Sigurnosni i regulatorni izazovi IoT-a u sustavu zdravstva

Vojvodić, Eduard

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Eduard Vojvodić

SIGURNOSNI I REGULATORNI IZAZOVI IOT-A U SUSTAVU ZDRAVSTVA

DIPLOMSKI RAD

Zagreb, 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 9. lipnja 2021.

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

DIPLOMSKI ZADATAK br. 6550

Pristupnik: **Eduard Vojvodić (0135243187)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **SIGURNOSNI I REGULATORNI IZAZOVI IOT-A U SUSTAVU ZDRAVSTVA**

Opis zadatka:

Implementacija IoT tehnologija u radno okruženje može bitno povećati kvalitetu i brzinu obavljanja određenih zadataka. Kako je u sustavu zdravstva vrijeme i kvaliteta obavljanja zadataka iznimno bitna, IoT može bitno pomoći ispunjavanju zadanih ciljeva. U radu treba navesti sigurnosne i regulatorne izazove suvremenog IoT okruženja u sustavu zdravstva, kako bi se potaknulo na povećanje razine sigurnosti IoT te umanjila vjerojatnost ugroze osobnih podataka ili ometanje rada IoT uređaja.

Mentor:

izv. prof. dr. sc. Goran Vojković

dr. sc. Melita Milenković (komentor)

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

SIGURNOSNI I REGULATORNI IZAZOVI IOT-A U SUSTAVU ZDRAVSTVA

SECURITY AND REGULATORY CHALLENGES OF IOT IN HEALTHCARE SYSTEM

Mentor: izv. prof. dr. sc. Goran Vojković

Student: Eduard Vojvodić

Neposredni voditelj/komentor:

JMBAG: 0135243187

dr. sc. Melita Milenković, mag. iur.

Zagreb, Rujan 2021.

SAŽETAK

Internet stvari ili IoT je tehnologija je 21. stoljeća koja je u stanju unaprijediti poslovanje organizacija prednostima koje dolaze s njenom implementacijom. Međutim, s obzirom da se radi o relativno mladoj tehnologiji, koja je uz to još idejno zamišljena da zbog broja uređaja koji se treba instalirati bude što jeftinija, ona ima mnogo mana, uglavnom vezanih za sigurnost podataka. Te mane imaju poseban značaj kada se razmišlja o uvođenju IoT tehnologija u sustav zdravstva koji barata s osjetljivim podacima o svojim korisnicima. Danas postoji mnogo zakona i propisa kojim se pokušava zaštiti umrežene korisnike neovisno o tome koju digitalnu opremu koriste ali ukoliko se želi postići bezbrižnija budućnost u kojoj se uživa u blagodatima IoT tehnologije potrebno je unaprijediti postojeće i donijeti nove protokole i standarde za IoT kao što se radilo kroz povijest računalne i mobilne mreže.

KLJUČNE RIJEČI: IoT; Zdravstvo; Tehnologija; Sigurnost

SUMMARY

The Internet of Things or IoT is technology of the 21st century that is able to enhance the business of organizations with the benefits that come with its implementation. However, given that this is a relatively young technology, which is also conceptually designed to be as cheap as possible due to the number of devices to be installed, it has many shortcomings, mainly related to data security. These shortcomings are of particular importance when considering the introduction of IoT technologies into a healthcare system that handles sensitive data about its users. Today, there are many laws and regulations that try to protect networked users regardless of what kind of digital equipment they use but if they care to achieve a more worry-free future enjoying the benefits of IoT technology, it is necessary to improve the existing ones and adopt new protocols and standards for IoT as has been done throughout history of computer and mobile networks.

KEYWORDS: IoT; Healthcare; Technology; Security

Sadržaj

1. UVOD

Implementacija IoT tehnologija u radno okruženje može drastično utjecati na kvalitetu i brzinu obavljanja određenih zadataka. S obzirom da u zdravstvenom sustavu o vremenu i kvaliteti obavljanja zadataka može ovisiti ljudski život logično je promišljati o implementaciji IoT tehnologije u njegovo okruženje.

Svrha diplomskog rada jest potaknuti na povećanje razvitka razine sigurnosti u IoT okruženjima kako bi se smanjila vjerojatnost krađe osobnih podataka ili ometanje rada IoT uređaja u sustavu zdravstva.

Cilj je diplomskog rada objasniti što je IoT tehnologija i gdje se može implementirati u radnom okruženju kao što je sustav zdravstva, ukazati na prednosti i mane uvođenja IoT tehnologije, te se posebno posvetiti problemu zaštite osobnih podataka. Naslov diplomskog rada jest: Sigurnosni i regulatorni izazovi IoT-a u sustavu zdravstva. Rad je podijeljen u sedam cjelina:

1. Uvod
2. Općenito o IoT tehnologiji
3. Uloga IoT tehnologije u zdravstvu
4. Prednosti i mane uvođenja IoT tehnologije u zdravstvo
5. Sigurnost i sigurnosni incidenti IoT tehnologije
6. Specifičnosti zaštite osobnih podataka u zdravstvu
7. Zaključak

U drugom se poglavlju objasnilo što predstavlja pojam 'Internet stvari', koju vrstu podataka može prenositi te kako je povezan sa korisnikom kao privatnom osobom, a kako sa korisnikom kao pravnom osobom.

Sustav zdravstva jedan je od osnovnih sustava unutar svake razvijene države. Treće poglavlje objašnjava kako razni komunikacijski standardi imaju različite prednosti i mane te kako zbog toga ne postoji jedan komunikacijski standard koji bi bio zadovoljavajući za svaku svrhu u sustavu zdravstva.

Četvrto poglavlje obuhvaća problematiku prednosti i mana koje IoT tehnologija donosi u sustav zdravstva kako za menadžment tako i za zaposlenike te korisnike sustava u slučajevima implementacije, a koji se spominju kasnije u radu.

U petom poglavlju navedeni su i objašnjeni sigurnosni problemi IoT tehnologije kao i sigurnosni incidenti koji su se dogodili kao rezultat tih propusta.

U šestom poglavlju definirat se koji zakoni i propisi stoje kao zaštita korisnicima za očuvanje tajnosti podataka.

2. OPĆENITO O IOT TEHNOLOGIJI

Internet stvari (engl. Internet of Things), skraćeno IoT, je izraz koji predstavlja fizičke uređaje i senzore čija je glavna zadaća prikupljanje podataka iz svoje okoline te imaju tehničku sposobnost i funkcionalnost uparivanja sa drugim IoT uređajima ili mrežama općenito. Najčešće se pomoću IoT-a želi postići optimizacija radnih procesa ili u drastičnijim slučajevima automatizacija sustava. Klasičan i među najboljim primjerima jest takozvana pametna kuća. Pametna kuća je kuća koja je opremljena s velikim brojem ugrađenih IoT uređaja ili predmeta. Primjeri takvih IoT predmeta mogu biti pametne rolete koje će se automatski dizati i spuštati u skladu sa zorom i sumrakom, pametna vrata koja će se automatski otključavati i otvarati kada vlasnik stane ispred njih ili pametno osvijetljene koje prati kuda se osoba kreće po kući te se pred njom automatski pale svjetla, a sve u svrhu olakšavanja i ubrzavanja svakodnevnih postupaka te eliminacija nepotrebnih radnji kojima se gubi na vremenu.

Olakšavanje i ubrzavanje postupaka bitno je i privatnim i poslovnim korisnicima, pa se u skladu s time, kada se priča o IoT tehnologiji, priča o dvama različitim IoT okruženjima: o IoT-u u okruženju privatnog korisnika i o IoT-u u poslovnom okruženju.

2.1. IoT u okruženju privatnog korisnika

IoT uređaji iz godine u godinu postaju sve privlačniji i dostupniji privatnom korisniku jer mu pružaju nove usluge koje mu predstavljaju dodatnu vrijednost u životu. Najčešće usluge koje se pružaju na IoT uređajima su:

a) Zdravstveni/biometrijski – usluge prikupljanja osobnih zdravstvenih i biometrijskih podataka čija svrha može biti od udaljenog kontroliranja zdravstvenog stanja do optimizacije kvalitete vježbanja
b) Prepoznavanje aktivnosti – usluga prepoznavanja kojom se sportskom aktivnošću bavi pojedinac u nekom trenutku temeljena na prepoznavanju uzoraka. Najčešće se uparuje sa biometrijskim uslugama kako bi se utvrdio i intenzitet sportske aktivnosti u svrhu kasnijeg pregleda detalja o obavljenoj sportskoj aktivnosti.

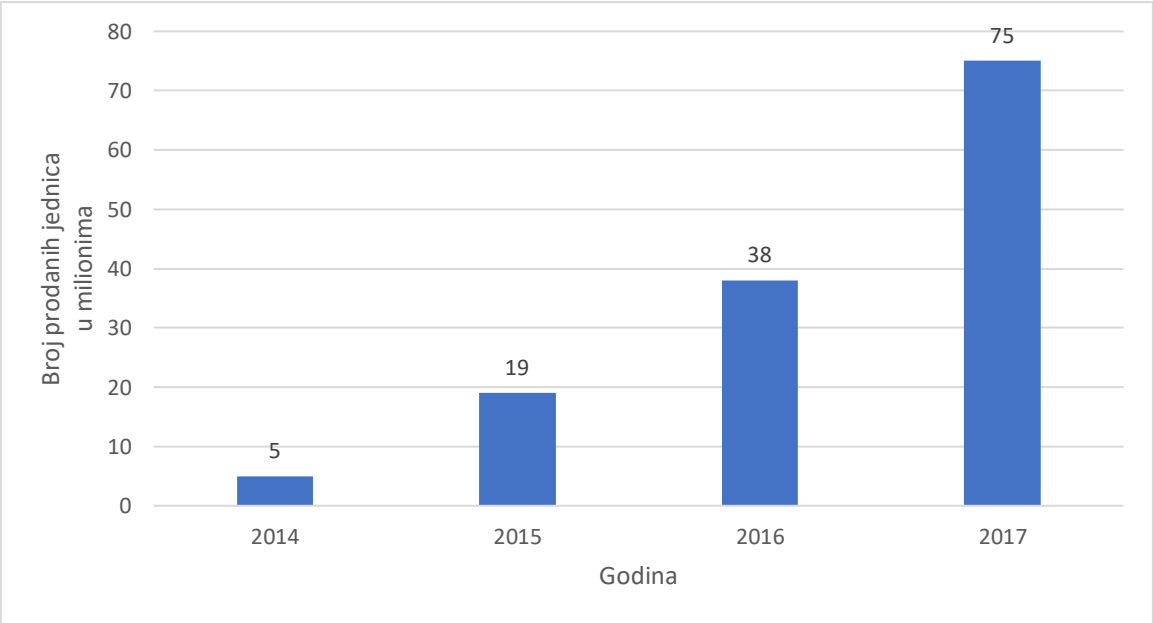
c) Lokacija/kretanje – usluga lociranja korisnika na karti u svrhu pružanja usluge navigacije.
d) Sigurnost – usluge vezane za pružanje dodatne sigurnosti, a mogu uključivati detekciju pada ili umor za volanom [1].

Na tržištu za privatne korisnike postoji široka lepeza IoT proizvoda, a to su najčešće:

a) Pametni satovi i narukvice,
b) Pametne naočale
c) Pametna odjeća
d) Medicinski uređaji

Pametni satovi i zdravstvene aplikacije u proteklim godinama su u povećanom razvoju, kako po svojim funkcionalnostima tako i po samom broju konkurentnih rješenja. Od mogućnosti da se prepozna da li korisnik , hoda, trči ili se bavi nekom drugom aktivnošću do EKG-a (Elektrokardiogram) i mjerenja tlaka što je vidljivo kasnije na stranici 32. Bitno je naglasiti da uređaji konzumne tehnike nisu atestirani pa se ne mogu koristiti u dijagnostičke svrhe. Tako na primjer prikupljene osjetljive informacija poput pulsa ili tlaka pojedinca ne mogu liječniku biti baza za donošenje dijagnoze zbog tog jer su dobivene uređajem koji nema atest. Može se zaključiti da uređaji konzumne tehnike zbog nedostatka atesta nisu adekvatni za primjenu u dijagnostičke svrhe u zdravstvu.

Prema podacima sa stranice Statista, ukupan broj prodanih pametnih satova 2016 godine iznosio je 38 miliona što je duplo više od prethodne godine i preko sedam puta više nego 2014 godine. Rast po godinama od 2014 do 2017 vidljiv je na grafikonu 1.



Grafikon 1. Prodana količina pametnih satova od 2014 do 2017

Izvor: [2]

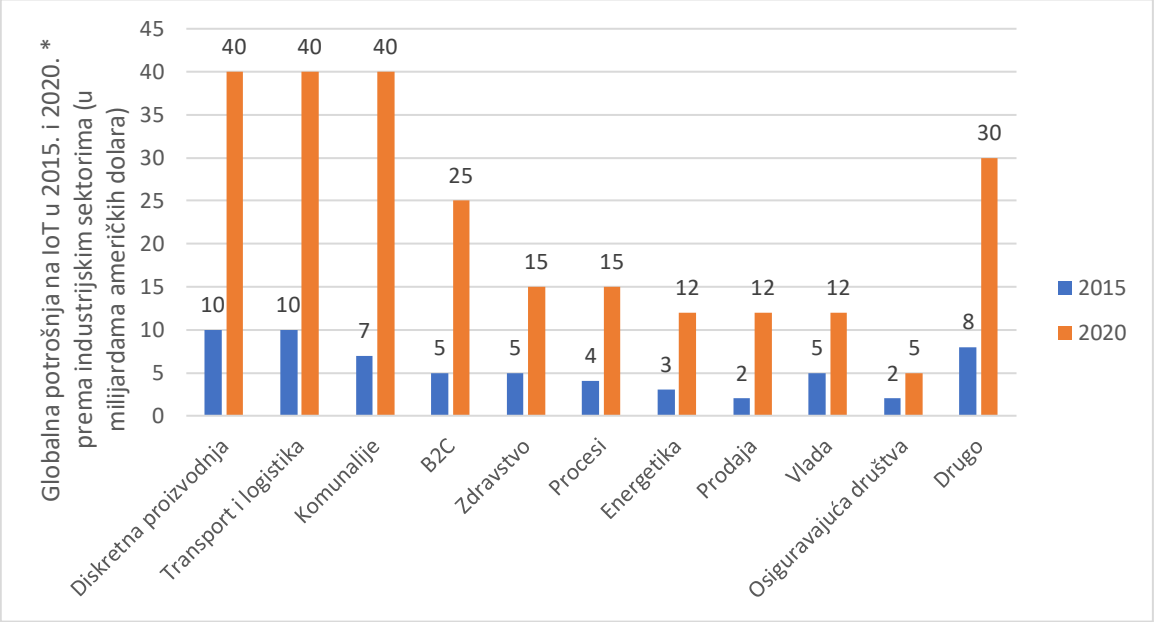
2.2. IoT u poslovnom okruženju

Iako većina ljudi misli da je njihovo vrijeme najvažnije, posljedica uštede ili optimizacije vremena prilikom obavljanja neke radnje u industrijskom sektoru može biti puno značajnija. Od financijskih ušteda i dobitaka do uspješnog spašavanja života, IoT nudi mnogo pogodnosti organizacijama u ostvarivanju uspješnog obavljanja njihove djelatnosti. Neke uobičajene prednosti korištenja IoT-a omogućuju tvrtkama:

a) nadgledati njihove cjelokupne poslovne procese;
b) poboljšati korisničko iskustvo;
c) ušteda vremena i novaca;
d) povećati produktivnost zaposlenika;
e) integrirati i prilagoditi poslovne modele;
f) donositi bolje poslovne odluke; i
g) generirati više prihoda [3].

