije razlog za brigu. Zabrinjava činjenica da malo manje od 50% ispitanika koji koriste pametni sat smatra da nema razloga za brigu za krađu podataka i njihovo iskorištavanje. Pretpostavlja se da su to one osobe kojima su prednosti ovakvog uređaja puno važnije od nedostataka i ne brine ih bi li mogli biti životno ugroženi, praćeni ili biti dio statistike na koju nisu pristali dok god taj uređaj njima olakšava život.

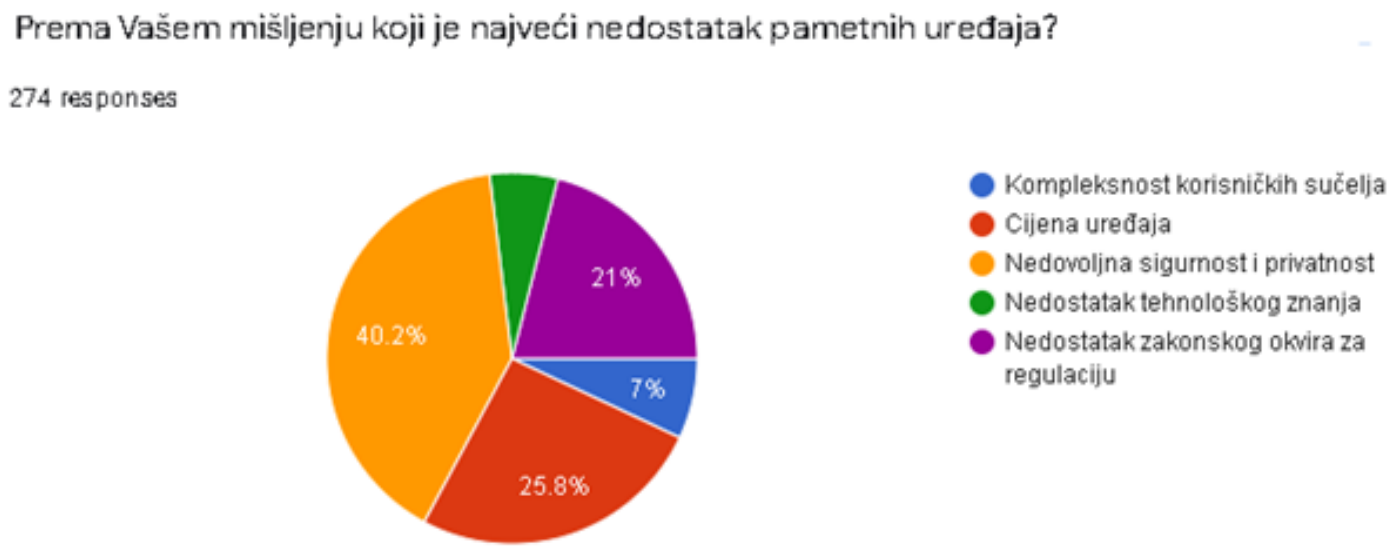
Jedna od poznatih aplikacija koja se koristi diljem svijeta je aplikacija Google Karte i upravo zbog njenog širokog korištenja korisnicima je postavljeno pitanje jer istu koriste na svojim pametnim uređajima. Preko 90 % ispitanika zna da navedena aplikacija stvara „vremensku traku“ koja pamti mjesta, vremena, dojmove i rute kretanja korisnika za svo vrijeme dok je lokacija na mobilnom uređaju uključena bez obzira što aplikacija nije korištena. Osobe koje ne znaju za navedenu mogućnost aplikacije, uglavnom su osobe od 45 na dalje godina.

S obzirom da su rezultati grafikona 3 bili očekivani, odnosno da će biti velika vjerojatnost da svi korisnici posjeduju barem jedan pametni uređaj, ispitanike je u naredna dva pitanja traženo da navedu najveću prednost korištenja pametnog uređaja što je prikazano na grafikonu 4 te najveći nedostatak istih prikazan na grafikonu 5. Prema mišljenju ispitanika, najveća prednost pametnih uređaja je upravo jednostavnije obavljanje svakodnevnih zadaća, što smatraju ispitanici svih dobnih skupina, spola i razine obrazovanja. Nadalje, automatizacija te bolja organizacija što smatraju pretežito žene. Bolji nadzor i povećana sigurnost smatra da je prednost tek 2% ispitanika što se podudara s činjenicom da mali broj ispitanika koristi nadzorne kamere za nadzor i očuvanje sigurnosti na taj način.



Grafikon 4. Najveća prednost pametnih uređaja

Najveći nedostatak prema većini ispitanika (40,2%) je privatnost i sigurnost. Uz to čak 21% ispitanika smatra da je nedostatak u nedovoljnom definiranju zakonskog okvira za isti problem, te se iz ova dva postotka može zaključiti da je preko 60% ispitanika je svjesno velikih propusta pametnog okruženja. Ostatak smatra da je nedostatak cijena uređaja, kompleksnost sučelja te nedostatak tehnološkog znanja gdje se analizom utvrdilo da ne postoji skupina koja se posebno izdvaja niti po spolu, godinama te stupnju obrazovanja.



Grafikon 5. Najveći nedostatak pametnih uređaja

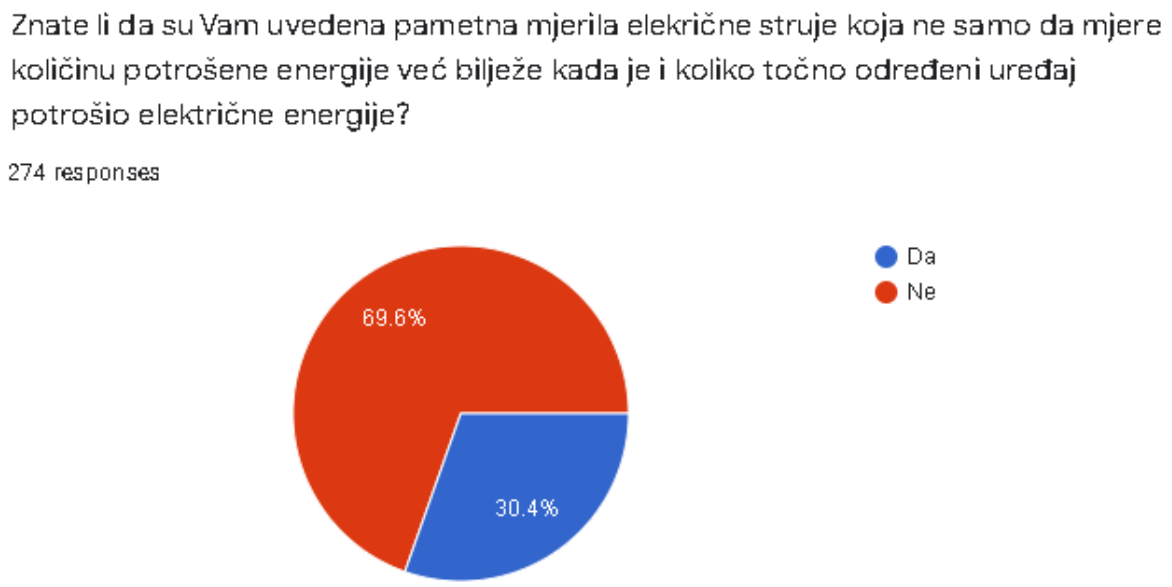
Preko 94% ispitanika nastavit će koristiti i ulagati u pametne uređaje bez obzira na njihove sigurnosne nedostatke i manjak sigurnosnih okvira. Bez obzira na to što većina smatra da je pametno okruženje nedovoljno zakonski regulirano te da podaci u njemu nisu sto posto sigurni, kroz prethodna pitanja je već zaključeno, a ovo samo potvrđuje to da su ljudi zavisni o tehnologiji te da je ona sastavni element njihova svakodnevnog dana. Tehnologija je uvijek trend, i uvijek je moderna te bez obzira na nedostatke koje ima, ljudi i oni svjesni i nesvjesni, i stariji i mlađi, i sa srednjom stručnom spremom ali i doktori, uvijek će ulagati u nju i puštati je u svoj život, tako i pametne uređaje. Koristeći pametne uređaje ljudi su bezbrižniji, mogu trčati s mobitelom u džepu mijenjajući glazbu koju slušaju na bežičnim slušalicama preko svog pametnog sata, kuću mogu nadzirati preko svog mobilnog uređaja, mogu mjeriti podatke sa svog treninga te brojne druge te je onaj rizik u koji se potrošači upuštaju, ponajprije onaj s aspekta sigurnosti i privatnosti zanemariv s obzirom na to koliko štede novca, vremena i energije koristeći pametne uređaje.