IoT potiče tvrtke da preispitaju načine na koje pristupaju svom poslu i daje im alate za poboljšanje njihovih poslovnih strategija. Općenito, IoT je najzastupljeniji u proizvodnim,

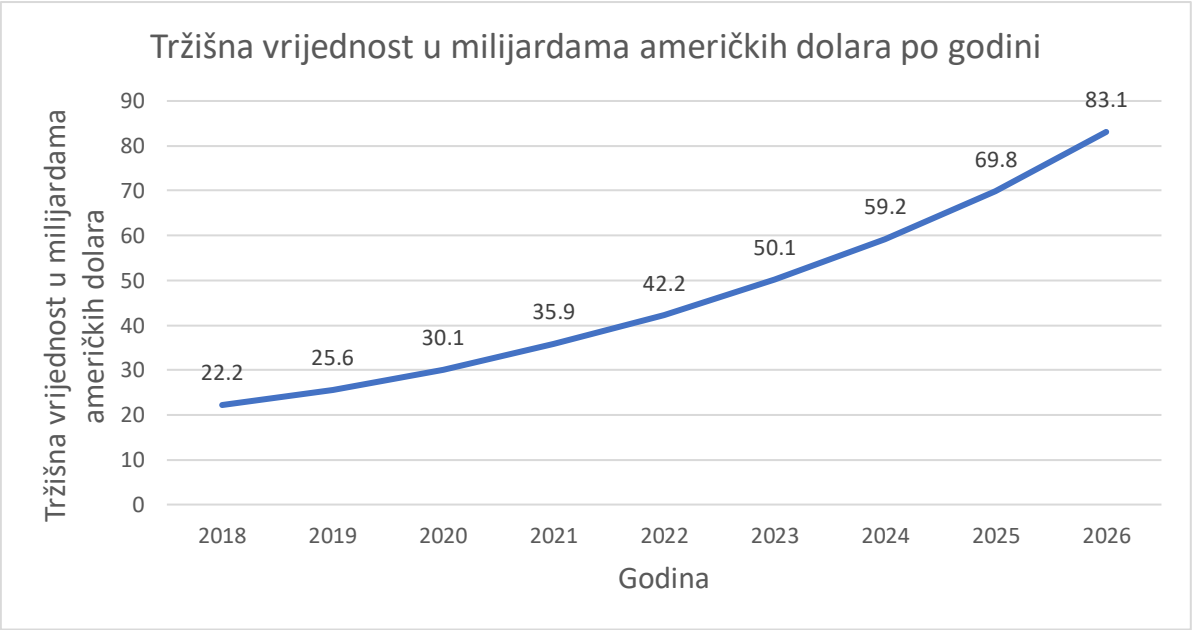
transportnim i komunalnim organizacijama, koristeći senzore i druge IoT uređaje. Međutim, IoT dotiče sve industrije, uključujući zdravstvo, financije, maloprodaju i proizvodnju [3]. Na grafikonu 2 prikazano je top 10 industrija koje najviše ulažu u IoT tehnologiju na godišnjoj razini. Analiza je iz 2019 godine tako da su podaci za 2020 godinu predviđanja [4].



Grafikon 2. Globalna potrošnja na IoT u 2015. i 2020. prema industrijskim sektorima

Izvor: [4]

Kada se pogleda globalno tržište pametnih bolnica, 2021. godine ono je procijenjeno na 35,9 milijardi američkih dolara. Prema budućim procjenama, predviđa se da će se tržišna vrijednost pametnih bolnica eksponencijalno povećati. Prema Statisti, predviđa se da će do 2026. godine tržište pametnih bolnica dosegnuti vrijednost od 83 milijarde američkih dolara što je i prikazano na grafikonu 3 [5].



Grafikon 3. Tržišna vrijednost u milijardama američkih dolara po godini

Izvor: [5]

2021. godine, rast pametnog bolničkog tržišta posebno je posljedica tri aspekta zdravstvene zaštite. Trenutno je segment daljinskog upravljanja lijekovima predstavljao većinu prihoda na tržištu. 2026. predviđa se da će ovaj segment zauzimati više od četvrtine tržišta. Elektronički zdravstveni kartoni i klinički tijek rada bili su drugi po veličini segment, praćeni ambulantnom budnošću [5].

3. ULOGA IOT TEHNOLOGIJE U ZDRAVSTVU

U današnje vrijeme pristup zdravstvenoj zaštiti uvodi se kroz digitalna rješenja, a da bi odgovorila na te promjene zdravstveni sustav treba implementirati nove tehnologije. Prema tome bolnice bi trebale usvojiti naprednije kliničke procese i redizajnirati sustave upravljanja implementacijom novih tehnologija kako bi išle u korak s digitalizacijom zdravstvene zaštite [5].

Kada se govori o implementaciji IoT-a u industrije najvažnije je razumjeti da postoji više vrsta tehnologija preko kojih IoT uređaji mogu vršiti svoju funkciju. Svaka tehnologija ima svoje tehničke prednosti i mane te su kao takve više ili manje prikladne za pojedina industrijska okruženja. Trenutno vodeće tehnologije prema primjeni sa IoT tehnologijom su:

1. LPWAN,
2. Mobilne mreže,
3. ZigBee,
4. Bluetooth i BLE,
5. WiFi,
6. RFID.

Svaka od navedenih ima svoje prednosti i mane te je u tablici 1 prema BehrTech-u prikazano za koji sektor je koja tehnologija optimalna, a za koja je primjenjiva [6].

Tablica 1. Prikaz optimalnih tehnologija prema industrijskim sektorima

	LPWAN mreža	Mobilne mreže	ZigBee mreža	Bluetooth LE mreža	WiFi mreža	RFID mreža
Industrija	Optimalno	Primjenjivo	Primjenjivo			
Pametno mjerenje komunalija (voda, plin i struja)	Optimalno					
Pametni gradovi	Optimalno					
Pametne zgrade	Optimalno		Primjenjivo	Primjenjivo		
Pametne kuće			Optimalno	Optimalno	Optimalno	
Nosivi uređaji	Primjenjivo			Optimalno		
Povezani automobili					Primjenjivo	
Povezano zdravstvo		Optimalno		Optimalno		
Pametna prodaja		Primjenjivo		Optimalno	Primjenjivo	Optimalno
Logistika	Primjenjivo	Optimalno				Optimalno
Pametna agrikultura	Optimalno					

Izvor: [6]

3.1. LPWAN

IoT aplikacija je u svijetu puno i one se međusobno mogu jako razlikovati po pitanju prednosti i mana povezanih sa njihovim načinom rada. Mogu se razlikovati po broju senzora, a samim tim i po načinu komunikacije između njih. Neke IoT aplikacije trebaju znatan broj senzora raspoređenih na velikom području. Takva instalacija zahtjeva bežičnu komunikaciju velikog dometa i male potrošnje energije, dok druge IoT aplikacije mogu koristiti znatno manji broj senzora na relativno malom području. Kad su u pitanju IoT aplikacije koje koriste vrlo veliki broj senzora potrebno je imati na umu da njihovo održavanje (npr. promjena baterija u svakom senzoru) povećava opseg posla i time ih znatno poskupljuje. Tu se javlja LPWAN ili

širokopojasne mreže male snage (engl. Low Power Wide Area Network) koje pružaju uslugu pokrivenosti širokog područja potrebnu za velike, granulirane bežične senzorske mreže po niskoj cijeni te maloj potrebnoj snazi napajanja. LPWAN je usmjeren za IoT telemetrijske aplikacije gdje se povremeno prenose male količine podataka [7]. Neki od mnogih primjera upotrebe gdje je potrebna tehnologija sa upravo takvim specifikacijama su:

- postavljanje senzora na vozila kako bi ih se mogla na primjer pratiti njihova lokacija
- u parkirnim garažama senzori otkrivaju slobodna parkirna mjesta i šalju jasnu i jednostavnu poruku 'Da' ili 'Ne',
- brave u školskim objektima koje se po potrebi mogu na daljinu aktivirati ili deaktivirati podižući razinu sigurnosti na viši nivo,
- senzori u spremnicima za otpad mogu dojavljivati nadležnoj službi razinu njihove popunjenosti optimizirajući na taj način rad poduzeća za odvoz otpada i tako dalje [8].

Postoji više novih izvedbi LPWAN tehnologije, a najpopularnije su LoRa, SIGFOX, Ingenu, Weightless i SymphonyLink i NB – IoT [9].

3.2. Mobilne mreže

Telekomunikacijska mreža je uređen skup prostorno distribuiranih tehničkih sustava odnosno kapaciteta ili resursa dizajniranih i izgrađenih prema temeljnom zahtjevu da uspješno poslužuju promet na određenom području [10].

Mobilna mreža je telekomunikacijska mreža koja nudi pouzdanu širokopojasnu dvosmjernu komunikaciju između mobilnih terminalnih uređaja. Zamišljena je za prijenos glasa, a s vremenski odmaknutim iteracijama po pitanju načina i tehnika prijenosa signala između njezinih generacija (1G ili NMT, 2G ili GSM, 3G ili UMTS, 4G ili LTE, 5G) prilagođena je i za brzi, pouzdani i siguran prijenos podataka.

Prednosti korištenja IoT uređaja preko mobilnih mreža su:

- veliko područje pokrivenosti – Koriste se već postojeća infrastruktura mobilnih mreža koje unutar država pokrivaju veliki postotak površine te države.

- mrežno prebacivanje – Za razliku od korisničkih SIM kartica, M2M SIM kartice mogu se prebacivati između mobilnih operatera kako bi se osigurala stalna i pouzdanu povezanost i minimizirano vrijeme nedostupnosti usluge.
- skalabilnost usluga u skladu sa potrebama – Različita poslovanja imaju različite QoS odnosno zahtjeve za uslugom (engl. Quality of Service).
- daljinsko upravljanje i analitika – IoT uređajima na mobilnim mrežama moglo bi se upravljati na daljinu pomoću IoT platforme, koja vam omogućuje povezivanje, odspajanje ili rješavanje problema s uređajima neovisno o njihovoj lokaciji.
- privatne mreže i sigurnosne opcije – IoT uređaji na mobilnim mrežama mogu koristiti tehnologiju privatne mreže (VPN-ovi, APN-ovi i IPsec protokoli) za dodavanje slojeva sigurnosti uređaju, mreži i podacima [11].

Međutim, jedan od mogućih problema korištenja ove tehnologije čija duljina rada ovisi o kapacitetu baterije je između ostalog i visoka potrošnja električne energije u usporedbi s sadašnjim tehnologijama. Jedan od primjera koji se spominje u radu, a koji se zbog svojih malih dimenzija ugrađuje u tijelo pacijenta je pacemaker. Uzročno posljedično tome, time je određena maksimalna veličina baterije koja ga napaja s električnom energijom, a s njenom veličinom i sam maksimalni kapacitet baterije.

S obzirom na navedeno ako se pretpostavi da je kapacitet baterije fiksan, uvođenjem tehnologije koja bi taj kapacitet brže trošila više bi se naškodilo sustavu jer bi se povećao intenzitet prometa pacijenata koji bi zahtijevali promjenu baterije u svom pacemakeru.

Međutim postoje razna područja primjene IoT tehnologije gdje bi mobilna mreža pružala idealnu podršku za njihov rad. Općeniti primjeri uključuju međusobnu povezanost vozila na cesti ili upravljanja voznim parkom u transportu i logistici. Tako bi na primjer njihova primjena u budućnosti omogućila daljnju implementaciju protokola o automatiziranom stvaranju hitnog koridora. Prije nego bi vozači osobnih vozila sami vidjeli interventno vozilo iza sebe dobili bi informaciju o potrebi micanja svog vozila u stranu zbog potrebe za stvaranjem koridora za prolaz vozila hitne intervencije čime bi se moglo drastično smanjilo vrijeme dolaska vozila hitne intervencije na mjesto nesreće.

3.3. ZigBee

Zigbee je bežična tehnologija razvijena kao otvoreni globalni standard za rješavanje jedinstvenih potreba jeftinih bežičnih IoT mreža male snage. Zigbee standard djeluje na IEEE 802.15.4 fizičkoj radio specifikaciji i radi u nelicenciranim opsezima, uključujući 2,4 GHz, 900 MHz i 868 MHz. Specifikacija 802.15.4 na kojoj djeluje Zigbee potvrdila je Institut inženjera elektrotehnike i elektronike (IEEE) 2003. godine. Specifikacija je paketni radio protokol namijenjen jeftinim uređajima na baterije. Protokol omogućuje uređajima da komuniciraju u različitim mrežnim topologijama i može im trajati nekoliko godina [12].