Više od pola ispitanika smatra da bi imala veće znanje i bolju kontrolu nad svojim podacima i uređajima kada bi Europska Unija bolje nadzirala privatnost pametnih uređaja i

uvela konkretnije zakonske okvire. Čak pola ispitanika koja smatra da je najveći nedostatak pametnih uređaja nedostatak zakonskog okvira smatra da ne bi imala bolje znanje i kontrolu nad podacima poboljšanjem zakonodavstva. Isto tako više od polovine ljudi koja se s tim također slaže su ispitanici po kojima je privatnost i sigurnost najveći nedostatak što dovodi do zaključka da više od pola osoba koje su odgovorile negacijom na ovo pitanje su osobe koje su svjesne sigurnosnih i pravni rizika. Grafikon 6 prikazuje stavove ispitanika po tom pitanju.

Grafikon 6. Mijenjanje stavova konkretnijim zakonskim okvirom

Da ispitanici nisu svjesni Interneta stvari oko sebe pokazuje jasno odgovor na sljedeće pitanje. Posljednje pitanje koje je postavljeno ispitanicima je ono o svijenosti da su im uvedena pametna mjerila što nije trend od jučer, već nešto što traje godinama. Skoro 70 % ispitanika nije znalo da potrošnju električne energije kućanskih aparata njihovih domaćinstava upravo mjere pametna mjerila koja bilježe kada i u koje vrijeme je koji uređaj potrošio određenu količinu električne energije na temelju koje se može prije svega dobiti statistika potrošnje određenog stanovništva, pratiti kad je neki stan ili objekt prazan ili kad je povećan broj ljudi u njemu na temelju izmjerenih podataka. Također može se vidjeti kakve su navike ljudi, koliko kasno objeduju, u koje doba idu spavati, koliko često se tuširaju, štede li energiju i brojne druge što je u jednu ruku zadiranje u intimni i privatni život ljudi. Ali bez obzira na to, velika većina ispitanika o tome nije obavještena i ne zna za to. Stavovi ispitanika prikazani su na grafikonu 7.



Grafikon 7. Svijesnost o pametnim brojilima električne energije

Na kraju analize podataka dobivenih od ispitanika različitih spolova, različite dobi i stupnja obrazovanja, dalo bi se zaključiti kako isti parametri nisu uglavnom mjerodavni ni važni za znanje i svijest o današnjoj tehnologiji. Ista pokazuje kako osobe do 17 godina u koje spadaju adolescenti i djeca te osobe starije životne dobi koje su dobar primjer jer su krajnje granice dobnih skupina, bez obzira na godine, iznenađujuće su svjesni doba u kojem žive te rizika koje tehnologija, konkretno pametni uređaji nose i primjenjuju sigurnosne prakse za koje ih se pitalo. Također, svi ispitanici različite dobi koriste minimalno jedan pametni uređaj, a većina i više od toga. Većina je svjesna nedostataka pametnog okruženja međutim velikoj većini su unatoč tome važnije prednosti koje ta tehnologija pruža i nastavit će je koristiti i dalje. Pretpostavka je da će posljednje pitanje o pametnom mjerilu barem malo potaknuti 70% svih ispitanika da se raspita o tome što im je uvedeno i što se mjeri, da će se raspitati i barem djelomično probuditi njihov interes i svijest o tome da ih u današnje vrijeme htjeli to ljudi ili ne, uvijek netko prati. Ako će posljednje pitanje barem djelomično zainteresirati one osobe koje za ovo prvi put čuju, i potaknuti ih na razmišljanje o svojoj privatnosti u današnjem svijetu, onda je ova anketa uspješna i ostvarila je svoj cilj.

7. ZAKLJUČAK

U današnje doba svjedoci smo velikog napretka tehnologije u svakom aspektu ljudskog života. Svjesni ili ne ljudi žive usporedno s tom tehnologijom koristeći je za poboljšanje kvalitete života i ekonomičnosti, a rezultat toga je nedovoljna privatnost potrošača i njihovih osobnih podataka. Svijet se mijenja, tehnologija napreduje, standarde diktiraju veliki igrači, a mali ljudi prisiljeni su pratiti trendove jer bez tehnologije ne mogu opstati. Da smo ovisni o tehnologiji pokazalo se za vrijeme pandemije koronavirusa Covid-19. Bez mobilnog uređaja, računala, tableta djeca nisu mogla pratiti školsku nastavu, ali ni većina ljudi raditi od kuće. Neke kompanije su čak opstale okrećući se digitalizaciji i Internetu stvari. Prisiljeni su koristiti tehnologiju, htjeli to ljudi ili ne, od najranije dobi do najstarije životne dobi. S obzirom da se trendovi ne mogu zaustaviti, itekako se može utjecati na njihovo limitiranje za što su zadužena standardizacijska i pravna tijela, ali i način korištenja tehnologije za što je zadužen svaki potrošač ponaosob. Kroz rad je pokazano kako potrošači imaju veliki utjecaj na to, hoće li i koji će podaci o njima biti prikupljeni. Ne mogu utjecati na sve ali mogu dijeliti minimalno sadržaja privatnih podataka, paziti na kompleksnosti korisničkog imena i zaporke i načina na koji ih dijele, paziti na redovna ažuriranja i sigurnosne zakrpe pa sve do sigurnosnih certifikata i certificiranih uređaja. Naravno, to ne znači da se podaci o njima neće i dalje prikupljati, no posljedice se mogu znatno ublažiti. Katalozi trgovina sve više sadrže niskobudžetne i proizvode u principu nedovoljno zaštićene, koji olakšavaju svakodnevne životne aktivnosti poput videokamera, robotskih usisavača, pametnih termostata, žarulja i drugih koji marketinškim trikovima i povoljnim cijenama zadobiju pažnju kupaca koji su nesvjesni ranjivosti takvih uređaja i rizika i donose takav uređaj u svoj dom. Zato je prije svega potrebno dobro sagledati tehnologiju, raspitati se i educirati se o istoj. Pokazalo se kako velika količina potrošača nema veliko tehnološko znanje ali unatoč tome koristi tehnologiju, jer u konačnici tehnologija je uvijek trend. No međutim, kako je trend za potrošače, tako je trend i za hakere koji postaju sve inovativniji, maštovitiji i sofisticiraniji. Krađa podataka, ugrožavanje privatnosti, postajanjem dijelom statistike, posljedice su koje korisnike ne brinu u velikoj mjeri kao što je pokazano kroz anketu s obzirom na prednosti koje IoT donosi. Zvuči pomalo bezazleno, ali ljudi nisu svjesni da se iza takvih bezazlenih pojmova mogu skrivati akcije poput krađe sredstava s bankovnih kartica, krađe identiteta i pripisivanje zločina, otmice, ucjene i različite vrste kriminalnih radnji i kršenja zakona. Stoga bi se potrošači trebali probuditi i trebali bi postati svjesni vremena u kojem živimo. IT kompanije i tijela zadužena za sigurnost trebali bi u sve većim mjerama educirati ljude koji sve više posežu za tehnologijom da ih osvijeste za istu, da ih nauče njihovoj primarnoj zaštiti, a zatim i zaštiti svog IoT okruženja. Tvrtke koje ugrađuju pametne uređaje u domaćinstva, trebale bi tražiti dozvolu od potrošača za isto, jednako kao i svi ostali uređaji koji prikupljaju podatke o korisnicima bez njihovog znanja i dozvole, no to je opet problem zakonodavnih i državnih tijela. Zato, ljudi bi se trebali fokusirati na one stvari koje oni mogu promijeniti i početi od sebe i svog ponašanja u digitaliziranom svijetu, jer u konačnici ne treba se bojati tehnologije, već onih koji stoje iza nje i koji je koriste kao alat za infiltraciju u tuđe živote i iz tog razloga treba je tretirati kao neznanca koji je odjednom došao u naš dom i postao dio našeg života.

LITERATURA

[1] Foote K.D. A brief history of the Internet of Things. Dataversity. 2022. Preuzeto s: https://www.dataversity.net/brief-history-internet-things/# [Pristupljeno: 27. ožujak 2022.]

[2] IoT ili Internet stvari. Ofir. 2019. Preuzeto s: https://www.ofir.hr/iot-ili-internet-stvari-2 [Pristupljeno: lipanj 2020.]

[3] Ashton K. That 'Internet of Things' Thing RFID Journal. 2009 Preuzeto s: http://www.rfidjournal.com/articles/view?4986 [Pristupljeno: lipanj 2020.]

[4] Žagar M., Mišura K. Open info trend. Internet stvari i srodna područja. Preuzeto s: http://www.infotrend.hr/clanak/2015/4/nevidljivi-internet,83,1144.html [Pristupljeno: 27. ožujak 2022.]

[5] Kušek M. Inovacije u području Interneta Stvari [prezentacija] Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu 2016.