Ključna komponenta Zigbee protokola je sposobnost podrške mrežnog umrežavanja. U mrežastoj mreži čvorovi su međusobno povezani s drugim čvorovima tako da više čvorova povezuje svaki čvor. Veze između čvorova dinamički se ažuriraju i optimiziraju kroz sofisticiranu, ugrađenu tablicu usmjeravanja mreža. Mrežaste su mreže decentralizirane prirode što zapravo znači da je svaki čvor sposoban za samootkrivanje na mreži. Također, kako čvorovi napuštaju mrežu, mrežasta topologija omogućuje čvorovima da ponovno konfiguriraju putove usmjeravanja na temelju nove mrežne strukture. Karakteristike mrežne topologije i Ad-hoc usmjeravanja pružaju veću stabilnost u promjenjivim uvjetima ili neuspjehu na pojedinačnim čvorovima [12].

Zigbee protokol osmišljen je kako bi pružio jednostavno bežično podatkovno rješenje koje karakteriziraju sigurne, pouzdane arhitekture bežične mreže. Zigbee 3.0 protokol dizajniran je za komunikaciju podataka kroz bučna RF okruženja koja su česta u komercijalnim i industrijskim primjenama. Verzija 3.0 nadograđuje se na postojeći Zigbee standard, ali objedinjuje specifične profile tržišta koji omogućavaju bežično povezivanje svih uređaja u istoj mreži, bez obzira na njihovu tržišnu oznaku i funkciju. Nadalje, Zigbee 3.0 sustav certificiranja osigurava interoperabilnost proizvoda različitih proizvođača. Povezivanjem Zigbee 3.0 mreža s IP domenom otvara se nadzor i kontrola s uređaja kao što su pametni telefoni i tableti na LAN-u ili WAN- u, uključujući Internet, i donosi stvarni IoT [12].

Značajke Zigbee PRO 2015 i novih protokola navedeni su u tablici 2.

Tablica 2. Značajke ZigBee tehnologije

Rješenje	Opis
Mrežna topologija	• Samoformirajući, samo izlječivi MESH
Tipovi mrežnih uređaja	• Koordinator (sposoban za usmjeravanje), • usmjerivač, • krajnji uređaj, • Zigbee Green Power uređaj
Veličina mreže (teoretski broj čvorova)	• Do 65.000
Radio tehnologija	• IEEE 802.15.4-2011
Frekvencijski opseg / kanali	• 2,4 GHz (ISM opseg) sa 16 kanala širine 2 MHz
Brzina prijenosa podataka	• 250 Kbit / s
Sigurnosni modeli	• Centralizirano (s podrškom za instaliranje kodova), • Distribuirano
Podrška za šifriranje	• AES-128 na mrežnom sloju, • AES-128 dostupan na aplikacijskom sloju
Komunikacijski (prosječni) domet	• Do 300+ metara (bez prepreka), • Do 75-100 metara u zatvorenom
Podrška male snage	• Uređaji za spavanje • Zigbee Green Power Uređaji (prikupljanje energije)
Podrška naslijeđenih profila	• Zigbee 3 uređaji mogu se pridružiti naslijeđenim mrežama Zigbee profila. • Naslijeđeni uređaji mogu se pridružiti Zigbee 3 mrežama (na temelju sigurnosnih pravila mreže)
Podrška za logičke uređaje	• Svaki fizički uređaj može podržavati do 240 krajnjih točaka (logičkih uređaja)

Izvor: [13]

Zigbee omogućuje široko utemeljeno postavljanje bežičnih mreža s jeftinim rješenjima male snage. Pruža mogućnost rada godinama na jeftinim baterijama za mnoštvo aplikacija za nadzor i upravljanje. Pametne energetske mreže, AMR (automatsko očitanje brojača), kontrole osvjetljenja, sustavi automatizacije zgrada, nadzor spremnika, HVAC kontrola, medicinski uređaji i aplikacije voznog parka samo su neki od mnogih prostora na kojima Zigbee tehnologija postiže značajan napredak [12].

3.4. Bluetooth

Bluetooth je protokol koji omogućuje razmjenu podataka na kratkim udaljenostima a nastao je 1994. godine [8]. Sa razvojem tehnologija i s obzirom da radi na principu ,,frequency hopping spread spectrum" (metoda ponavljajućeg prebacivanje nosive frekvencije tijekom radijskog prijenosa kako bi se smanjile smetnje i izbjeglo presretanje [14]), čime se postiže relativno sigurna transmisija podataka, postao je primjenjiv i u privatnim i u poslovnim okruženjima. Od svog nastanka do danas Bluetooth je postao standardna opcija za međusobno bežično povezivanje dvaju ili više uređaja u svrhu transmisije podataka. Njime se vrši povezivanje male snage i velike pojasne širine. Domet povezivanja je također mali, odnosno uređaji koji se povezuju moraju biti na maloj udaljenosti kako bi se povezali [8].

Tokom svog nastajanja Bluetooth je bio namijenjen prijenosnoj opremi i njoj srodnim aplikacijama. Zato se nameće kao najpraktičniji kad je potrebno povezati samo dva uređaja sa minimalnom konfiguracijom. Koristi slabe signale, ima ograničene smetnje i funkcionira u „bučnim" okruženjima. Te karakteristike pokazale su se vrlo korisne i praktične u industrijskom IoT-u gdje radni strojevi šalju kratke nizove podataka u bučnom okruženju [8].

Razvojem Bluetooth 5 u prosincu 2016. godine postupno se potiskuje neograničeni potencijal IoT-a. Bluetooth 5 može se pohvaliti četverostrukim dosegom, dvostrukom brzinom i povećava kapacitet razmjene poruka do 800% u usporedbi sa prethodnom verzijom te uvodi mogućnost isprepletenog umrežavanja (engl. Meshnet) [8]. Isprepleteno umrežavanje je mreža u kojoj su uređaji ili čvorovi povezani međusobno kroz grananje s drugim uređajima ili čvorovima, a takve su mreže postavljene za učinkovito usmjeravanje podataka između uređaja i klijenta. [15]

Bluetooth Low Energy ili BLE na tržište se pojavio 2011. godine kao Bluetooth 4.0. Kada se govori o BLE tehnologiji u odnosu na Bluetooth, ključna razlika je u niskoj potrošnji energije Bluetooth 4.0. Iako to možda zvuči kao nešto negativno, zapravo je izuzetno pozitivno kada se govori o M2M komunikaciji. Uz potrošnju energije BLE aplikacije mogu raditi na bateriji niskog kapaciteta četiri do pet godina. Iako ovo nije idealno za telefonski razgovor, vitalno je za aplikacije koje samo povremeno trebaju razmjenjivati male količine podataka [16].

Baš kao i Bluetooth, BLE radi u 2,4 GHz ISM opsegu. Za razliku od klasičnog Bluetootha, BLE ostaje u stanju mirovanja neprestano, osim kada je veza uspostavljena. Stvarna vremena povezivanja su samo nekoliko milisekundi, za razliku od Bluetootha koji u prosjeku treba 100ms. Razlog zbog kojeg su veze tako kratke je taj što su brzine prijenosa podataka visoke na 1 Mb/s [16].

BLE-ove IoT M2M mjesta aplikacije mogu biti:

- Mjerači krvnog tlaka
- Uređaji poput fibita
- Industrijski senzori za nadzor
- Geografske, ciljane promocije (iBeacon)
- Aplikacije za javni prijevoz

Primjer vrlo korisne primjene Bluetootha je nadzor imovine u zatvorenom prostoru. Primjenom metode triangulacije za određivanje položaja nadzirane imovine preko više Bluetooth „svjetionika“ koristeći jačinu signala. Može se zaključiti da je Bluetooth snažna opcija povezivanja za mnoge unutarnje internetske aplikacije [8].

3.5. WiFi

Wi-Fi je tehnologija bežičnog umrežavanja koja omogućuje terminalnim uređajima da se povežu s Internetom. Pod pojmom terminalni uređaji podrazumijevaju se sve vrste računala, mobilnih uređaja (pametni mobilni telefoni i svi drugi nosivi uređaji) i ostala oprema (pisači i video kamere). Wi-Fi omogućuje svim ovim uređajima, međusobnu razmjenu informacija, a gdje se pritom stvara mreža [17].

Wi-Fi ima nekoliko značajnih razlika od ostalih bežičnih tehnologija. Na primjer, Wi-Fi emitira na frekvencijama od 2,4 GHz ili 5 GHz. Te su frekvencije mnogo veće od frekvencija koje se koriste za stanični prijenos. Viša frekvencija znači da signali mogu prenijeti više podataka. Velikom brzinom prijenosa podataka, WiFi troši puno energije, a nema puno dometa. Zbog tog, WiFi može biti dobar za one IoT aplikacije:

- koje se ne moraju brinuti zbog odvoda energije (npr. Uređaji koji su priključeni na utičnicu),
- koji trebaju poslati puno podataka (npr. Video) i
- kojima nije potreban velik domet [17].

Dakle, iako Wi-Fi trenutno nije sjajan za mnoge IoT aplikacije, postoje dva Wi-Fi standarda koja su razvijena i razvijaju se i dalje, posebno za IoT. To su WiFi HaLow (802.11ah) i HEW (802.11ax). WiFi HaLow ratificiran je 2016. godine. Usmjeren je na rješavanje problema dometa i snage za IoT aplikacije. HEW ili High Efficiency Wireless (hrv. Visokoučinkovita bežična mreža) nadolazeći je standard koji se nadovezuje na HaLow i dodaje dodatne značajke prikladne za IoT [17].

3.6. RFID

Radio frequency identification system, skraćeno RFID, je sustav za identifikaciju radio frekvencija. To je tehnologija koja omogućuje strojevima ili računalima da identificiraju predmete, snime meta podatke ili kontroliraju pojedinačnu metu putem radio valova [18].

RFID sustavi sastoje se od oznaka i čitača. Oznake su odašiljači, a čitači su prijemnici. RFID čitač komunicira s RFID oznakom pomoću radio valova. Glavna prednost RFID tehnologije je automatizirana identifikacija i prikupljanje podataka u svrhu poslovnih aktivnosti, a čiji je cilj smanjiti troškove već korištenih sustava. Patent Charlesa Waltona 1983. godine prvi je patent koji je koristio kraticu RFID. Od tada je ona napredovala i evoluirala. Tijekom posljednjeg desetljeća doživljava značajniji razvoj zbog potrebe smanjenja troškova kao glavnog ograničenja u mnogim implementacijama [18].

Funkcije RFID sustava obično uključuju tri aspekta: nadgledanje, praćenje i nadzor. Nadgledanje općenito znači biti svjestan stanja sustava ponavljanim promatranjem određenih uvjeta, posebno da bi se otkrili i upozorili na promjene. Praćenje je promatranje osoba ili predmeta u pokretu i pružanje pravodobno poredanog niza podataka o određenom položaju modelu. Nadzor je praćenje ponašanja, aktivnosti ili drugih promjenjivih informacija, obično ljudi. To se ponekad radi na tajni ili neupadljivi način. RFID aplikacije su brojne i dalekosežne.

Najzanimljivije i najuspješnije aplikacije uključuju one za upravljanje lancem opskrbe, kontrolu proizvodnog procesa i upravljanje praćenjem objekata [18].

Prednosti RFID tehnologije u zdravstvu su različite, od integriranja sustava automatizacije u bolnicama koji koriste RFID tehnologiju za ubrzanje inventara do bolje vidljivosti protoka ljudi i korištenja prostora za kontrolu infekcija i bolje upravljanje tokovima rada [19]. Druge potencijalne nove primjene RFID tehnologije u zdravstvu su:

- Učinkovito praćenje, upravljanje i pravodobno održavanje skupe bolničke opreme.
- Jednostavno lociranje i upravljanje medicinskim uređajima zahvaljujući razvoju RFID uređaja za praćenje.
- Automatizirani popis i upravljanje proizvodima i lijekovima za jednokratnu upotrebu. Poboljšana točnost i ažuriranje zaliha u stvarnom vremenu.
- Smanjeni troškovi rada; povećana produktivnost uz manje napora.
- Poboljšano iskustvo za pacijente, posjetitelje, pružatelje usluga.
- Optimizirani radni raspored i rutine za zdravstvene djelatnike.
- Eliminirane ljudske pogreške i gubitak vrijednih podataka.
- Bolja sigurnost u bolnicama.
- Zajamčena kvaliteta medicinskih proizvoda zahvaljujući autentifikaciji temeljenoj na RFID-u.
- Pojačane mjere protiv širenja infekcije, krađe lijekova i bolničke imovine [19].

Nedostatke RFID sustava mogu se uočiti analizirajući ga sa tehnološkog aspekta i sa pozicije korisnika. Ti problemi su:

a) Problemi interferencije – Komunikacija između oznaka i čitača u osnovi je osjetljiva na elektromagnetske smetnje. Predloženi su mnogi protokoli protiv interferencije za identifikaciju RFID oznaka, ali gotovo svi poznati protokoli pokazuju ukupnu učinkovitost identifikacije manje od 50%. Ipak, protokol stabla interferencije (CT), nadmašuje sve ostale do sada predložene protokole protiv interferencije.
b) Pitanja sigurnosti i privatnosti – Problemi sa sigurnošću i privatnošću RFID oznaka bitni su i organizacijama i pojedincima. Zbog ograničenja troškova i resursa, RFID sustav nema dovoljnu podršku za sigurnost i privatnost. Mnogi istraživači i znanstvenici rade

na primjeni jeftinog protokola sigurnosti i privatnosti kako bi povećali primjenjivost. Za RFID je predloženo puno laganih rješenja, ali oni su i dalje skupi i ranjivi na sigurnost, te ne rješavaju u potpunosti sigurnosne probleme.

c) Ostali izazovi – Ostali izazovi RFID-a su svakako: trošak, dizajn i integracija RFID-a u postojeće sustave. Važno je razviti učinkovit RFID posrednički softver koji bi se koristio za povezivanje novih RFID sustava u postojeće pozadinske infrastrukture [18].

Mjesta primjene RFID sustava su brojni i dalekosežni. Najzanimljivije i najuspješnije aplikacije uključuju one za upravljanje lancem opskrbe, kontrolu proizvodnog procesa i upravljanje praćenjem objekata. Sada se RFID postupno i široko koristi u sljedećim poljima:

- Logistika i opskrba
- Prerađivačka industrija
- Zdravstvena zaštita i medicina
- Operacije na morskim terminalima
- Vojska i obrana
- Platne transakcije
- Okoliš, i sustavi upozorenja
- Transport i maloprodaja
- Skladišni i distribucijski sustavi
- Ostale primjene u mnogim poslovnim sektorima na primjer, u proizvodnji [18].