[6] Gelo D. Internet of Things (IoT) - Izazovi i mogućnosti cyber sigurnosti povezane s IoT-om. Diplomski rad. Zagreb, Visoko učilište Algebra; 2019. Preuzeto s: https://zir.nsk.hr/en/islandora/object/algebra%3A428/datastream/PDF/view [Pristupljeno: 27. ožujak 2022.]

[7] IoT Practitioner, aligning IoT with industry. The Good, the Bad, and the Inevitable About Industrial Revolution. 2019.Preuzeto s: https://iotpractitioner.com/the-good-the-bad-and-the-inevitable-about-industrial-revolution/ [Pristupljeno: 27. ožujak 2020.]

[8] Sharma N.,Shamkuwar M., Singh I. *Internet of Things and Big Data Analytics for Smart Generation* 2018. pp 27-51. Preuzeto s: https://link.springer.com/chapter/10.1007/978-3-030-04203-5_3 [Pristupljeno: 27. ožujak 2022.]

[9] Wikipedia, the free encyclopedia. Fourth Industrial Revolution. Preuzeto s: https://en.wikipedia.org/wiki/Fourth_Industrial_Revolution. [Pristupljeno: lipanj 2020.]

[10] Statista Research Department. Internet of Things - number of connected devices worldwide 2015-2025. 2016. Preuzeto s: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ [Pristupljeno: 27. ožujak 2022.]

[11] Gills A.S. What is the internet of things (IoT)? TechTarget IoTAgenda. 2022. Preuzeto s: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT#:~:text=The%20internet%20of%20things%2C%20or,human%2Dto%2Dcomputer%20interaction. [Pristupljeno: 27. ožujak 2022]

[12] Quic Solv. How IoT works with real Life IoT Examples. Preuzeto s: https://www.quicsolv.com/internet-of-things/how-iot-works/ [Pristupljeno: 27. ožujak 2022.]

[13] Što je stroj za stroj (m2m)? - definicija iz tehopedije - Hardver - 2022. Preuzeto s: https://hr.theastrologypage.com/machine-machine [Pristupljeno: 27. ožujak 2022.]

[14] CARNet. RFID identifikacija. CCERT-PUBDOC-2007-01-179. Revizija v1.1. 2007. Preuzeto s :https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-01-179.pdf [Pristupljeno: 28. ožujak 2022.]

[15] Tech Vidvan. How IoT works? Preuzeto s: https://techvidvan.com/tutorials/how-iot-works/ [Pristupljeno: 27. ožujak 2022.]

[16] IEEE Standards association. IEEE 802.15.4-2020. IEEE Standard for Low-Rate Wireless Networks. 2017. Preuzeto s: https://standards.ieee.org/ieee/802.15.4/7029/ [Pristupljeno: 2. travanj 2022.]

[17] Pahwa V. 5 reasons Zigbee is ideal for smart homes. einfochips. The solutions people. Preuzeto s: https://www.einfochips.com/blog/5-reasons-zigbee-is-ideal-for-smart-homes/ [Pristupljeno: 2. travanj 2022.]

[18] Što je Zigbee i koji su uređaji kompatibilni? Preuzeto s: https://hr.your-best-home.net/7344671-what-is-zigbee-and-which-devices-are-compatible [Pristupljeno: 2. travanj 2022.]

[19] Rosencrance L. Zigbee. Techtarget. IoT Agenda. Preuzeto s: https://www.techtarget.com/iotagenda/definition/ZigBee [Pristupljeno: 2. travanj 2022.]

[20] Homey. What is Zigbee? Explaining the World's Most Popular Smart Light Network Technology. Preuzeto s: https://homey.app/en-au/wiki/what-is-zigbee/ [Pristupljeno: 2. travanj 2022.]

[21] RF Page. What are tha major components of Intenet of things. 2021. Preuzeto s: https://www.rfpage.com/what-are-the-major-components-of-internet-of-things/ [Pristupljeno: 28. ožujak 2022.]

[22] RedHat. What is REST API? 2020. Preuzeto s: https://www.redhat.com/en/topics/api/what-is-a-rest-api#:~:text=choose%20Red%20Hat%3F-,Overview,by%20computer%20scientist%20Roy%20Fielding. [Pristupljeno: 28. ožujak 2022.]

[23] Embitel. How IoT works - an overview of the technology architecture. Preuzeto s: https://www.embitel.com/blog/embedded-blog/how-iot-works-an-overview-of-the-technology-architecture-2 [Pristupljeno: 28. ožujak 2022.]

[24] Data Flair. How IoT works - 4 main components of iot system. Preuzeto s: https://data-flair.training/blogs/how-iot-works/ [Pristupljeno: 28. ožujak 2022.]

[25] Researchgate. The Internet of Things (IoT) Reference Model. Preuzeto s: https://www.researchgate.net/figure/The-Internet-of-Things-IoT-Reference-Model_fig3_331280965 [Pristupljeno: 28. ožujak 2022.]

[26]ISO/IEC 30141:2018(en) Internet of Things (loT) — Reference Architecture Preuzeto s: https://www.iso.org/obp/ui/#iso:std:iso-iec:30141:ed-1:v1:en [Pristupljeno: 2. travanj 2022]

[27] IOTa. An introduction to iot architectures. Preuzeto s: https://iotac.eu/an-introduction-to-iot-architectures/ [Pristupljeno: 28. ožujak 2022.]

[28] ResearchGate. Architecture of an IoT platform. Preuzeto s: https://www.researchgate.net/figure/Architecture-of-an-IoT-platform-Source-ISO-IEC-301412018_fig1_338280045 [Pristupljeno: 28. ožujak 2022.]

[29] Forcepoint. What is the OSI model? The OSI model defined, explained and explored. Preuzeto s: https://www.forcepoint.com/cyber-edu/osi-model#:~:text=The%20OSI%20Model%20(Open%20Systems,between%20different%20products%20and%20software. [Pristupljeno: 28. ožujak 2022.]

[30] ISO/IEC JTC 1/SC 41 Internet of things and digital twin Preuzeto s: https://www.iso.org/committee/6483279.html [Pristupljeno: 2. travanj 2022]

[31] IEC. *IoT 2020: Smart and secure IoT platform.* Whitepaper. Preuzeto s: https://storage-iecwebsite-prd-iec-ch.s3.eu-west-1.amazonaws.com/2019-09/content/media/files/iec_wp_iot_2020_en.pdf [Pristupljeno: 28. ožujak 2022.]

[32] IEC 62264-1:2013 Preuzeto s: https://www.iso.org/standard/57308.html [Pristupljeno: 2. travanj 2022]

[33] IEC 62890:2020 Preuzeto s: https://webstore.iec.ch/publication/30583 [Pristupljeno: 2.travanj 2022]

[34] IEC Webstore. IEC 62264-6:2020. Preuzeto s: https://webstore.iec.ch/publication/59706 [Pristupljeno: 1. travanj 2022.]

[35] IoT-A Deliverable D1.3 - Updated reference model for IoT v1.5 2012. Preuzeto s: https://cocoa.ethz.ch/downloads/2014/01/1524_D1.3_Architectural_Reference_Model_update.pdf [Pristupljeno: 1. travanj 2022.]

[36] IEC Webstore. IEC 62890:2020. Preuzeto s: https://webstore.iec.ch/publication/30583 [Pristupljeno: 1. travanj 2022.]

[37] Patel K.K., Patel S.M. *Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges.* Department of Electrical Engineering Faculty of Technology and Engineering-MSU, Vadodara, Gujarat, India. Preuzeto s: http://www.opjstamnar.com/download/Worksheet/Day-110/IP-XI.pdf [Pristupljeno: 1. travanj 2022.]

[38] i-scoop. What is IoT? The Internet of Things defined and explained Preuzeto s: https://www.i-scoop.eu/internet-of-things-iot/internet-of-things-what-definition/ [Pristupljeno: 3. travanj 2022.]

[39] IoT Analytics. *IoT Use Case Adoption Report 2021*. Preuzeto s: https://iot-analytics.com/product/iot-use-case-adoption-report-2021-2/ [Pristupljeno: 3. travanj 2022.]

[40] IoT Analytics. *Top 10 use case.* Preuzeto s: https://iot-analytics.com/top-10-iot-use-cases/ [Pristupljeno: 3. travanj 2022.]

[41] PlantConnect. Condition Monitoring of bottling lines. Preuzeto s: https://aiplindia.com/casestudy/Condition-Monitoring-of-bottling-lines/ [Pristupljeno: 3. travanj 2022.]

[42] Lindsay. Grower Insights with Adam McVeigh. Preuzeto s: https://www.lindsay.com/usca/en/resource/grower-insights-adam-mcveigh/ [Pristupljeno: 3. travanj 2022.]

[43] Advantech. Advantech LTE Routers: Helping Deliver an Efficient, Dynamic Application of Oilfield Fluids Preuzeto s: https://www.advantech.com/resources/case-study/advantech-lte-routers-helping-deliver-an-efficient-dynamic-application-of-oilfield-fluids [Pristupljeno: 3. travanj 2022.]

[44] Bosch. Lineas: Digitalizing rail transport Preuzeto s: https://bosch.io/customers/logistics/digitalizing-rail-transport/ [Pristupljeno: 3. travanj 2022.]

[45] Greyp G6: Rimac predstavio prvi pametni električni bicikl ove vrste na svijetu. Novilist. Preuzeto s: https://www.novilist.hr/ostalo/sci-tech/tehnologija/greyp-g6-rimac-predstavio-prvi-pametni-elektricni-bicikl-ove-vrste-na-svijetu/?meta_refresh=true [Pristupljeno: 3. travanj 2022.]

[46] Cognizant. Early detection of defects is driving force behind better safety. Preuzeto s: https://www.cognizant.com/us/en/case-studies/hardware-in-loop-auto-safety [Pristupljeno: 3. travanj 2022.]

[47] Chung G., Derajtys J. Breakout session: Connected supply chain. DHL Global Energy Conference 2018, Houston Preuzeto s: https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-breakout-on-connected-supply-chains-gina-chung-and-joe-derajtys.pdf [Pristupljeno: 3. travanj 2022.]

[48] Pruitt W. Getting Smarter about ‘Machine Health’ to Improve Supply Chain Reliability. Linkedin. Preuzeto s: https://www.linkedin.com/pulse/getting-smarter-machine-health-improve-supply-chain-warren-pruitt/ [Pristupljeno: 3. travanj 2022.]

[49] Salih K.O.M., Rashid T.A., Radovanovic D., Bacanin N. A Comprehensive Survey on the Internet of Things with the Industrial Marketplace. *Sensors. MDPI.* Preuzeto s: https://www.mdpi.com/1424-8220/22/3/730 [Pristupljeno: 5. Travanj 2022.]

[50] Digwatch. Internet of things. Preuzeto s: https://dig.watch/topics/internet-of-things-iot [Pristupljeno: 5. travanj 2022.]

[51] IoT Analytics. New Report Indicates Worldwide IoT Security Market To Become A US$4.4 Billion Opportunity By 2022. Preuzeto s: https://iot-analytics.com/new-iot-security-report/ [Pristupljeno: 5. travanj 2022.]

[52] IoT Analytics. MWC Barcelona 2022 review: 5G, AI, and Security the most discussed technology topics. Preuzeto s: https://iot-analytics.com/mwc-barcelona-2022-review/ [Pristupljeno: 5 travanj 2022.]

[53] Norton. Privacy vs. security: What’s the difference? Preuzeto s: https://us.norton.com/internetsecurity-privacy-privacy-vs-security-whats-the-difference.html#:~:text=Privacy%20and%20security%20are%20related,your%20personal%20information%20is%20protected. [Pristupljeno: 5 travanj 2022.]

[54] Internet Society. The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things. Preuzeto s: https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/ [Pristupljeno: 5 travanj 2022.]

[55] Intellias. Focus on Risks: Trends That Will Define IoT Security in 2020. Preuzeto s: https://intellias.com/focus-on-risks-trends-that-will-define-iot-security-in-2020/ Preuzeto s: [Pristupljeno: 9. travanj 2022.]

[56] Lastine. Security for the Internet of things. Preuzeto s: https://www.lastline.com/use-cases/your-challenge/protect-the-internet-of-things/ [Pristupljeno: 5. travanj 2022.]

[57] PrattJason M.K., Sparapani J. What is digital transformation? *TechTarget*. Preuzeto s: https://www.techtarget.com/searchcio/definition/digital-transformation. [Pristupljeno: 9. travanj 2022.]

[58] Shea S., Wigmore I. IoT security (internet of things security). *Techtarget*. Preuzeto s: https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security [Pristupljeno: 9. travanj 2022.]

[59] Scroxton A. Belgian security researcher hacks Tesla with Raspberry Pi. *ComputerWeekly.com.* Preuzeto s: https://www.computerweekly.com/news/252492564/Belgian-security-researcher-hacks-Tesla-with-Raspberry-Pi?_gl=1*1fnmzsg*_ga*MTcwNjQ2Mjk4Mi4xNjQ1OTE3NDI2*_ga_TQKE4GS5P9*MTY

0OTUzMTg3MC4yNy4xLjE2NDk1MzU3ODQuMA..&_ga=2.83708310.1660109558.1649529642-1706462982.1645917426 [Pristupljeno: 9. travanj 2022.]

[60] Atlam H.F., Alenezi A., Alassafi M.O., Alshdadi A.A. Security, Cybercrime and Digital Forensics for IoT. *Researchgate*. January 2020. Intelligent Systems Reference Library. In book: Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm (pp.551-577) Preuzeto s: [Pristupljeno: 9. travanj 2022.]

[60] Aydos M., Vural Y., Tekerek A. Assessing risks and threats with layered approach to Internet of Things security. Measurement and Control. 1-6. 2019. Preuzeto s: https://www.researchgate.net/publication/332392350_Assessing_risks_and_threats_with_layered_approach_to_Internet_of_Things_security [Pristupljeno: 10. travanj 2022.]

[61] L.D.Xu, W.He., S.Li. Internet of things in industries. A survey. *IEEE Trans. Ind. Informat*., vol 10, no. 4, pp. 2233-2243, Nov 2014.

[62] M.Farooq, M.Waseem, A.Khairi, S.Mazhar. A critical analysis on the security concerns of Internet of things (IoT*). Int. J. Computer Application*, vol. 111, no. 7, pp. 1-6, 2015.

[63] Sikdar A.K., Petracca G., Aksu H., Jager T., Ulugac A.S. A survey on sensors-based threats to IoT devices and applications. Feb 2018., ArXiv:1802.02041.

[64] Miraz M.H., Ali M., Excell P.S., Picking R. A review on Internet of things(IoT), Internet od everything(IoE) and Internet of nano things(IoNT). Sept 2015. Internet technologies and applications (ITA)

[65] Bitdefender. Security. Vulnerabilities Identified in Wyze Cam IoT Device. Whitepaper. Preuzeto s: https://www.bitdefender.com/files/News/CaseStudies/study/413/Bitdefender-PR-Whitepaper-WCam-creat5991-en-EN.pdf [Pristupljeno: 10. travanj 2022.]

[66] Greig J. Three vulnerabilities found in Wyze Cam devices allow for outside access. *The Record.* 2022. Preuzeto s: https://therecord.media/three-vulnerabilities-found-in-wyze-cam-devices-allow-for-outside-access/ [Pristupljeno: 10. travanj 2022.]

[67] Henriquez M. Serious security vulnerabilities found in Wyze Cam devices. *Security*. Preuzeto s: https://www.securitymagazine.com/articles/97331-serious-security-vulnerabilities-found-in-wyze-cam-devices [Pristupljeno: 10. travanj 2022.]

[68] CVE-2019-9564. Preuzeto s: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9564#:~:text=A%20vulnerability%20in%20the%20authentication,v2%20versions%20prior%20to%204.49. [Pristupljeno: 10. travanj 2022.]

[69] CVE-2019-12266. Preuzeto s: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12266#:~:text=Stack%2Dbased%20Buffer%20Overflow%20vulnerability,1.47. [Pristupljeno: 10. travanj 2022.]

[70] Stone B. Nokia: Botnet DDoS attacks are on the rise. *TechRepublic*. 2022. Preuzeto s: https://www.techrepublic.com/article/nokia-botnet-ddos-attacks-are-on-the-rise/ [Pristupljeno: 10. travanj 2022.]

[71] Nokia. Nokia Deepfield Network intelligence Report DDoS in 2021. Prezeto s: https://onestore.nokia.com/asset/211059?_ga=2.117247750.1008124375.1649589078-475976518.1649589078 [Pristupljeno: 10. travanj 2022.]

[72] Laovitz C. The rise of botnet DDoS. 2022. Preuzeto s: https://www.nokia.com/blog/the-rise-of-botnet-ddos/ [Pristupljeno: 10. travanj 2022.]

[73] Default Passwords: The Biggest Weakness in IoT Security. *phtek*. 2018. Preuzeto s: https://ophtek.com/default-passwords-biggest-weakness-iot-security/ [Pristupljeno: 10. travanj 2022.]

[74] Darkhound. Fancy Bear Exploiting IOT devices with weak passwords. Preuzeto s: https://www.darkhoundsecurity.com/fancy-bear-exploiting-iot-devices-with-weak-passwords/ [Pristupljeno: 10. travanj 2022.]

[75] Montalbano E. Hacker Leaks More Than 500K Telnet Credentials for IoT Devices. *Threatpost*. 2021. Preuzeto s:https://threatpost.com/hacker-leaks-more-than-500k-telnet-credentials-for-iot-devices/152015/ [Pristupljeno: 10. travanj 2022.]