4. PREDNOSTI I MANE UVOĐENJA IOT TEHNOLOGIJA U ZDRAVSTVO

Korištenje bilo kojeg alata ili tehnologije u usporedbi sa drugim alatom ili tehnologijom ima svoje prednosti i mane.

Korist od implementacije može imati administracija koja će imati uvid u relevantne podatke kako zaposlenici obavljaju svoje dužnosti, ali i zaposlenici koji bi zahvaljujući većem broju podataka u određenim slučajevima bili u stanju dati bolju dijagnozu. U skladu s time može se zaključiti da se prednosti i mane implementacije IoT tehnologije mogu gledati sa raznih stajališta koja uključuju:

1. menadžment,
2. zaposlenike,
3. korisnike.

4.1. Prednosti i mane implementacije IoT-a sa stajališta menadžmenta

Najvažniji segment poslovanja jest upravljanje njime. „Poslovno upravljanje odnosi se na upravljanje poslovnim sustavom, što uključuje planiranje, organiziranje, vođenje i kontrolu napora i resursa organizacije da bi se ostvarili definirani ciljevi poslovanja“ [20].

Kako bi se poslovno upravljanje moglo kvalitetno obavljati potrebno je kontinuirano prikupljati relevantne podatke i vršiti analizu nad njima. Ovisno o opsegu prikupljanja podataka, vrijeme potrebno za njegovo prikupljanje može biti neželjeno dugo. Kako bi se izbjeglo gubljenje vremena, te kako bi se osigurali što točniji podaci najbolje bi bilo koristiti mrežu uređaja i senzora za prikupljanje podataka o svojoj okolini, a upravo je to IoT.

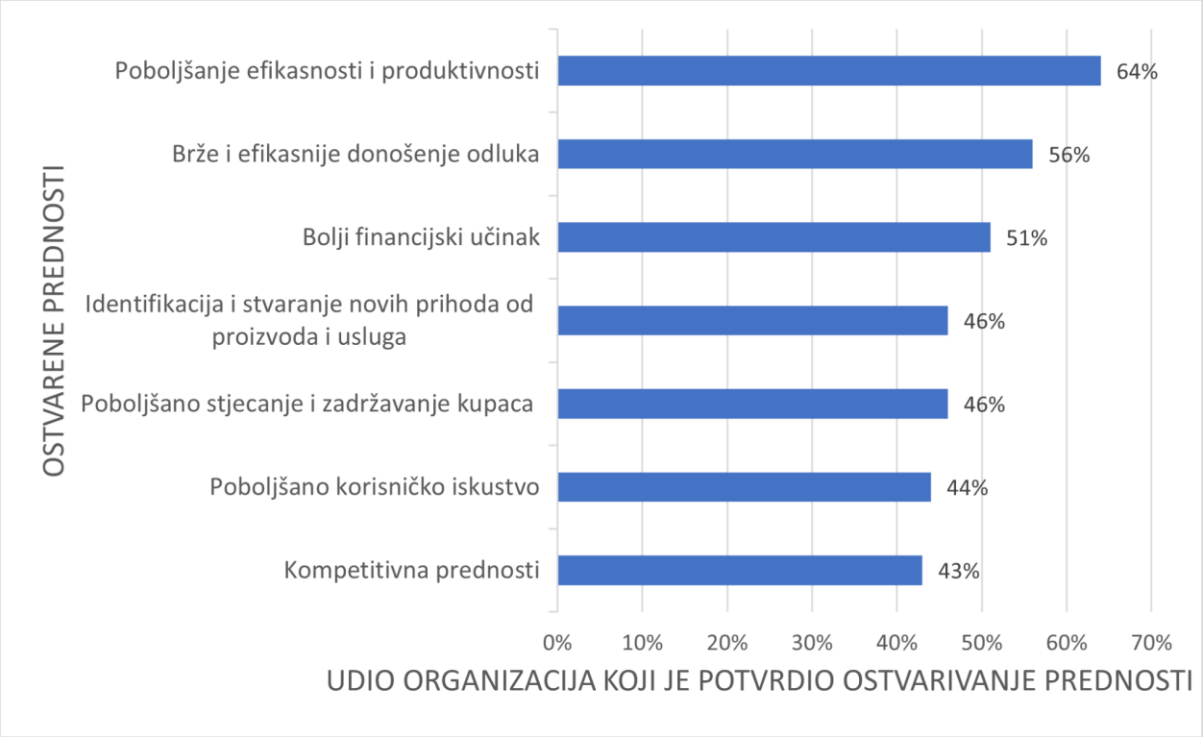
IoT može pomoći u automatizaciji tijeka zdravstvene zaštite i zdravstvene zaštite pacijenta kroz rješenje 'mobilno zdravstvo'. Mobilno zdravstvo je pojam kojim se opisuje sustav nosivih IoT uređaja koji prikupljaju informacije o zdravstvenom stanju pojedinca koji ih nosi. IoT u zdravstvu omogućuje interoperabilnost, komunikaciju od stroja do stroja, razmjenu informacija i kretanje podataka što može smanjiti troškove smanjivanjem nepotrebnih

posjeta i korištenjem resursa bolje kvalitete čineći isporuku zdravstvenih usluga izuzetno isplativom. Time menadžment može postići poboljšanje postupaka raspodjele i planiranja resursa [21].

Osim poboljšanja postupaka raspodjele i planiranja resursa mogu se postići brojne druge prednosti. Neke uobičajene prednosti korištenja IoT-a omogućuju tvrtkama:

a) nadgledati njihove cjelokupne poslovne procese;
b) poboljšati korisničko iskustvo;
c) ušteda vremena i novaca;
d) povećati produktivnost zaposlenika;
e) integrirati i prilagoditi poslovne modele;
f) donositi bolje poslovne odluke; i
g) generirati više prihoda [3].

Prema podacima sa Statiste iz 2019 godine, na grafikonu 4 su prikazane glavne prednosti koje su organizacije ostvarile upotrebom analize nad prikupljenim podacima. „Oko 64 posto ispitanika izjavilo je da je korištenjem podataka i analitike postignuta poboljšana učinkovitost i produktivnost“ [22].



Grafikon 4. Prednosti koje su organizacije ostvarile upotrebom metoda prikupljanja podataka i njihovom analizom [22]

Primjeri podataka koji bi se mogli prikupljati, a od interesa za menadžment su:

1. Podaci o kretanju zaposlenika
2. Podaci o lokaciji, kretanju i korištenju opreme i uređaja
3. Podaci o radu opreme i uređaja
4. Podaci o radnim i bolničkim uvjetima

4.1.1. IoT oprema i uređaji

Podaci o lokaciji, kretanju i korištenju opreme bitni su za nekoliko stvari. Prva je za praćenje trenutne lokacije nekog komada opreme. Ova usluga može biti od koristi u slučajevima kada ustanova nije predimenzionirana po pitanju opreme, već radi s ograničenim brojem određenih uređaja, a taj je broj manji od broja potrebnih uređaja u vršnom satu. Vršni sat je sat u kojem se javlja najveća potražnja za određenom uslugom. Tada, u slučaju kada na primjer odjel A treba neki uređaj koji su drugi odjeli već uzeli, osoba iz odjela A moći će u

sustavu potražiti gdje su uređaji zahvaljujući čemu će potencijalno brže moći do uređaja koji im treba nego da sam zove svaki odjel posebno da provjeri je li komad opreme na tom odjelu. Druga je za slučaj ukoliko se želi napraviti analiza optimiziranosti lokacije za pohranu neke opreme. Na temelju analize višestrukih uzoraka tko je, kada i na koliko dugo trebao neki komad opreme, menadžment može odlučiti da se oprema smjesti bliže odjelu sa većom potražnjom ili da je vrijeme nova ulaganja u opremu. Treća stvar zašto je bitno prikupljati ove podatke jest jer pruža uvid u navike zaposlenika u služenju, ili ne služenju, s određenom opremom kao i potencijalno neovlašteno služenje opremom, neovlašten pristup ormariću s lijekovima ili pronalazak zametnute opreme.

Podaci o radu opreme su tehnički podaci o parametrima rada, greškama i kvarovima na opremi. Ovi podaci su od interesa za menadžment jer omogućuju mogućnost kvalitetnijeg preventivnog održavanja opreme te manji broj potrebnog ljudstva za provjeru sve opreme što znači i veće uštede u poslovanju.

Podaci o radnim i bolničkim uvjetima bitni su jer pružaju uvid o stanju u radnim prostorijama po pitanju temperature, razine vlage, tlaka i razine CO_2 (ugljikov dioksid) u zraku. Ne zadovoljavajuće razine navedenih parametara mogu dovesti do smanjenih performansi zaposlenika te do sporijeg oporavka pacijenata, ni jedno od čega ne pridonosi reputaciji ustanove. Također je bitno za napomenuti da su takvi uvjeti nedopustivi na odjelima za infektologiju gdje je širenje infekcija najveća briga kako i za pacijente i za zaposlenike. U skupinu uređaja koji prikupljaju ove podatke mogli bi se svrstati i IoT uređaji čija bi zadaća bila brojati broj korištenja sanitarnog čvora. Osim što bi se iz tih podataka moglo pametnije odlučiti kada i koliko često osoblje zaduženo za čistoću tih prostorija mora dezinficirati te prostorije, liječnici bi mogli imati bolji uvid u učestalost obavljanja nužde pacijenata čime se može samo poboljšati njihovo liječenje [23].

4.1.2. Optimizacija osoblja

Ukoliko se želi adekvatno djelovati na sustav važno je sustav poznavati. Jedan od načina upoznavanja i analiziranja sustava zdravstva je pomoću realizacije da se radi o podvorbenom sustavu. Podvorbeni sustav ili sustav posluživanja je sustav u koji pristižu određeni entiteti i traže uslugu. Podvorbeni sustav je sustav koji se sastoji od korisnika, repa, poslužitelja i zbirke pravila prema kojima se obavlja posluživanje dolazećega korisnika. Rep je skup korisnika koji čekaju na posluživanje. Ukoliko se želi djelovati na rep na način da se smanji prosječno vrijeme čekanja u repu najbolje je djelovati na podvorbenu stegu, način kako korisnici ulaze u rep, kako se ponašaju te kako izlaze iz njega. Međutim na podvorbenu stegu je teško utjecati jer definiraju način poslovanja. Za primjer se mogu uzeti podvorbene stege FIFO i SPT. FIFO ili first in first out (hrv. prvi unutra prvi van) je način posluživanja bez prioriteta, odnosno korisnike se poslužuje na temelju tko je prvi stao u rep sustava. Ovakav način posluživanja provodi se na primjer na blagajnama u trgovinama. Ovo je dobar način posluživanja u slučajevima gdje korisnicima, u ovome slučaju pacijentima, vrijeme provedeno čekajući u redu nije od presudne važnosti. SPT ili Shortest Processing Time (hrv. Najkraće vrijeme posluživanja) je način posluživanja gdje se prednost daje onom korisniku čije će posluživanje najkraće trajati. Ova podvorbena stega ima najmanje repove ali nije prikladna u organizacijama kao što su bolnice. Razlog tomu je što je vrijeme potrebno za dijagnozu često proporcionalno težini oboljenja. Drugim riječima, duže treba liječniku da utvrdi da se radi o ozbiljnijoj bolesti nego o lakšoj, a pritom bi ozbiljnija bolest trebala imati prednost kako ne bi dovela do smrtnog slučaja. Stoga, vođenje zdravstvene ustanove na temelju SPT podvorbene sprege nije poželjno [24].

Drugi način utjecaja na smanjenje repova jest smanjenje prosječnog vremena posluživanja uz očuvanje kvalitete pružene usluge. Povećanje učinkovitosti poslužitelja može se postići na više načina:

- automatiziranje procesa posluživanja ,
- smanjivanje trajanja posluživanja zbog izdvajanja poslova poslužitelja koje treba obavljati korisnik ,
- neke djelatnosti poslužitelja premjestiti korisniku ,
- posluživanje istodobno više korisnika ,

- posluživanje korisnika u skupinama ,
- izmjenjivanje vrsta korisnika [24].

Svi ti načini smanjenja čekanja djelovanjem na proces posluživanja mogu se kvantitativno obraditi s pomoću teorije podvorbenih sustava. Zbog kompliciranosti problema, tu se često rabe grafičke metode i aproksimacije [24].

Također je bitno za napomenuti da je sa IoT tehnologijom moguće bilježiti podatke o kretanju zaposlenika. Ovi podaci su bitni za prikupljanje ukoliko menadžment želi uvid u rad ustanove po pitanju ljudstva. Na temelju toga mogu se donijeti odluke o raspoređivanju medicinskog osoblja po različitim odjelima, ali se može steći i uvid o radnim navikama zaposlenika.

4.1.3. Mane implementacije IoT-a sa stajališta menadžmenta

Ukoliko se napravi korak nazad i pritom se vrati sa optimizacije osoblja, opreme i uređaja, dolazi se do teme mana implementacije IoT-a sa pogleda menadžmenta. Glavne mane su:

a) Sigurnost i privatnost,
b) Tehnička složenost,
c) Povezanost i ovisnost o snazi,
d) Integracija,
e) Zahtjevno i skupo za provedbu [25].

4.1.3.1. Sigurnost

Razvoj i primjena IoT uređaja je svakim danom sve veća. Proporcionalno njihovoj primjeni raste zahtjevnost održavanja sigurnosti prikupljenih i prenesenih podataka. To je zahtjevan zadatak i veliki izazov za stručnjake koji se njime bave. IoT uređaji nisu uvijek uključeni u strategiju kibernetičke sigurnosti i to je problem. Oni moraju biti zaštićeni sa različitih aspekata:

- zaštićeni od fizičkog korištenja neovlaštenih osoba
- zaštićeni od hardverskih napada
- zaštićenih od softverskih napada koji dolaze sa interneta i
- zaštićeni od mrežnih napada [25].

4.1.3.2. Privatnost

Održava li se sigurnost IoT uređaja, kao i prikupljenih i prenesenih podataka na potrebnoj razini osigurava se privatnost podataka. Privatnost je imperativ svakog korisnika. IoT uređaji se koriste u područjima djelovanja koje barataju sa delikatnim informacijama i podacima. To su u prvom redu područje financija i zdravstva. Činjenica da se u zemljama razvijenog dijela svijeta doneseni zakoni o privatnosti podataka govori koliko je to važna problematika. I ne djeluju smo na lokalnoj razini unutar pojedinih država već također stupaju na snagu na globalnoj razini sugerirajući nam da je održavanje privatnosti podataka postao globalni problem [25].

4.1.3.3. Tehnička složenost

U velikim tvrtkama je često potrebno provesti integriranje protokola šifriranja i zaštite s IoT uređajima sa velikom flotom uređaja. Zbog složenosti i opsega ovakvog posla, troškovi vremena, truda i novca mogu biti vrlo veliki. To je razlog da tvrtke ovaj trošak zamjenjuju manjim koristeći neadekvatne jeftinije ili besplatne platforme. Činjenica je da će takvo poduzeće nakon samo jednog prekršaja naučiti, dakle na svojoj koži, tešku lekciju. Za lakšu i kvalitetniju implementaciju IoT uređaja bitno je razviti strategiju kako, zašto i gdje ih rasporediti. Time će se između ostalog, osigurati sigurnost njihovog rada i njihova podrška. Često se na prvi pogled čini da IoT uređaji izvode jednostavne i banalne zadatke, poput brojanja prolazaka kroz sigurna vrata. Međutim u njihovo stvaranje uključena je vrlo složena tehnologija, a zadatak im je vrlo bitan iako se čini bazičan. Ako ovi uređaji daju podatke drugom sustavu, mogli bi posredno utjecati na podatke tog sustava i na sve što je sa njim povezano [25].

4.1.3.4. Povezanost i ovisnost o snazi

Za ispravno funkcioniranje mnogih IoT uređaja osim neprekidnog napajanja električnom energijom važna je i internetska povezanost. Prestankom napajanja električnom energijom ili prekidom veze sa internetom uređaji prestaju sa radom i prekidaju komunikaciju i rad sa svime sa čime su bili povezani. To za posljedicu ima djelomični ili potpuni prekid rada tvrtke u kojoj su postavljeni. Zbog tog bi tvrtke koje koriste IoT uređaje trebale proaktivno planirati prekide. Prekid je neminovna pojava. Dogodit će se kad-tad. Pravilnom pripremom posljedice prekida će se ublažiti. Pravilna provedba procesa rješavanja problema i upravljanja incidentima osigurat će zaposlenicima znanje što učiniti kada uređaji iznenada prestanu sa radom [25].

4.1.3.5. Integracija

Za funkcioniranje IoT protokola i standarda različitih proizvođača ne postoji konsenzus. To znači da uređaji različitih proizvođača najvjerojatnije neće raditi sa istom postojećom tehnologijom. Svaki od njih može zahtijevati različite konfiguracije i hardverske veze. To otežava učinkovito raspoređivanje uređaja. Zbog tog, tvrtka mora razumjeti mrežne potrebe kako bi se lakše i brže prilagodila situaciji. Također, bitno je planiranje dodatnog vremena s implementacijama uređaja za rješavanje problema koji mogu nastati. Takvim kvalitetnim planiranjem zasnovanom na znanju i iskustvu struke smanjit će se vrijeme i troškovi obavljanja posla te će se povećati konkurentnost na tržištu [25].

4.1.3.6. Zahtjevno i skupo za provedbu

Uvođenje IoT uređaja u ovisnosti o veličini tvrtke koja će ih koristiti može biti tehnički, vremenski vrlo zahtjevan a time i skup proces. Ovaj proces uključuje:

- broj uređaja koje treba kupiti i konfigurirati
- stručnjaci koji će ih instalirati

- stručnjaci koji će ih integrirati u mrežu i podržati pozive proizvođaču za pomoć.

Simultani zajednički i usklađen rad svih sudionika u ovom procesu osigurat će kvalitetniju a jeftiniju investiciju. Pritom treba imati u vidu bude li se posao tvrtki širio, može se očekivati da će trošak eksponencijalno rasti. Kvalitetnom organizacijom eliminirat će se eventualne prepreke s kojim se moguće susresti. Zato je važno planiranje proračuna i strategije prije kupnje IoT uređaja. Iako na prvi pogled vrlo zahtjevna i skupa provedba uvođenja IoT uređaja, može biti vrlo korisna ali samo ako tvrtke točno znaju u što se upuštaju. Uz malo planiranja, tvrtke će imati bolju predodžbu o tome što im treba i kako IoT uređaji mogu pomoći [25].

4.2. Prednosti i mane implementacije IoT-a sa stajališta zaposlenika

Uvođenjem IoT-a u poslovanje ne profitiraju samo tvrtke već i njihovi zaposlenici. Jedna od prednosti koje ostvaruju je na primjer, povećanje učinkovitosti. To može značiti da će zaposlenici moći posao brže i kvalitetnije obaviti ili da će imati manje određenog posla. Primjer smanjenja količine posla bi na primjer bilo prikupljanje podataka (tlak, temperatura, broj otkucaja srca…), o stanju pacijenta. Primjenom IoT uređaja neka mjerenja bi mogli pacijenti samostalno izvršiti ili bi taj uređaj olakšao i ubrzao posao medicinskih djelatnika (medicinskih sestara i liječnika). Za ovaj primjer je također važno istaknuti da liječnici korištenjem sustava za prikupljanje podataka ne bi trebali prestati komunicirati i razvijati odnos sa pacijentom u kvalitativnom smislu, već naprotiv ostalo bi im više vremena za kvalitetnije dijagnosticiranje. Važno je da liječnici prilikom korištenjem ovog sustava barataju sa točnijim podacima te tako mogu donositi bolje zaključke o pacijentu. Dakle, prednosti uvođenja IoT-a, ali i novih tehnologija općenito, za zaposlenike unutar zdravstvenog sektora su sljedeće mogućnost:

a) donošenja boljih poslovnih odluka – dijagnoza se može postaviti brže i ona može biti točnija jer se temelji na većem broju podataka
b) povećanja produktivnosti – kao posljedica kvalitetnije raspodjele i iskorištenosti radnog vremena liječnika i drugih zdravstvenih djelatnika

c) uštede vremena i resursa – kvalitetnim iskorištavanjem uređaja uštedit će se vrijeme svih korisnika zdravstvenog sustava, omogućit će se brža i bolja dijagnostika, a time posljedično i adekvatnije liječenje
d) poboljšanja korisničkog iskustva svih sudionika zdravstvenog sustava
e) financijska dobit - kao posljedica kvalitetnijeg liječenja i povećanja broja ozdravljenja, poboljšanja korisničkog iskustva i boljih poslovnih odluka u konačnici smanjuje se vjerojatnost tužbi od strane pacijenata i povećava otvorenost velikih donatora [21].

Kako bi se ostvarile navedene prednosti koriste se različite nove tehnologije koje se razvijaju usporedno sa razvojem suvremene medicine i zdravstva.

IoT uređaji smanjuju velik dio ručnog rada, što liječnik ili medicinska sestra moraju obaviti tijekom dijagnosticiranja i kontroliranja pacijenta dok je on hospitaliziran. IoT senzori mogu mjeriti sve vrste podataka kao što su na primjer krvni tlak i tjelesna temperatura. Svi dobiveni podaci mogu se ucrtati u aplikaciju povezanu na uređaje za mjerenje putem IoT-a. To čini podatke o pacijentu lako dostupnim za stručni pregled i analizu. Takva IoT aplikacija mogla bi uštedjeti do 15 sati tjedno na liječničkom priručnom mapiranju [21].

Prilikom primjene IoT-a u zdravstvu važno je simultano izvještavanje, praćenje odgovarajućeg asortimana podataka i analiza dobivenih podataka.

U slučaju hitne medicinske pomoći praćenje u stvarnom vremenu putem povezanih uređaja može spasiti milijun života u situacijama poput zatajenja rada srca, dijabetesa, napada astme i drugih sličnih bolesti. Povezani IoT uređaj prikuplja i prenosi zdravstvene podatke kao što su podaci o krvnom tlaku, kisiku i razinama šećera u krvi, težini i EKG-ima. Uz praćenje stanja u stvarnom vremenu pomoću pametnog medicinskog uređaja povezanog s aplikacijom za pametni telefon, povezani uređaji mogu prikupljati i druge različite korisne medicinske i zdravstvene podatke. Prikupljeni podaci se pohranjuju u oblaku i mogu se podijeliti s ovlaštenom osobom prema ovlaštenju za pristup dijeljenju. Spomenuta osoba može biti liječnik, osiguravajuće društvo, zdravstvena tvrtka koja sudjeluje ili vanjski savjetnik i omogućit će joj uvid u prikupljene podatke bez obzira na njihovo mjesto i vrijeme.

Upravljanje golemom količinom podataka za zaposlene i poslom okupirane zdravstvene djelatnike nije tako lako kako zvuči. Podaci prikupljeni u stvarnom vremenu putem mobilnih uređaja s omogućenom IoT-om mogu se analizirati i razdvojiti kroz rješenja za mobilnost koja pokreće IoT. To će smanjiti prikupljanje sirovih podataka i može pokrenuti vitalnu zdravstvenu analitiku i uvide koji se temelje na podacima, što će u konačnici smanjiti pogreške i ubrzati donošenje odluka [21].

Mane za zaposlenike nisu mnogobrojne ali nisu ni zanemarive. One uključuju mogućnost praćenja radnog osoblja, krađu podataka o njima, te na temelju provedenih analiza podataka o radu mogućnost dobivanja otkaza.

4.3. Prednosti i mane implementacije IoT-a sa stajališta korisnika

Praćenje i upozorenja u stvarnom vremenu u situacijama opasnim po život iznimno su dragocjena za korisnika. Stalnim obavijestima i upozorenjima u stvarnom vremenu za pravilno praćenje, analizu i dijagnozu može se zaštititi i spasiti zdravlje kritičnog pacijenta. Rješenja za zdravstvenu mobilnost pokrenuta IoT-om omogućuju praćenje, upozoravanje i nadzor u stvarnom vremenu. To omogućuje praktično liječenje, bolju preciznost i prikladnu intervenciju liječnika, što poboljšava kompletne rezultate pružanja njege pacijenta.

Vrlo je neugodna situacija za pacijenta koji traži liječničku pomoć, ali se ne može povezati s liječnikom zbog različitih razloga kao na primjer: nedostupnost mjesta pacijenta, nedostatak znanja i nesposobnosti kod vrlo starih i nemoćnih osoba, neradni dani i slično. Ovakve situacije našle su odgovor u rješenjima za mobilnost omogućenima IoT-om koji pacijentima mogu pomoći u pružanju odgovarajuće medicinske pomoći u pokretu.

Pacijenti mogu također, uzimati liječničke recepte kod kuće putem lanaca pružanja zdravstvene zaštite koji su povezani s pacijentima putem IoT uređaja [21].

S potrebom olakšavanja svakodnevnog života konstantno se razvijaju nove naprave koje imaju mogućnost povezivanja s internetom ili drugim uređajima u svojoj okolini. Nosivi uređaji poput pametnih satova su bili među prvima koji su se pojavili na tržištu i nudili navedene pogodnosti. Kada se te mogućnosti uvedu u svrhu stalnog nadzora zdravstvenog

stanja pojedine osobe dolazi se do termina mobilno zdravstvo. Mobilno zdravstvo je izuzetno važno za razvoj osjećaja sigurnosti bolesnih i nemoćnih osoba te bi trebalo postati imperativ svakog suvremenog društva.

IoT aplikacije u zdravstvu nisu namijenjene samo zdravstvenim ustanovama, već i pacijentima. Prednosti koje pacijenti mogu primijeniti sa implementacijom IoT-a su:

- Smanjeno vrijeme čekanja u bolnicama
- Udaljeno praćenje stanja pacijenata
- Olakšana briga o uzimanju lijekova

Te se prednosti ne mogu ostvariti bez implementacije različitih vrsta IoT uređaja, kako u zdravstvenom sustavu tako i u pacijentovom okruženju [21].

Inovativni mHealth pametni dozator tableta dviju tvrtki MedMinder i Thales prikazan na slici 1, značajno poboljšava upravljanje lijekovima. Uređaj je namijenjen bolesnicima za svrhu podsjećanja i olakšanog vođenja evidencije o redovitosti uzimanja propisanih lijekova. Također, liječnici, medicinske sestre i drugi ovlašteni njegovatelji mogu se prijaviti na MedMinder – ovo web sučelje kako bi u stvarnom vremenu promatrali pridržavanje lijekova i intervenirali kad je potrebno [26].

Oni tvrde da je MedMinder – ov uređaj prvo povezano rješenje takve vrste koje nudi usklađenost s Zakonom o prenosivosti i odgovornosti za zdravstveno osiguranje (engl. The Health Insurance Portability and Accountability Act), poznatim pod akronimom HIPAA, koji uz sigurnu povezanost i šifriranje koje omogućava Thalesova tehnologija Cinterion® omogućuje:

- Praćenje i izvještavanje o unosu lijekova na poslužitelj zasnovan na oblaku (engl. Cloud),
- Slanje upozorenja,
- Slanje narudžbe za dopunu,
- Poboljšava poštivanje strogog određivanja vremena uzimanja lijekova [26].

Slika 1. Pametni dozator tableta

Izvor: [26]

Mjerač glukoze, koji se naziva i glukometar, medicinski je uređaj za određivanje približne koncentracije glukoze u krvi. Broj oboljelih od dijabetesa porastao je sa 108 milijuna 1980. na 422 milijuna 2014. godine, a 1,5 milijuna smrtnih slučajeva izravno se pripisuje dijabetesu svake godine [27]. Ova vrsta uređaja je nužna u dijagnosticiranju boluje li netko od te bolesti.

TouchCare Slim CGM, prikazan na slici 2, je sustav za kontinuirano mjerenje glukoze u realnom vremenu. On svake 2 minute, 720 puta dnevno, pruža podatke o izmjerenoj razini glukoze u krvi. Time se dobivaju podaci u realnom vremenu. Strelice trendova prikazuju smjer kretanja glukoze, a alarmi za glukozu upozoravaju na nagle promjene te niske i visoke vrijednosti glukoze u organizmu [28].