[76] Frustaci M., Pace P. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE INTERNET OF THINGS JOURNAL*, VOL. 5, NO. 4, AUGUST 2018, pp. 2483-2495.

[77] Rizvi S., Pfeffer J., Kurtz A., Rizvi M. Securing the Internet of Things(IoT): A Security Taxonomy for IoT. 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference On Big Data Science and Engineering, 2018, pp 163-168.

[78] Sajjad H., Arshad M.J. Evaluating Security Threats for each Layers of IoT System. *Researchgate*. 2019. Preuzeto s: https://www.researchgate.net/publication/336149742_Evaluating_Security_Threats_for_each_Layers_of_IoT_System [Pristupljeno: 14. travanj 2022.]

[79] IEEE 802.11-2020. Preuzeto s: https://standards.ieee.org/ieee/802.11/7028/ [Pristupljeno: 14. travanj 2022.]

[80] Mohammadnia H., Slimane S.B. IoT-NETZ: Practical Spoofing Attack Mitigation Approach in SDWN Network. *2020 Seventh International Conference on Software Defined Systems (SDS)*, 2020, pp. 5-13, doi: 10.1109/SDS49854.2020.9143903.

[81] Nakutavicite J. Hacker terrorizes family by hijacking baby monitor. NordVPN. Preuzeto s: https://nordvpn.com/blog/baby-monitor-iot-hacking/ [Pristupljeno: 14. travanj 2022.]

[82] Whatismyipaddress. What Makes a Network Unsecure? Preuzeto s: https://whatismyipaddress.com/unsecured-network-2 [Pristupljeno: 14. travanj 2022.]

[83] IPCisco. Wireless security protocols. Preuzeto s: https://ipcisco.com/lesson/wireless-security-protocols/ [Pristupljeno: 14. travanj 2022.]

[84] How we ended up in WPA3? – Wi-Fi security evolution. *Grandmetric*.2018. Preuzeto s: https://www.grandmetric.com/2018/07/06/ended-wpa3-wi-fi-security-evolution/ [Pristupljeno: 14. travanj 2022.]

[85] Wi-Fi Alliance. Who we are. Preuzeto s: https://www.wi-fi.org/who-we-are [Pristupljeno: 14. travanj 2022.]

[86] WPA2 KRACK Attack: The WiFi Hack and What it Means. auth0.Preuzeto s: https://auth0.com/blog/krack-attack-wpa2-and-what-it-means/ [Pristupljeno: 14. travanj 2022.]

[87] Key Reinstallation Attacks. Breaking WPA2 by forcing nonce reuse. Preuzeto s: https://www.krackattacks.com/ [Pristupljeno: 14. travanj 2022.]

[88] Wpa2 vs. Wpa3. Diffen. Preuzeto s: https://www.diffen.com/difference/WPA2_vs_WPA3 [Pristupljeno: 14. travanj 2022.]

[89] Edwards B. What's the Best Wi-Fi Encryption to Use in 2022? *How to geek.* 2022. Preuzeto s: https://www.howtogeek.com/782993/whats-the-best-wi-fi-encryption-to-use-in-2022/ [Pristupljeno: 14. travanj 2022.]

[90] Burkhalter M. Researchers find new IoT security risk: Bluetooth spoofing. Perle. 2022. Preuzeto s: https://www.perle.com/articles/researchers-find-new-iot-security-risk-bluetooth-spoofing-40189953.shtml [Pristupljeno: 14. travanj 2022.]

[91] Wazid M., Kumar D.A., Rodrigues J.J.P.C., Shetty S., Parks Y. IoMT Malware Detection Approaches: Analysis and Research Challenges. IEEE Access. 2019. Preuzeto s: https://www.researchgate.net/publication/338000202_IoMT_Malware_Detection_Approaches_Analysis_and_Research_Challenges [Pristupljeno: 14. travanj 2022.]

[92] Dunlap T. The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History. *IoT forall.* 2020. Preuzeto s: https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities [Pristupljeno: 15. travanj 2022.]

[93] New Linux Worm Attacks IoT Devices. *Informa. Dark reading.* Preuzeto s: https://www.darkreading.com/iot/new-linux-worm-attacks-iot-devices [Pristupljeno: 15. travanj 2022.]

[94] Brown A. Top cyber attacks on IoT devices in 2021. Firedome. Preuzeto s: https://firedome.io/blog/top-cyber-attacks-on-iot-devices-in-2021/ [Pristupljeno: 15. travanj 2022.]

[95] Školnik M. Minimize Loss of Sales - Based on Verkada Breach. Firedome. 2021. Preuzeto s: https://firedome.io/blog/cyber-breach-recovery-plan-based-on-verkada-breach/ [Pristupljeno: 15. travanj 2022.]

[96] Shaked I. Western Digital: Where Things Went Wrong & 3 Steps for Product Managers to Remedy. Firedome. 2021. Preuzeto s: https://firedome.io/blog/western-digital-where-things-went-wrong-3-steps-for-product-managers-to-remedy/ [Pristupljeno: 15. travanj 2022.]

[97] Leuth K.L. The impact of Covid-19 on the Internet of Things – now and beyond the Great Lockdown: Part 1. IoT Analytics. Preuzeto s: https://iot-analytics.com/the-impact-of-covid-19-on-the-internet-of-things/ [Pristupljeno: 16. travanj 2022.]

[98] Use of Onsight Remote Expertise is up 745% in Most Impacted Regions. Liberstream. 2020. Preuzeto s: https://librestream.com/blog/onsight-usage-up-745-percent/ [Pristupljeno: 16. travanj 2022.]

[99] XAG introduces drone disinfection operation to fight the coronavirus outbreak. *Health Europa.* 2020. Preuzeto s: https://www.healtheuropa.com/xag-introduces-drone-disinfection-operation-to-fight-the-coronavirus-outbreak/97265/ [Pristupljeno: 16. travanj 2022.]

[100] Millard N. How South Korea's smart city startups curbed the spread of COVID-19. e27. 2020. Preuzeto s: https://e27.co/how-south-koreas-smart-city-startups-curbed-the-spread-of-covid-19-20200323/ [Pristupljeno: 16. travanj 2022.]

[101] Wray S. Boston launches Covid-19 data dashboards for residents. SmartCitiesWorld. 2020. Preuzeto s: https://www.smartcitiesworld.net/news/news/boston-launches-covid-19-data-dashboards-for-residents-5161 [Pristupljeno: 16. travanj 2022.]

[102] Kinsa HealthWeather. Preuzeto s: https://healthweather.us/ [Pristupljeno: 16. travanj 2022.]

[103] Livongo Announces Preliminary First Quarter 2020 Revenue; Exceeds Previously Announced Guidance. Livongo. 2020. Preuzeto s: https://www.globenewswire.com/news-release/2020/04/07/2012804/0/en/Livongo-Announces-Preliminary-First-Quarter-2020-Revenue-Exceeds-Previously-Announced-Guidance.html [Pristupljeno: 16. travanj 2022.]

[104] Check Point. A Perfect Storm: the Security Challenges of Coronavirus Threats and Mass Remote Working. Preuzeto s: https://blog.checkpoint.com/2020/04/07/a-perfect-storm-the-security-challenges-of-coronavirus-threats-and-mass-remote-working/ [Pristupljeno: 15. travanj 2022.]

[105] Nicols S. Bad news: Cognizant hit by ransomware gang. Worse: It's Maze, which leaks victims' data online after non-payment. *The register*. 2020. Preuzeto s: https://www.theregister.com/2020/04/21/cognizant_maze_malware/ [Pristupljeno: 15. travanj 2022.]

[106] Leuth K.L. The impact of Covid-19 on the Internet of Things – now and beyond the Great Lockdown: Part 2. IoT Analytics. Preuzeto s: https://iot-analytics.com/the-impact-of-covid-19-on-the-internet-of-things-part-2/ [Pristupljeno: 16. travanj 2022.]

[107] Accent Systems. Preuzeto s: https://accent-systems.com/accent-systems-developed-connected-wristband-technology-contain-covid19/ [Pristupljeno: 15. travanj 2022.]

[108] Ross C. After 9/11, we gave up privacy for security. Will we make the same trade-off after Covid-19? *STAT*. 2020. Preuzeto s: https://www.statnews.com/2020/04/08/coronavirus-will-we-give-up-privacy-for-security/ [Pristupljeno: 15. travanj 2022.]

[109] Wagenseil P. Zoom security issues: What's gone wrong and what's been fixed. Tom's guide. 2020. Preuzeto s: https://www.tomsguide.com/news/zoom-security-privacy-woes [Pristupljeno: 16. travanj 2022.]

[110] Brodie D. The Necessity of Healthcare IoT Security in an Interconnected World. Geektime. 2022. Preuzeto s: https://www.geektime.com/the-necessity-of-healthcare-iot-security-in-an-interconnected-world/ [Pristupljeno: 15. travanj 2022.]

[111] Tercatin R.,Jaffe-Hoffman M. 72% increase in cyberattacks against healthcare sector over the weekend. The Jerusalem post. 2021. Preuzeto s: https://www.jpost.com/breaking-news/cyberattack-attempts-towards-israeli-hospitals-thwarted-govt-682221 [Pristupljeno: 15. travanj 2022.]

[112] Wigmore I. IoT security (internet of things security). TechTarget.IotAgenda. Preuzeto s: https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security [Pristupljeno: 17. travanj 2022.]

[113] Korda Z. HEP-ova pametna brojila donose brojne koristi, ali kriju i skupe zamke. tportal.hr. 2018. Preuzeto s: [Pristupljeno: 17. travanj 2022.]

[114] Vojković G., Milenković M. IoT Devices and the Need to Inform Utility Users of Collecting, Controlling and Processing of Personal Data

Hrvatska. 2020. Preuzeto s: https://www.bib.irb.hr/1082931 [Pristupljeno: 17. travanj 2022.]

[115] Xiaomi Iot privacy white paper. 2021. Preuzeto s: https://trust.mi.com/pdf/Xiaomi__IoT_Privacy_White_Paper_EN_June_2021.pdf [Pristupljeno: 17. travanj 2022.]

[116] Xiaomi laid out proposed global standards for IoT security. FutureIOT. 2022. Preuzeto s: https://futureiot.tech/xiaomi-laid-out-proposed-global-standards-for-iot-security/ [Pristupljeno: 17. travanj 2022.]

[117] Cipher. A Quick NIST Cybersecurity Framework Summary. Preuzeto s: https://cipher.com/blog/a-quick-nist-cybersecurity-framework-summary/ [Pristupljeno: 17. travanj 2022.]

[118] Scully P. Understanding IoT Security – Part 1 of 3: IoT Security Architecture on the Device and Communication Layers. IoT analytics. 2016. Preuzeto s: https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/ [Pristupljeno: 17. travanj 2022.]

[119] Scully P. Understanding IoT Security – Part 2 of 3: IoT Cyber Security for Cloud and Lifecycle Management. IoT analytics. 2017. Preuzeto s: https://iot-analytics.com/understanding-iot-cyber-security-part-2/ [Pristupljeno: 17. travanj 2022.]

[120] Basatwar G. Guide To OWASP IoT Top 10 For Proactive Security. appsealing. 2021. Preuzeto s: https://www.appsealing.com/owasp-iot-top-10/ [Pristupljeno: 17. travanj 2022.]

[121] Rykov M. 5 IoT Security best practices to consider after the Covid-19 lockdown. IoT Analytics. 2020. Preuzeto s: https://iot-analytics.com/5-iot-security-best-practices-after-the-covid-19-lockdown/ [Pristupljeno: 17. travanj 2022.]

[122] Businesswire. Zscaler Annual IoT Report Identifies Shift in Shadow IoT Behavior Threatening Enterprise Security PosturePreuzeto s: https://www.businesswire.com/news/home/20200225005401/en/Zscaler-Annual-IoT-Report-Identifies-Shift-Shadow [Pristupljeno: 17. travanj 2022.]

[123] Oswal A. Cisco AI Network Analytics: Making Networks Smarter and Simpler to Manage. Cisco. 2019. Preuzeto s: [Pristupljeno: 17. travanj 2022.]

[124] Kukec T. Najveća hrvatska cyber stručnjakinja upozorava: Neke pametne uređaje koji su na tržištu EU nikad nije smjela dozvoliti, mogu ugroziti i ljudski život. *Jutarnji list.* 2018. Preuzeto s: https://100posto.jutarnji.hr/news/tehnoloski-divovi-ne-drze-se-pravila-o-zastiti-osobnih-podataka-a-u-eu-se-prodaju-uredaji-koji-nikada-ne-bi-smjeli-biti-na-trzistu [Pristupljeno: lipanj 2020.]

[125] CNET autori. California governor signs country's first IoT security law. *CNET NEWS.* 2018. Preuzeto s: https://www.cnet.com/news/politics/california-governor-signs-countrys-first-iot-security-law/ [Pristupljeno: lipanj, 2020.]

[126] Zervaki M. *Regulating the IoT: 2020 and beyond 2020*. 16.06.2020. Preuzeto s: https://www.accesspartnership.com/regulating-the-iot/ [Pristupljeno: 20. ožujka 2022.]

[127] The white house. About the white house. Our government. The U.S. Federal Government is composed of three distinct branches. Preuzeto s: https://www.whitehouse.gov/about-the-white-house/our-government/ [Pristupljeno: 26. ožujak 2022.]

[128] Sjedinjene Američke Države. *Hrvatska enciklopedija, mrežno izdanje.* Leksikografski zavod Miroslav Krleža, 2021. Preuzeto s: http://www.enciklopedija.hr/Natuknica.aspx?ID=56303 [Pristupljeno 26. ožujak 2022.]

[129] California Legisltive Information. CIVIL CODE - CIV. DIVISION 3. OBLIGATIONS [1427 - 3273.16] (Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14.) PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS [1738 - 3273.16] (Part 4 enacted 1872.). TITLE 1.81.26. *Security of Connected Devices* [1798.91.04 - 1798.91.06] (Title 1.81.26 added by Stats. 2018, Ch. 860, Sec. 1.) Preuzeto s: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.26.&part=4.&chapter=&article= [Pristupljeno: 2.4.2022.]

[130] California Legisltive Information . CIVIL CODE - CIV. DIVISION 3. OBLIGATIONS [1427 - 3273.16] (Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14.) PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS [1738 - 3273.16] (Part 4 enacted 1872.) TITLE 1.81.5. *California Consumer Privacy Act of 2018* [1798.100 - 1798.199.100] (Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.) Preuzeto s: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 [Pristupljeno: 2.4.2022.]

[131] Gloss K. Navigate IoT regulations at local and global levels TechTarget IoTAgenda 2021. Preuzeto s: https://internetofthingsagenda.techtarget.com/feature/Navigate-IoT-regulations-at-local-and-global-levels [Pristupljeno: 20. ožujak 2022.]

[132] Govinfo. Public Law 116-207 134 STAT. 1001 - *Internet of Things Cybersecurity Improvement Act of 2020'' or the ``IoT Cybersecurity Improvement Act of 2020.* Preuzeto s: https://www.govinfo.gov/content/pkg/PLAW-116publ207/pdf/PLAW-116publ207.pdf [Pristupljeno: 2.4.2022.]

[133] NIST. Draft NISTIR 8259D. *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government* Preuzeto s: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259D-draft.pdf [Pristupljeno: 2.4.2022.]

[134] NIST. NISTIR 8259 series. NISTIR 8259A: *Core Device Cybersecurity Capability Baseline* (May 29, 2020) Preuzeto s: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf [Pristupljeno: 2.4.2022.]

[135] govinfo. S. 965 (Introduced in Senate) - *Cyber Shield Act of 2021* Preuzeto s: https://www.govinfo.gov/content/pkg/BILLS-117s965is/pdf/BILLS-117s965is.pdf [Pristupljeno: 2.4.2022.]

[136] govinfo. S. 2020 (Introduced in Senate) - *Cyber Shield Act of 2017* Preuzeto s: https://www.govinfo.gov/content/pkg/BILLS-115s2020is/pdf/BILLS-115s2020is.pdf [Pristupljeno: 2.4.2022.]

[137] govinfo. H.R. 4792 (Introduced in House) - *Cyber Shield Act of 2019* Preuzeto s: https://www.govinfo.gov/content/pkg/BILLS-116hr4792ih/pdf/BILLS-116hr4792ih.pdf [Pristupljeno: 2.4.2022.]

[138] McMurrough M., Ponder J., Oksasoglu J. Cyber Shield Act Calling for IoT Device Certification Reintroduced in Congress. 2021. Preuzeto s:

https://www.insideprivacy.com/cybersecurity-2/cyber-shield-act-calling-for-iot-device-certification-reintroduced-in-congress/ [Pristupljeno: 20. ožujak 2022.]

[139] ISO/IEC JTC1 SC27 WG4 (2021). ISO/IEC 27402*: Cybersecurity – IoT Security and Privacy – Device Baseline Requirements* (2nd committee draft). U izradi.

[140] Biden's executive order on cybersecurity: a good beginning. PWC. Preuzeto s: https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/bidens-executive-order-cybersecurity.html [Pristupljeno: 25. ožujak 2022.]

[141] The white house. Statement by Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger on SolarWinds and Microsoft Exchange Incidents Preuzeto s: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/19/statement-by-deputy-national-security-advisor-for-cyber-and-emerging-technology-on-solarwinds-and-microsoft-exchange-incidents/ [Pristupljeno: 25. ožujak 2022.]