Odašiljač za mjerenje glukoze prima podatke o vrijednosti glukoze iz senzora. Podaci se mogu učitati na pametni uređaj nakon određenog razdoblja ili se može držati senzor stalno povezanim s pametnim uređajem i iskoristiti mogućnosti očitanja podataka u stvarnom vremenu. Mobilna aplikacija EasySense za TouchCare Slim CGM sustav dostupni su za Android (Google Play) i za iOS (AppStore) čineći ih dostupnim izuzetno velikom broju uređaja i korisnika [28].

Slika 2. TouchCare Slim CGM sustav za kontinuirano mjerenje glukoze u realnom vremenu

Izvor: [29]

Može se reći da su ti uređaji danas pioniri po pitanju uvođenja IoT-a u područje zdravstva. Pametni satovi su korisnicima vrlo poželjni zbog široke palete svojih mogućnosti od praćenja sportskih aktivnosti do mogućnosti izrade EKG-a što nadalje prikazano na slici 3. Po pitanju zdravstva odlični su jer nisu nametljive poput uređaja za automatsko mjerenje glukoze u krvi pa su time korisnici često otvoreniji prema njihovom korištenju.

Glavna prednost korištenja pametnog sata po pitanju zdravstva su promoviranje zdravog života kroz gibanje, redoviti unos vode i uredan ritam spavanja. Međutim, korištenjem modela pametnih satova koji pružaju dodatne funkcionalnosti po pitanju prikupljanja podataka o korisnikovom zdravstvenom stanju potencijalno se može ranije doći do točnijih rezultata, odnosno dijagnoze poremećaja ili bolesti.

Slika 3. Pametni sat sa mogućnošću izrade EKG-a

Izvor: [30]

Glavne mane korištenja uređaja s mogućnošću povezivanja s drugim uređajima i mrežama općenito tiču se sigurnosti, „sposobnost ili mogućnost biti siguran – biti oslobođen od opasnosti“ [31], i privatnosti, nečije pravo da čuva svoje osobne stvari, podatke i odnose u tajnosti [32], korisničkih podataka. Te mane su dodatno naglašene kada se govori o uvođenju takvih tehnologija u područje zdravstva gdje je sigurnost i privatnost korisničkih osobnih zdravstvenih podataka od iznimnog značaja.

4.4. SWOT analiza implementiranja IoT tehnologije u sustav zdravstva

SWOT analiza je analiza snaga (engl. Strengths), slabosti (engl. Weaknesses), mogućnosti (engl. Opportunities) i prijetnji (engl. Threats) i predstavlja okvir koji se koristi za procjenu konkurentske pozicije tvrtke i razvoj strateškog planiranja. SWOT analiza procjenjuje unutarnje i vanjske čimbenike, kao i sadašnji i budući potencijal [33].

Ona je osmišljena kako bi omogućila, temeljen na činjenicama dobiveni, iz prikupljenih podataka, realističan pogled na prednosti i slabosti organizacije ili unutar svoje industrije.

Svaka analiza trebala bi biti što točnija i usredotočena kontekst stvarnih događanja. Pri tom je nužno izbjegavati unaprijed zamišljena uvjerenja. Tvrtke bi je trebale koristiti kao vodič za daljnje planiranje. SWOT analiza sastoji se od:

- Snage – opisuju u čemu se organizacija ističe i što je odvaja od konkurencije: snažan brand, baza lojalnih kupaca, snažna bilanca, jedinstvena tehnologija itd. Na primjer, hedž fond je možda razvio vlasničku strategiju trgovanja koja vraća rezultate koji su pobijedili tržište. Zatim mora odlučiti kako će koristiti te rezultate za privlačenje novih ulagača.
- Slabosti – sprječavaju organizaciju da radi na optimalnoj razini. To su područja u kojima se poslovanje mora poboljšati da bi ostalo konkurentno: slaba marka, promet veći od prosjeka, visoka razina duga, neodgovarajući lanac opskrbe ili nedostatak kapitala.
- Prilike – odnose se na povoljne vanjske čimbenike koji bi organizaciji mogli dati konkurentsku prednost. Na primjer, ako neka zemlja smanji carine, proizvođač automobila može izvesti svoje automobile na novo tržište, povećavajući prodaju i tržišni udio.
- Prijetnje – odnose se na čimbenike koji mogu naštetiti organizaciji. Na primjer, suša prijeti tvrtki koja proizvodi pšenicu jer može uništiti ili smanjiti prinos usjeva. Druge uobičajene prijetnje uključuju stvari poput povećanja troškova materijala, povećanja konkurencije, ograničene ponude radne snage. i tako dalje [33].

U skladu sa svime do sada napisanim tablica 3 predstavlja SWOT analizu implementiranja IoT tehnologije u zdravstvo.

Tablica 3. SWOT analiza implementiranja IoT tehnologije u zdravstvo

Snage	**Slabosti**
Ostvarivanje konkurentske prednosti Bolja kvaliteta liječenja Smanjuje redove čekanja Bolji nadzor zdravstvenog stanja pacijenata Bolji nadzor nad radom organizacije Ostvarivanje većeg profita Ušteda vremena i resursa Poboljšanje korisničkog iskustva Brendiranje na tržištu	Skupa implementacija Skupo održavanje Mogući gubitak radnih mjesta Osjetljivost na gubitak električne energije Nedovoljno znanje o korištenju Povećanje kompleksnosti sustava
Prilike	**Prijetnje**
Prikupljanje veće količine podataka o stanju pacijenata radi daljnjih analiza Mogućnost bolje logističke organizacije Mogućnost donošenja boljih poslovnih odluka Daljinski nadzor rada opreme Mogućnost dolaska do novih saznanja na području znanosti	Osjetljivost na hakerske napade Gubitak korisnika zbog ne prihvaćanja mogućnosti izlaganja privatnih podataka hakerskim napadima Neovlašteno prikupljanje podataka o korisniku

5. SIGURNOST I SIGURNOSNI INCIDENTI IOT TEHNOLOGIJE

Prema Steffenu Sorrellu, glavnom analitičaru u Juniper Researchu, IoT bi se mogao opisati, kao davatelj podataka digitalnih transformacija. Digitalna transformacija se može opisati kroz dva procesa. Prvi proces podrazumijeva povezivanje mnoštva uređaja koji pružaju puno upotrebljivih informacija. Nakon ovog, sljedeći proces je provođenje analitike kako bi se dobiveni podaci obradili, analizirali i pretvorili u dodanu vrijednost, odnosno postali korisni daljnjim korisnicima tih podataka [34].

Svakodnevni izazovi suvremenog društva naglašavaju važnost digitalne strategije za poslovnu otpornost. Pri tom se ne smije izgubiti iz vida činjenica da je svaka žurba rizična. Požurivanje uvođenja novih digitalnih tehnologija sa sobom nosi sigurnosni rizik zbog nedovoljno vremena za proučavanje i uvođenje prilagođenih i pravih sigurnosnih mjera kao odgovor na sigurnosne izazove koje nova tehnologija donosi [34].

5.1. Sigurnosni izazovi IoT tehnologije

Zakon o informacijskoj sigurnosti (NN79/07) iz članka broj 2 Republike Hrvatske govori da je informacijska sigurnost: „… stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda“ [35]. Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini dok su standardi informacijske sigurnosti organizacijske i tehničke procedure i rješenja namijenjena sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti [36].

Većina IoT uređaja izdvaja i prikuplja podatke iz vanjskog okruženja. To može biti pametni termostat, HVAC ili sustav grijanja ventilacije i klimatizacije (engl. Heating ventilation, and air conditioning), televizori, medicinski uređaji. Ali ponekad ti uređaji šalju prikupljene podatke u oblak bez ikakve enkripcije ili omogućavaju bilo kojoj neautoriziranoj osobi da se spoji na njega kao da je autorizirana za to. Kao rezultat toga, haker može dobiti pristup IoT uređaju, stječući nadzor nad njim i gdje će moći u najmanju ruku pristupiti ako ne i mijenjati

podatke koji su prikupljeni. Takav uređaj koji je pod vanjskom kontrolom može se koristiti za slanje lažnih signala, a ukoliko se radi o uređaju Internet medicinskih stvari (engl. Internet of Medical Things) skraćeno IoMT, to znači da može natjerati zdravstvene radnike na poduzimanje radnji koje mogu oštetiti zdravlje njihovih pacijenata. Takve scenarije omogućuju sigurnosni propusti, a trenutno ih IoT tehnologija ima više.

5.1.1. Slaba zaštita vjerodajnicama

Korištenje vjerodajnica, kombinacija korisničkog imena i lozinke, pouzdan je način ograničavanja neovlaštenog pristupa sustavu i podacima kojima on barata. Međutim, ukoliko su vjerodajnice previše općenite (primjer: korisničko ime: 'korisničkoime'; lozinka: 'lozinka') sustav postaje jako ranjiv. Još jedan problem koji se zna pojaviti na uređajima je takozvano tvrdo kodiranje vjerodajnica (engl. Hard coded credentials). Tvrdo kodirane vjerodajnice su one koje se nekriptirane nalaze zapisane unutar koda zahvaljujući čemu osobe koje znaju pristupiti tom kodu mogu lako ostvariti pristup tim informacijama, a time i samom sustavu. Zlonamjerni softveri Mirai i Reaper, koji su detaljnije objašnjeni u poglavlju 5.2.1., dobri su primjeri napada na sustave na temelju objašnjenog sigurnosnog izazova [34].

U siječnju 2020. ZDNet je detaljno objasnio kako je haker objavio popis vjerodajnica za Telnet za 515 000 poslužitelja, usmjerivača i IoT uređaja. Ovo izbacivanje lozinke dobiveno je korištenjem tvornički zadanih korisničkih imena i lozinki i pogađanjem jednostavnih prilagođenih lozinki. ZDNet je podijelio te informacije s istraživačima sigurnosti koji su obavijestili davatelje internetskih usluga početkom 2020 [34].

Rješenje ovog problema može se postići na razne načine. Neki od njih su da proizvođači IoT uređaja prilikom proizvodnje trebaju osigurati jedinstvene lozinke za svaki pojedini uređaj. Uklanjanje prakse tvrdo kodiranja vjerodajnica. Uređaji bi trebali sadržavati fleksibilne, sigurne zadane postavke i, posebno, neobavezne mehanizme poput složenosti lozinke, isteka lozinke, zaključavanja računa i jednokratne lozinke koja prisiljava korisnike da mijenjaju zadane vjerodajnice prilikom postavljanja uređaja. Mrežni upravitelji koji koriste prilagođena IoT Identity i Access Management rješenja imaju širok raspon značajki provjere autentičnosti uređaja kako bi smanjili izloženost IoT napadima pa u skladu s tim

mogućnostima trebaju provoditi testove za nove uređaje. Autentifikacija u dva ili više koraka, biometrijska autentičnost ili digitalni certifikati (pomoću infrastrukture javnog ključa) mogu osigurati da nitko ne može dobiti neovlašteni pristup povezanim uređajima [34].

Gartner napominje da je privilegirano upravljanje pristupom (PAM) za sve uređaje ključno za rješavanje IoT sigurnosnih problema i osiguravanje da IoT mreže ne mogu biti hakirane [34].

5.1.2. Nedostatak redovitih ažuriranja

Jedan od izvora IoT sigurnosnih rizika je i nesigurni softver ili firmware. Iako proizvođač može prodati uređaj koji je trenutno siguran, gotovo je neizbježno da će se s vremenom pojaviti nove ranjivosti na tim uređajima. Rješenje ovog problema nalazi se u redovitim ažuriranjima koja bi trebala biti dostupna u najkraćem mogućem roku od otkrivanja novih ranjivosti. Ipak, u usporedbi sa pametnim telefonima ili računalima koji redovito dobivaju automatska ažuriranja neki IoT uređaji i dalje se koriste bez potrebnih ažuriranja [37].

IoT proizvodi razvijaju se s ciljem lakoće upotrebe i povezivanja. Oni možda mogu biti sigurni u trenutku kupnje, ali od tog trenutka kada postanu dostupni na tržištu pitanje je vremena kada će hakeri pronaći nove sigurnosne probleme ili programske pogreške. Ako se ne poprave redovitim ažuriranjima, IoT uređaji s vremenom postaju izloženi napadima [34].

Kako bi se zlonamjerni softveri koji ciljaju na ovu slabost spriječili u budućnosti odgovorni proizvođači trebali bi uložiti dodatne napore kako bi u potpunosti osigurali ugrađeni softver ili firmware ugrađen u svoje uređaje. Također bi trebali kreirati i objavit sigurnosna ažuriranja za svoje IoT uređaje u najkraćem mogućem roku od kad se otkriju ranjivosti.

Poduzeća tada mogu pružiti kritična sigurnosna ažuriranja IoT uređaja na terenu ukoliko sami nisu razvili vlastito rješenje za sigurnosni problem. Upravitelji mreža također bi trebali obratiti posebnu pozornost na mehanizme ažuriranja koji bi trebali uključivati samo potpisana ažuriranja i šifrirane razmjene radi osiguravanja autentičnosti.

Također je važno za napomenuti unutar ovog konteksta da bi se neočekivana ažuriranja firmware morala izbjegavati jer su do sada naučila programere teškim lekcijama o važnosti dobro isplanirane strategije firmware over the Air (FOTA) [34].

Ne iznenađuje da kalifornijski i oregonski IoT zakoni o kibernetičkoj sigurnosti (na snazi od 1. siječnja 2020.) ili britanski Zakon o internetskoj sigurnosti IoT (2020.) zahtijevaju da IoT uređaji koji se prodaju na njihovim teritorijima budu opremljeni „razumnim sigurnosnim značajkama“, poput jedinstvenih lozinki , redovita sigurnosna ažuriranja i posebno otkrivanje ranjivosti [34].