[142] NIST Special Publication 800-213A. *IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog* Preuzeto s: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213A.pdf [Pristupljeno: 2.4.2022.]

[143] European Commission, i2010, a European information society for growth and employment communication from the Commission to the Council, the European parliament, *the European Economic and Social Committee and the Committee of the Regions, European Commission, 2010*. Preuzeto s: https://op.europa.eu/en/publication-detail/-/publication/4bafb6d8-1f35-4993-b0cf-6b6fb34d8c81 [Pristupljeno: 2.4.2022.]

[144] European Commision. *i2010 – A European Information Society for growth and employment*, MEMO 05/184. Bruxelles 2005. Preuzeto s: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_05_184 [Pristupljeno: lipanj 2020.]

[145] BBVA Research. *The Internet of Things: European regulation, Digital Economy Outlook.* 2016. Preuzeto s: https://www.bbvaresearch.com/wp-content/uploads/2016/07/DEO_ Jul16_Cap3.pdf [Pristupljeno: lipanj 2020.]

[146] Eur-Lex. *DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL* of 16 April 2014 Preuzeto s: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053 [Pristupljeno: 2.4.2022.]

[147] Eur-Lex. *Nova pravila o komercijalizaciji radijske opreme.* 2014. Preuzeto s: https://eur-lex.europa.eu/legal-content/HR/LSU/?uri=CELEX%3A32014L0053 [Pristupljeno: lipanj 2020.]

[148] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* Preuzeto s: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1648911044186 [Pristupljeno: 2.4.2022.]

[149] Eur-Lex. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (*Directive on privacy and electronic communications*) Official Journal L 201, 31/07/2002 P. 0037 – 0047 Preuzeto s: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 [Pristupljeno: 2.4.2022.]

[150] Weber M. *Regulacija tržišta usluga Interneta stvari u pametnim gradovima*. Doktorski rad; Sveučilište u Zagrebu. Fakultet elektrotehnike i računarstva; 2019. Preuzeto s: https://repozitorij.fer.unizg.hr/en/islandora/object/fer%3A6608/datastream/PDF/view [Pristupljeno: lipanj 2020.]

[151] Eur-Lex. REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (*Regulation on Privacy and Electronic Communications*) Brussels, 10.1.2017 Preuzeto s: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010 [Pristupljeno: 2.4.2022.]

[152] Marčinko I. Uredba o e-privatnosti. *Fortuno* 2019. Preuzeto s: https://www.fortuno.hr/uredba-o-e-privatnosti/ [Pristupljeno: lipanj 2020.]

[153] DIREKTIVA 2013/40/EU EUROPSKOG PARLAMENTA I VIJEĆA od 12. kolovoza 2013. *o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP* Preuzeto s: https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=celex%3A32013L0040 [Pristupljeno: 2.4.2022.]

[154] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 *concerning measures for a high common level of security of network and information systems across the Union* (OJ L 194 19.07.2016, p. 1) Preuzeto s: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148) [Pristupljeno: 2.4.2022.]

[155] Filla K. NIS Direktiva: Još jedan razlog zašto vam treba sigurno IT okruženje. Span. 2019. Preuzeto s: https://span.eu/2018/03/nis-direktiva-preprecuje-filmske-scenarije/ [Pristupljeno: lipanj 2020.]

[156] The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification. 2019. Preuzeto s: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity [Pristupljeno: lipanj 2020.]

[157] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and *on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)* Preuzeto s: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881 [Pristupljeno: 2.4.2022.]

[158] The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification. 2019. Preuzeto s: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity [Pristupljeno: lipanj 2020.]

[159] Enisa. About enisa. The European Union Agency for Cybersecurity. Towards a Trusted and Cyber Secure Europe. Preuzeto s: https://www.enisa.europa.eu/about-enisa [Pristupljeno: lipanj 2020.]

[160] Europska Unija. Uredbe, direktive i ostali pravni akti. Preuzeto s: https://europa.eu/european-union/eu-law/legal-acts_hr [Pristupljeno: lipanj 2020.]

[161] Council of Europe. *Convention on Cybercrime* (ETS No. 185). Budapest 2001. Preuzeto s: https://rm.coe.int/1680081561 [Pristupljeno: 2. travanj 2022.]

[162] Republika Hrvatska. *Zakon o izmjenama i dopunama kaznenog zakona.* Izdanje: 105. Zagreb: Narodne novine; 2004

[163] Council of Europe. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. Strasbourg, 28.I.2003. Preuzeto s: https://rm.coe.int/168008160f [Pristupljeno: 2. travanj 2022.]

[164] Vojković G., Štambuk-Sunjić M. Konvencija o kibernetičkom kriminalu i kazneni zakon Republike Hrvatske. Znanstveni članak. 2005. Preuzeto s: https://intranet.pravst.hr/dokumenti/zbornik/200681/zb200601_123-136.pdf [Pristupljeno: lipanj 2020.]

[165] Republika Hrvatska. *Zakon o elektroničkim komunikacijama.* Izdanje: 73. Zagreb: Narodne novine; 2008.

[166] Republika Hrvatska. *Zakon o elektroničkim komunikacijama*. Izdanje: 73. Zagreb: Narodne novine; 2008.

[167] Republika Hrvatska. *Zakon o izmjenama i dopunama zakona o elektroničkim komunikacijama*. Izdanje: 72. Zagreb: Narodne novine; 2017.

[168] Republika Hrvatska. *Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga*. Izdanje: 64. Zagreb: Narodne novine; 2018.

[169] Republika Hrvatska. Ured vijeća za nacionalnu sigurnost. Donesen Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Preuzeto s: https://www.uvns.hr/hr/aktualnosti-i-obavijesti/donesen-zakon-o-kibernetickoj-sigurnosti-operatora-kljucnih-usluga-i-davatelja-digitalnih-usluga [Pristupljeno: lipanj 2020.]

[170] Republika Hrvatska. *Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga.* Izdanje: 68. Zagreb: Narodne novine; 2018.

[171] Republika Hrvatska. Zavod za sigurnost informacijskih sustava. Uredba o kibernetičkoj sigurnosti operatora ključnnih usluga i davatelja digitalnih usluga. Preuzeto s: https://www.zsis.hr/default.aspx?id=403 [Pristupljeno: lipanj 2020.]

[172] Hrvatski Sabor. 9. Saziv Hrvatskoga sabora (14.10.2016. – 22.7.2020.) Prijedlog zakona o dopunama zakona o elektroničkim komunikacijama. Preuzeto s: https://www.sabor.hr/prijedlog-zakona-o-dopunama-zakona-o-elektronickim-komunikacijama-s-konacnim-prijedlogom-zakona?t=115803&tid=208662 [Pristupljeno: 2.4.2022.]

[173] Zakon o elektroničkim komunikacijama. NN 73/08, 90/11, 133/12, 80/13, 71/14, 72/17,2017., članak 104.

[174] Petković M. Osvrt na Prijedlog dopunama Zakona o elektroničkim komunikacijama. 2020. Preuzeto sa: https://informator.hr/vijesti/osvrt-na-prijedlog-dopunama-zakona-o-elektronickim-komunikacijama [Pristupljeno: lipanj 2020.]

[175] Ured vijeća za nacionalnu sigurnost. O nama. Preuzeto s: https://www.uvns.hr/hr/o-nama/djelokrug/informacijska-sigurnost-nsa [Pristupljeno: lipanj 2020.]

[176] CERT.hr. O nama. Preuzeto s: https://www.cert.hr/onama/ [Pristupljeno: lipanj 2020.]

[177] Republika Hrvatska. *Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske* Izdanje:79. Zagreb: Narodne novine; 2006.

[178] Republika Hrvatska. *Zakon o informacijskoj sigurnosti.* Izdanje:79. Zagreb: Narodne novine; 2007.

[179] Republika Hrvatska. *Uredba o mjerama informacijske sigurnosti.* Izdanje:46. Zagreb: Narodne novine; 2008.

[180] Zavod za sigurnost informacijskih sustava. O nama. Preuzeto s: https://www.zsis.hr/default.aspx?id=13 [Pristupljeno: lipanj 2020.]

[181] Republika Hrvatska. *Zakon o mjerama za smanjenje troškova postavljanja elektroničkih komunikacijskih mreža velikih brzina.* Izdanje: 121. Zagreb: Narodne novine; 2016.

[182] Republika Hrvatska. *Zakon o poštanskim uslugama.* Izdanje: 88. Zagreb: Narodne novine; 2009.

[183] Republika Hrvatska. *Zakon o regulaciji tržišta željezničkih usluga i zaštiti prava putnika u željezničkom prometu.* Izdanje: 104. Zagreb: Narodne novine; 2017.

[184] Republika Hrvatska. *Zakon o željeznici.* Izdanje: 32. Zagreb: Narodne novine; 2019.

[185] HAKOM. Misije, vrijednosti i ciljevi. Preuzeto s: https://www.hakom.hr/default.aspx?id=142 [Pristupljeno: lipanj 2020.]

[186] Republika Hrvatska. *Zakon o provedbi Opće uredbe o zaštiti podataka.* Izdanje: 42. Zagreb: Narodne novine; 2018.

[187] Republika Hrvatska. *Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka.* Izdanje: 4. Zagreb: Narodne novine; 2005.

[188] AZOP. O agenciji. Preuzeto s: https://azop.hr/about-the-agency/ [Pristupljeno: 2.4.2022.]

POPIS KRATICA

AES (Advanced Encryption Standard) Napredni enkripcijski standard

AI (eng. Artificial intelligence - AI) Umjetna inteligencija

AIOTI (The Alliance for Internet of Things Innovation) Savez za inovacije IoT-a

API (Application programming interface) Programsko sučelje aplikacije

APM (Asset performance management) Upravljanje performansama imovine

ARM (eng. Architectural Reference Model) Arhitektonski referentni model

AZOP Agencija za zaštitu osobnih podataka

BLE (Bluetooth Low Energy)

BLESA (BLE spoofing Attacks)

CARNET (Croatian academic and research network) Hrvatska akademska i istraživačka mreža

CCMP(Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) Način brojača šifriranja s protokolom za provjeru autentičnosti poruke u lančanom bloku

CCPA (California Consumer Privacy Act) Kalifornijski zakon o privatnosti potrošača

CERT (Computer emergency response team)

CIoT (The Consumer Internet of Things) Potrošački Internet stvari

DDoS (Distributed denial-of-service)

ECU (Engine control unit) Upravljačka jedinica motora

ENISA (The European Union Agency for Cybersecurity) Agencija za kibernetičku sigurnost Europske unije

EU (European Union) Europska Unija

GDPR (The General Data Protection Regulation) Opća uredba o zaštiti podataka

GPRS (General Packet Radio Service)

HAKOM Hrvatska regulatorna agencija za mrežne djelatnosti

ICT (Information and communication technology) Informacijsko komunikacisjke tehnologije

IDS/IPS (eng. Intrusion Detection Systems/Intrusion Prevention Systems)

IIC (The Industrial Internet Consortium)

IIoT (The Industrial Internet of Things) Industrijski Internet stvari

IEEE (The Institute of Electrical and Electronics Engineers) Institut inženjera elektrotehnike i elektronike

IIRA (Industrial Internet Reference Architecture)

IoT (Internet of things) Internet stvari

IoT-A(Internet of things architecture) Internet stvari arhitektura

IoT RA (Internet of things reference architecture) Referentna arhitektura interneta stvari

IP (Internet protocol) Internet protokol

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission)

KRACK (Key Reinstallation AttaCK) Napad ponovne instalacije ključa

LoRa (Long Range Technology)

LTE (Long-Term Evolution)

M2M (Machine to machine) Stroj-stroj

MITM (Man in the middle) Napad čovjeka u sredini

MSM (Messaging Service Model)

MWC (Mobile World Congress) Svjetski kongres mobilnih uređaja

NATO (The North Atlantic Treaty Organization) *Sjevernoatlantski savez*

NBIoT (Narrow Band IoT)

NIS (Network and Information Security Directive) Direktiva o mrežnoj i informacijskoj sigurnosti

NIST (National Institute of Standards and Technology)

NISTIR (National Institute of Standards and Technology Interagency/Internal Report)

NSA (National Security Authority) Ured Vijeća za nacionalnu sigurnost

ODM (eng. Original Design Manufacturer)

OEM (eng. Original Equipment Manufacturing)

OMD (Operations & Management Domain)

OSI Model (Open Systems Interconnection Model)

PED (Physical Entity Domain)

RAID (Resource Access & Interchange Domain)

RAMI 4.0 (The Reference Architectural Model Industrie 4.0) Referentni arhitektonski model industrije 4.0

RF (Radio frequency) Radiofrekvencija

PKI (Public key infrastructure) Infrastruktura javnog ključa

SAD Sjedinjene Američke Države

SCD (Sensing and Controlling Domain)

SD (Secure Digital)

SIEM (eng. Security information and event management)

TKIP (Temporal Key Integrity Protocol) Protokol integriteta vremenskog ključa

TPM (eng. Trusted platform modules)

UART (Universal asynchronous receiver-transmitter) Univerzalni asinkroni prijemnik/odašiljač

WEP(Wired Equivalent Privacy)

WLAN (Wireless local area network) Bežična lokalna mreža

WPA (Wi-Fi Protected Access)

WPAN (Wireless personal area network)

ZSIS Zavod za sigurnost informacijskih sustava

POPIS SLIKA

POPIS GRAFIKONA

PRILOZI

Prilog 1. – Pitanja za anketu

1. Spol
   - muško
   - žensko

2. Dob
   - do 17 godina
   - 18-30 godina
   - 31-45 godina
   - 46-60 godina
   - preko 60 godina

3. Stupanj obrazovanja
   - Završeno osnovnoškolsko obrazovanje
   - Završeno srednjoškolsko obrazovanje
   - Završen preddiplomski studij
   - Završen diplomski studij
   - Završen poslijediplomski studij

4. Koristite li neke od navedenih Cloud servisa za pohranu i razmjenu podataka poput OneDrive, Dropbox, Google Drive, iCloud, AmazonDrive i sl.?
   - Da
   - Ne

5. Koje od navedenih podataka pohranjujete ili dijelite preko Cloud servisa?
   - Fotografije
   - Glazba
   - Video (snimci, filmovi, programi)
   - Dokumenti
   - E-knjige, novine, tekstualne datoteke
   - Ne koristim Cloud servise

6. Smatrate li da su podaci koji se nalaze na Cloudu sigurni i zaštićeni, te da njima ne može pristupiti nitko drugi osim Vas?
   - Da
   - Ne

7. Jesu li Vaše zaporke koje koristite za servise i aplikacije vezane uz datume, godine i mjesta rođenja, imena i prezimena Vas, Vaših bližnjih i kućnih ljubimaca?
   - Da
   - Ne

8. Koje od navedenih uređaja svakodnevno koristite?
   - Pametni telefon
   - Pametni sat
   - Pametni TV
   - Bluetooth slušalice i zvučnik
   - Pametne žarulje
   - Sigurnosne kamere
   - Pametni kućanski aparati (štednjaci, perilice, frižider, usisavač)
   - Niti jedan

9. Koristite li pametni sat?
   - Da
   - Ne

10. Zašto prvenstveno koristite pametni sat?
    - Zabava
    - Sport (rute, puls, vrijeme, kalorije i dr.)
    - Komunikacija (poruke, pozivi)
    - Koristim ga samo zato jer je cool i u trendu.
    - Ne koristim pametni sat

11. Brine li Vas da bi neželjena osoba mogla doći do podataka prikupljenih s Vašeg pametnog sata (puls, tlak, vrijeme spavanja, razina stresa, razina kisika u krvi, lokacija, ruta kretanja, poruke, pozivi, kontakti, datoteke s vašeg mobilnog uređaja) i iskoristiti ih?
    - Da
    - Ne

12. Jeste li svjesni da aplikacija Google Karte sadrži statističke podatke o Vašem kretanju, lokacijama na kojima ste bili i vremenu kada i koliko ste gdje boravili, te da isto bilježi svaki put kada uključite lokaciju na svom mobilnom uređaju?
    - Da
    - Ne

13. Prema Vašem mišljenu koja je najveća prednost pametnih uređaja?
    - Ušteda vremena i novca
    - Jednostavnije obavljanje svakodnevnih zadaća
    - Bolja organizacija
    - Bolji nadzor
    - Automatizacija
    - Povećana sigurnost

14. Prema Vašem mišljenju koji je nnajveći nedostatak pametnih uređaja?
    - Kompleksnost korisničkih sučelja
    - Cijena uređaja
    - Nedovoljna sigurnost i privatnost
    - Nedostatak tehnološkog znanja
    - Nedostatak zakonskog okvira za regulaciju

15. Hoćete li nastaviti koristiti i ulagati u pametne uređaje bez obzira na njihove sigurnosne nedostatke i manjak zakonskih okvira?
    - Da
    - Ne

16. Smatrate li da bi imali veće znanje i bolju kontrolu nad svojim podacima i uređajima kada bi Europska Unija bolje nadzirala privatnost pametnih uređaja i uvela konkretnije zakonske okvire?
    - Da
    - Ne

17. Znate li da su Vam uvedena pametna mjerila električne struje koja ne samo da mjere količinu potrošene energije već bilježe kada je i koliko točno određeni uređaj potrošio električne energije?
    - Da
    - Ne

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad

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

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Privatnost i sigurnost podataka unutar IoT okruženja , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 25. travnja 2022.

Jelena Benduka
(ime i prezime, *potpis*)