5.1.3. Nesigurna sučelja

Svi IoT uređaji obrađuju i komuniciraju podatke. Za komunikaciju trebaju aplikacije, usluge i protokole, a mnoge IoT ranjivosti potječu iz nesigurnih sučelja. Povezani su s webom, API-em aplikacija, oblakom i mobilnim sučeljima i mogu ugroziti uređaj i njegove podatke. Uobičajeni problemi uključuju nedostatak ili nedovoljnu provjeru autentičnosti i autorizacije uređaja te slabu enkripciju ili nikakvu. Rješenja uključuju:

- Autentifikaciju uređaja. Koristi se za osiguravanje pristupa povezanom uređaju i podacima koje generira, samo ovlaštenim osobama i aplikacijama koje mogu dokazati da su ovlašteni.
- Digitalne certifikate. Omogućuju digitalnom entitetu (IoT uređaj, računalo itd.) siguran prijenos podataka ovlaštenim stranama. Certifikati X509 standardni su formati certifikata koje obično potpisuje pouzdano tijelo za izdavanje certifikata. Omogućuju jedinstveno prepoznavanje i provjeru svakog IoT uređaja [34].

Najbolji korak je u startu izgraditi aplikacije koristeći najnovije sigurnosne standarde i protokole. Različite politike, standardi, najbolje prakse i smjernice dostupni su iz različitih izvora kao što su ENISA i NIST.

- U Sjedinjenim Državama, Nacionalni institut za standarde i tehnologiju (NIST) objavio je u siječnju 2020. svoj drugi nacrt „Preporuke proizvođačima IoT uređaja: temeljne aktivnosti i osnovna sposobnost kibernetske sigurnosti uređaja“.

- Agencija Europske unije za mrežnu i informacijsku sigurnost (ENISA) aktivno doprinosi europskoj politici kibernetičke sigurnosti. ENISA će stvoriti okvir za certificiranje, posebno za IoT uređaje. ENISA je nedavno objavila „Dobre prakse za sigurnost IoT-a - životni ciklus sigurnog razvoja softvera“ (studeni 2019.). Ovaj dokument detaljno opisuje kako primijeniti sigurnost dizajniranim za IoT. Dolazi kao dodatak svojoj publikaciji iz 2017. godine o „Osnovnim sigurnosnim preporukama za IoT sigurnost“ [34].

5.1.4. Nedovoljna zaštita podataka po pitanju komunikacije i pohrane podataka

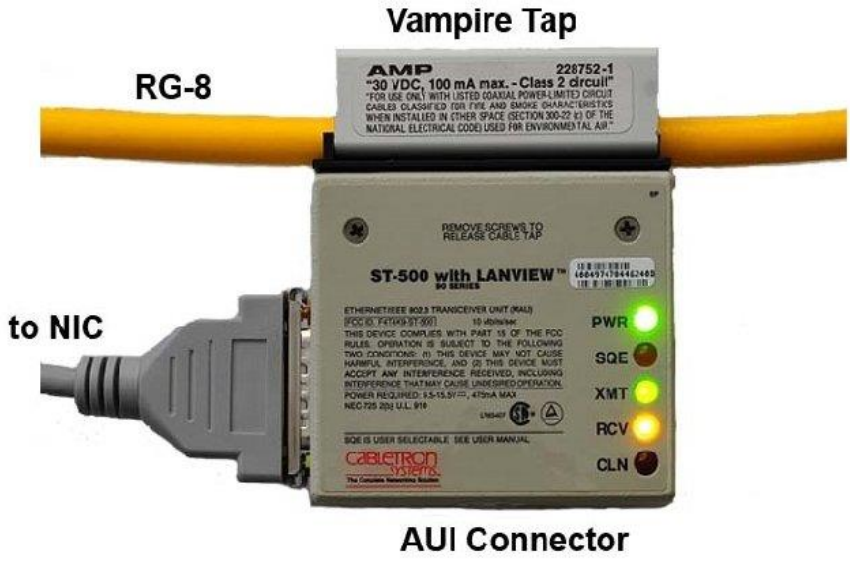
Problem nedovoljne zaštite podataka po pitanju komunikacije i pohrane podataka obuhvaća komunikaciju s mobilnog na mobilni uređaj, komunikaciju aplikacija-poslužitelj ili komunikaciju s mobilnog uređaja na nešto drugo. Ovaj rizik uključuje sve komunikacijske tehnologije koje mobilni uređaj može koristiti, a to su:

- TCP/IP,
- WiFi,
- Bluetooth/Bluetooth-LE,
- NFC,
- audio,
- infracrveno,
- 2G ili GSM,
- 3G ili UMTS,
- 4G ili LTE,
- 5G,
- SMS [38].

Istaknute karakteristike uključuju pakiranje neke vrste osjetljivih podataka i njihovo slanje po mreži sa ili prema nekom uređaju. Neki primjeri osjetljivih podataka uključuju ključeve za šifriranje, lozinke, privatne podatke o korisniku, pojedinosti o računu, tokene

sesija, dokumente, meta podatke i binarne datoteke. Definirajuća karakteristika ovog rizika je postojanje dva uređaja koji međusobno komuniciraju.

Uobičajeni rizici nesigurne komunikacije su oko integriteta podataka, povjerljivosti podataka i integriteta podrijetla. Dobar primjer ovog problema je ako se podaci mogu mijenjati tijekom tranzita, a da se promjena ne može otkriti (npr. Putem napada čovjeka u sredini). Ako se povjerljivi podaci mogu otkriti, naučiti ili izvesti promatranjem komunikacije koja se događa (tj. Prisluškivanjem), na primjer sa uređajem 'Vampire tap' prikazanom na slici 4, ili snimanjem razgovora kako se događa i napadom na njega kasnije (izvan mrežni napad), također predstavlja komunikacijski problem. Neuspješno postavljanje i provjeravanje TLS veze (npr. Provjera certifikata, slabe šifre, drugi problemi s konfiguracijom TLS -a) je još jedna stavka koja spada pod problem nesigurne komunikacije [38].



Slika 4. Vampire tap uređaj

Izvor slike: [39]

Iz navedenog jasno je vidljivo da je problem nesigurne komunikacije širok pojam koji obuhvaća velik broj 'manjih' problema koji su iz raznih razloga još uvijek dio komunikacijskih protokola.

Jedan od učinkovitih načina za rješavanje ovog problema je upotreba kriptografije. Kriptografija je znanstvena disciplina koja se bavi proučavanjem sigurnih komunikacijskih tehnika koje dopuštaju samo pošiljatelju i namjeravanom primatelju da pregleda njezin sadržaj kroz postupke šifriranja i dešifriranja [40]. Šifriranje i dešifriranje podataka osiguravaju očuvanje privatnosti i povjerljivosti podataka te umanjuje rizik od krađe podataka.

Kriptografija je i učinkovito rješenje protiv napada prisluškivanja (koristi se u industrijskoj špijunaži), poznatog i kao napadi njuškanja kada kibernetički kriminalac pasivno pristupa podacima dok oni propagiraju mrežom. Kriptografija je također standardna obrana od aktivnog prisluškivanja (tzv. Čovjek u sredini) u kojem haker presreće sve relevantne poruke i ubacuje nove između dva uređaja.

5.1.5. Loše upravljanje IoT uređajima

Studija objavljena u srpnju 2020. analizirala je preko 5 milijuna IoT-a, IoMT-a i neupravljanih povezanih uređaja u raznim industrijama. Izvještaj je otkrio uznemirujuće činjenice i trendove:

- Do 15% uređaja bilo je nepoznato ili neovlašteno.
- 5 do 19% koristilo je nepodržane stare operativne sustave.
- 49% IT timova nagađalo je ili se poigravalo sa svojim postojećim IT rješenjima kako bi postiglo vidljivost uređaja
- 51% njih nije bilo svjesno koje su vrste pametnih objekata aktivne u njihovoj mreži.
- 75% implementacija imalo je kršenja VLAN-a
- 86% primjena zdravstvene zaštite uključivalo je više od deset uređaja s kojih se opoziva FDA (Food and Drug Administration).

- 95% zdravstvenih mreža integriralo je uređaje Amazon Alexa i Echo uz bolničku opremu za nadzor [34].

Iz navedenih rezultata vidi se da organizacije imaju praksu lošeg upravljanja IoT uređajima na mreži. Od loših konfiguracija mreže do mogućnosti da se na nju spoje neautentificirani uređaji. Sve to olakšava hakerima da lakše pristupe mreži i naruše njezin rad. Ransomware napadi posebno ciljaju zdravstvo više od bilo koje druge domene u Sjedinjenim Državama. Prema Health IT security, napadi ransomware-a na pružatelje zdravstvenih usluga porasli su za 350% u Q4 (četvrtom tromjesečju) 2019, a 560 pružatelja zdravstvenih usluga postalo je žrtvom ransomware-a u 2020. godini. Istraživački rad Checkpoint-a objavljen krajem 2020. pokazao je da se prosječni broj dnevnih napada ransomware-a povećao za 50% u Q3 (treće tromjesečje) u odnosu na H1 (prva polovica) 2020 [34].
S obzirom da zaustavljanje kritičnih aplikacija i držanje podataka o pacijentima može ugroziti njihove živote i da je vjerojatnije da će te organizacije platiti otkupninu kako bi vratile ukradene podatke ili ostvarile pristup svojoj opremi nije čudno zašto ih kriminalci ciljaju.
Rezultati posljednjih napada na ransomware uključuju:

- prekid rada,
- ugroženi podaci i sigurnost kupaca,
- gubitak informacija, financijski gubici,
- reputacijska šteta [34].

Dobre vijesti su da se te ranjivosti i IoT sigurnosne prijetnje mogu radikalno smanjiti primjenom IoT platformi za upravljanje uređajima. One pružaju vodeće mogućnosti upravljanja životnim ciklusom u klasi za postavljanje, nadgledanje, održavanje, upravljanje i ažuriranje IoT uređaja. Time odgovaraju na potrebe kupaca za cjelovitim rješenjima i na ključne sigurnosne izazove s kojima se rješava upravljanje uređajima. Te vrste platforma mogu, na primjer, pomoći u poboljšanju osiguranja imovine, nadogradnji firmware-a, sigurnosnom zakrpavanju, dojavi upozorenja i izvještavanju o određenim mjernim podacima povezanim s IoT imovinom. Kombinacija takvih obavještajnih podataka može se pokazati vrlo učinkovitom u otkrivanju štetnih prijetnji i pronalaženju rješenja [34].

5.1.6. Nedostatak vještina sa IoT-om

Kroz godine služenja Internetom, njegovi korisnici usvojili su prakse izbjegavanja neželjene i phishing elektroničke pošte, phishing stranica izvršiti skeniranje virusa na svojim osobnim računalima i zaštititi svoje WiFi mreže i račune na online servisima jakom kombinacijom korisničkog imena i lozinke [37].

Za razliku od Interneta, IoT je nova tehnologija i ljudi još uvijek ne znaju puno o tome. Iako je većina rizika od IoT sigurnosnih problema i dalje na proizvodnoj strani, korisnici i poslovni procesi mogu stvoriti veće prijetnje. Jedan od najvećih IoT sigurnosnih rizika i izazova je neznanje i nedostatak svijesti korisnika o IoT funkcionalnosti.

Obmana čovjeka najčešće je najlakši način za pristup mreži. Vrsta IoT sigurnosnog rizika koji se često previđa su napadi socijalnog inženjeringa gdje umjesto da se ciljaju uređaji, haker cilja čovjeka i njegovo osobno ne znanje.

Socijalni inženjering korišten je u napadu Stuxnet 2010. na nuklearno postrojenje u Iranu. Napad je usmjeren na industrijske programabilne logičke kontrolere (PLC), koji također spadaju u kategoriju IoT uređaja. U napadu je oštećeno 1.000 centrifuga i elektrana je eksplodirala. Vjeruje se da je unutarnja mreža bila izolirana od javne mreže kako bi se izbjegli napadi, ali sve što je bilo potrebno jest da radnik priključi jedan neprovjereni USB u jedno od internih računala [37].

Čak i kada se riješe svi ostali problemi, bili oni spomenuti u ovom radu ili ne, ovaj će problem ostati ne rješiv u potpunosti. Za rješenje ovog problema postoji samo jedan lijek, naučiti nove korisnike što je to IoT i osnove o načinu rada s ciljem približavanja problematike, sigurnosti, te pružiti dodatnu naobrazbu za IT sektor tvrtke koji će uvijek ići u korak sa najnovijim prijetnjama. Korisnike također treba naučiti da iako je IoT nova tehnologija, ustaljene prakse vezane za Internet i tehnologiju općenito, od čega su samo neke oprez prilikom BYOD-a (bring your own device), snažna kombinacija korisničkog imena i zaporke i prepoznavanje pokušaja phishing napada, su izuzetno dobrodošle te smanjuju rizik od uspješnog provođenja napada.

5.1.7. Nedostatak fizičke zaštite

Jedna od prednosti pojedinih IoT uređaja je što bi oni nakon stavljanja u pogon trebali moći raditi autonomno, odnosno bez ikakve intervencije korisnika. To je odlična kvaliteta proizvoda ukoliko je njegova svrha prikupljati podatke sa od korisnika udaljenih i možda ne pristupačnih lokacija. Međutim, kako se radi o programibilnoj jedinici potrebno je uočiti potencijalnu opasnost od neovlaštenog ažuriranja softvera na uređaju putem na primjer USB-a s zlonamjernim softverom [37].

Osiguravanje fizičke sigurnosti IoT uređaja trebala bi početi od proizvođača na način da unaprijede dizajn uređaja sa dodatnim senzorima koji bi detektirali i na neki način dojavili da je došlo do ažuriranja softvera.. No, izgradnja sigurnih senzora i odašiljača u uređajima koji su idejno razrađeni da budu jeftini, izazovni je zadatak za proizvođače [37].

Drugo rješenje moglo bi se postići softverski korištenjem blockchain tehnologije. Ideja blockchain tehnologije je detektirati i najmanju promjenu u kodu u svrhu osiguravanja integriteta mreže. Na temelju te detekcije moguće je provesti zaključavanje pristupa te čak i isključivanja sigurnosno ugroženih uređaja iz IoT mreže.

5.1.8. Kripto rudarenje s IoT botnet mrežom

Rudarenje kriptovaluta zahtijeva kolosalne CPU i GPU resurse. S porastom performansi IoT uređaja postala je primamljiva pomisao kreiranja Botnet mreža u svrhu rudarenja kriptovaluta. Taj problem ima više manjih, ali ne i manje opasnih, problema [37].

Prvo to su softveri koji ne djeluju na sustav sa ciljem da se mreža učini nesposobnom za svoj rad već 'samo' smanjuje efikasnost sustava tako što se na tom sustavu provode za taj sustav nepotrebni procesi.

Drugo sama činjenica da se na toj mreži provode neovlašteni procesi poteže pitanje integriteta mreže i podataka. U slučaju kada bi jedna pametna bolnica bila inkriminirana sa botnet-om moralo bi se postaviti ozbiljno pitanje do kojih je sve sustava napadač ostvario

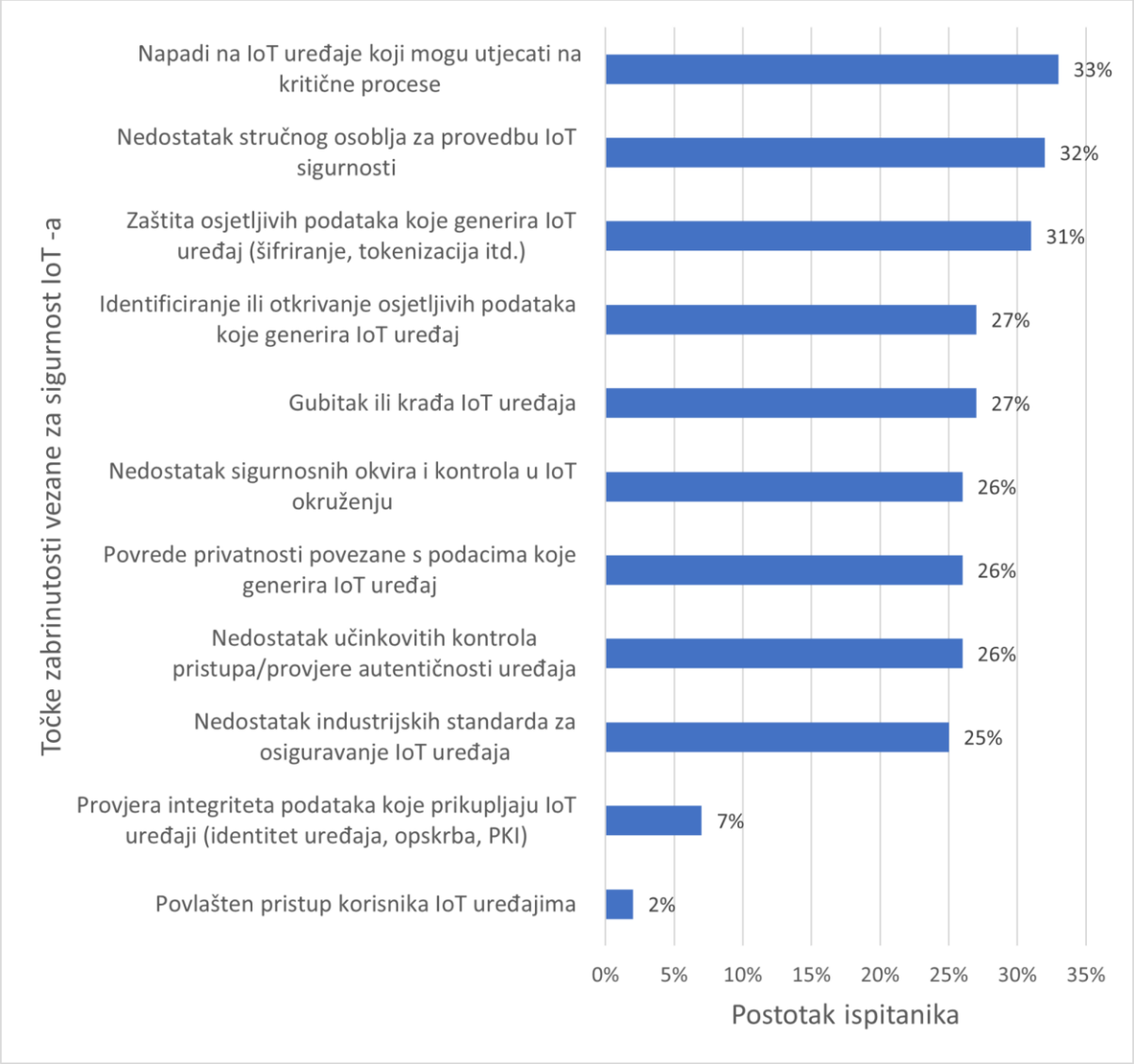
pristup te najvažnije je li narušena sigurnost korisničkih (u ovom primjeru zdravstvenih) podataka.

Treći problem je sama detekcija takvih softvera. S obzirom da napadač ostvaruje više prihoda što više vremena provede rudareći kriptovalute u interesu mu je da kreira što bolji softver po pitanju njegove neprimjetnosti na sustavu.

Prema Salad-u puno zlonamjernih softvera koristi iste izvršne datoteke zbog čega antivirusni programi tretiraju većinu rudarskih knjižnica kao zlonamjerne. Antivirusni programi zato preventivno blokiraju sve instance ovih izvršnih datoteka na računalu [41].

Pohvalno je što su navedenih problema svjesni i korisnici što je vidljivo i na provedenoj statistici Statiste prikazanoj na grafikonu 5. Ova statistika prikazuje koliki je postotak ispitanika potvrdilo svoju zabrinutost po pitanju aktualnih sigurnosnih problema IoT uređaja. Na grafikonu je vidljivo da više od 30 posto ispitanika ima zabrinutost po barem jednom pitanju od:

- napada na IoT uređaje koji mogu utjecati na kritične procese,
- nedostataka stručnog osoblja za provedbu IoT sigurnosti i
- zaštite osjetljivih podataka koje generiraju IoT uređaji [42].



Grafikon 5. Sigurnosne prijetnje i zabrinutosti Interneta stvari (IoT) diljem svijeta od kraja 2019

Izvor: [42]

5.2. Sigurnosni incidenti IoT uređaja

Cjelokupna strategija kibernetske sigurnosti mora imati za cilj zaštititi tri temeljna stupa koji podupiru povezane uređaje i usluge:

- Povjerljivost – zaštita informacija kod koje je potrebno spriječiti otkrivanje informacija od strane neovlaštenih osoba ili sustava.

- Integritet – Očuvanje integriteta podataka znači da korisnik podatke ne može izmijeniti bez odobrenja, tj. da su podaci potpuni i ispravni.
- Dostupnost – garancija ovlaštenim korisnicima da će im informacijski sustav biti na raspolaganju kada ga imaju potrebu koristiti [43].

Primjenom sigurnosnih opcija, poput rješenja za upravljanje uređajima i provjerom autentičnosti, temeljenih na tehnikama šifriranja, uz stručno znanje mobilizirano što je prije moguće, tvrtke mogu spriječiti neovlašteni pristup podacima, uređajima i softveru [34]. Međutim, kada organizacije zanemare sigurnost pitanje je vremena kada će im se dogoditi sigurnosni incident neke vrste.

U rujnu 2020. IBM X-Force izvijestio je da su IoT napadi koje smo promatrali od listopada 2019. do lipnja 2020. porasli 400% u usporedbi s ukupnim brojem IoT napada u prethodne dvije godine [44].

Nadzirani mrežni napadi koje smo prikupili pokazuju 500% porast ukupnih IoT napada iz godine u godinu. Istraživanje X-Force-a otkrilo je da je ovaj skok u velikoj mjeri posljedica aktivnosti Mozi botnet-a koji dijeli preklapanje koda s Mirai-em. U 2020. godini ovaj je zlonamjerni softver činio 89% ukupnih IoT napada otkrivenih za godinu dana [44].

5.2.1. Botnet napadi

Mirai botnet iz 2016. godine zarazio je velik broj raznih IoT uređaja. Od usmjerivača do video kamera i video snimača, uspješnim pokušajem prijave pomoću tablice od 61 uobičajena tvrdo kodirana zadana korisnička imena i lozinke ovaj zlonamjerni softver ostvario je pristup na preko 400 000 povezanih uređaja. U rujnu 2016. uređaji zaraženi Mirai zlonamjernim softverom korišteni su za pokretanje prvog svjetskog napada Distributed Denial-of-Service (DDoS) od čak 1Tbps na servere u središtu internetskih usluga čime se onemogućio pristup velikim dijelovima Interneta koji su uključivali GitHub, Netflix, Twitter, Reddit i Airbnb [34].

Djelomično zasnovan na Mirai softveru, Reaper je prvi put izašao na vidjelo krajem 2017. godine. Otkriveno je da je Reaper ugrozio između 20 000 i 30 000 uređaja koji se mogu koristiti za pokretanje DDoS napada. Arbor Networks kaže kako misli da je Reaper stvoren za tržište "DDoS na najam ", na kojem kriminalci mogu iznajmiti botnet mreže kako bi pokušali ukloniti one web stranice s kojima se ne slažu, koje im predstavljaju konkurenciju na tržištu ili zbog čijeg bi pada ostvarili neku drugu vrstu koristi [34].

Satori je još jedan zlonamjerni softver koji se širi i djeluje slično kao Mirai. Ovaj zlonamjerni softver isporučuje crva tako da se infekcija može širiti s uređaja na uređaj bez ljudske interakcije. Prvo, ne širi se samo pogađanjem vjerodajnica o kojima se već pričalo u prethodnom poglavlju, već je utvrđeno da cilja poznate ranjivosti u određenim dometima WiFi usmjerivača. Također otkriveno je da se Satori širi i na arhitekture pametnih procesora koje su IoT malware, SuperH i ARC ignorirali [34].

5.2.2. Napadi temeljeni na lošoj razini sigurnosti jednog uređaja

Istraživači iz Darktracea su 2017. godine otkrili sofisticirani napad na neimenovani kasino. U tom napadu hakeri su pristupili bazi podataka takozvanih 'Velikih potrošača' pristupivši mreži putem termostata pričvršćenog na akvarij. Jednom kad su se ubacili u mrežu, uspjeli su ostvariti pristup i preuzeti oko 10 GB podataka o korisnicima kasina [34].

Tehnički sličan incident u odnosnu na napad na kasino otkrila je Njemačka savezna mrežna agencija koja je klasificirala Caylu, prikazana na slici 5, kao "ilegalni aparat za špijunažu". Pristup toj dječjoj lutki putem Bluetootha bio je potpuno nesiguran, bez ikakve zaštite lozinkom čime se, s obzirom na brzu reakciju agencije samo potencijalno, mogla ugroziti dječja privatnost i sigurnost [45].

Slika 5. Zabranjena Lutka Cayla

Izvor: [45]

Par stručnjaka za kibernetičku sigurnost krenuli su 2015. godine u hakiranje potpuno novog Jeep-a Grand Cherokee-a koristeći njegov multimedijski sustav. Bili su uspješni. Pokazali su da se pomoću multimedijskog sustava mogu povezati s drugim softverom u vozilu, reprogramirati ga, a zatim kontrolirati motor, upravljač, kočnice, mjenjač i druge sustave čime su učinkovito pretvorili Jeep Grand Cherokee u automobil s daljinskim upravljačem [46].

Za sva tri slučaja kriva je nedovoljna zaštita po pitanju komunikacije ili pohrane podataka. Kao posljedica reklame koju su ti incidenti nanijeli, te praksa implementacije nižih ili nikakvih standarda zaštite od neovlaštenog pristupa najčešći je izvor zabrinutosti u sigurnost podataka IoT aplikacija.

5.2.3. Incident u sustavu zdravstva

Početkom 2017 godine CNN je napisao: „FDA je potvrdila da implantacijski srčani uređaji St. Jude Medical imaju ranjivosti koje bi hakeru mogle omogućiti pristup uređaju. Kad uđu, mogli bi isprazniti bateriju ili primijeniti pogrešan tempo ili šokove, rekla je FDA. Uređaji, poput pacemakera i defibrilatora, koriste se za nadgledanje i kontrolu rada srca pacijenta i prevenciju srčanog udara" [47].

Srećom, ovo je do sada jedini slučaj u sustavu zdravstva gdje je život pacijenata mogao biti direktno ugrožen da je neki haker uspješno proveo napad na navedeni uređaj prikazan na slici 6.

Slika 6. Pacemaker St. Jude Medical

Izvor: [48]

6. SPECIFIČNOSTI ZAŠTITE OSOBNIH PODATAKA U ZDRAVSTVU

Zdravstveni sustav raspolaže sa privatnim zdravstvenim podacima pojedinaca. Problem uvođenja IoT tehnologije u zdravstvo se očituje kroz činjenicu da njegovo korištenje sa trenutnim manjkavostima koje su spomenute u prethodnom poglavlju otvara novu površinu za hakerske napade. Prikupljeni podaci kojima se koristi zdravstveni sustav su često vrlo osobne prirode ili predstavljaju specifičnost pojedinca. Otkrivanje tih podataka zbog hakerskog napada moglo bi utjecati na kvalitetu života osoba čiji su podaci objavljeni. S druge strane hakerski napad može biti zloćudniji kada se njime zlonamjerno modificira rad IoT uređaja. Tako na primjer haker može narediti inzulinskoj pumpi da daje korisniku (pacijentu) inzulin krivim tempom ili u krivoj količini. Time se korisnika može dovesti u životnu opasnost. Osim tog doznavanje bilo kakve vrste tuđih podataka vrlo često je predmet ucjene. Zbog tog je potreba zaštite podataka od iznimnog značaja u zdravstvenom sustavu.

U Republici Hrvatskoj je zakonski regulirano pitanje hakerskih napada. Kaznena djela protiv računalnih sustava, programa i podataka definirana su Kaznenim zakonom (NN 125/2011) i to člancima 266. do 273 [49]. Osim kaznenog zakona važno je spomenuti i Zakon o elektroničkim komunikacijama (NN 73/2008) [50], Zakon o zaštiti osobnih podataka (NN 106/2012) [51] te uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) OJ L 119, 4.5.2016 (trenutno na snazi) [52].

6.1. Kazneni zakon

Kaznenim zakonom se, između ostaloga, definira kažnjivost neovlaštenog pristupa, ometanja rada računalnog sustava, oštećenja računalnih podataka, neovlaštenog presretanja računalnih podataka, računalnog krivotvorenja, računalne prijevare, zlouporabe naprava te počinjenja teških kaznenih djela protiv računalnih sustava, programa i podataka [49].

6.2. Zakon o elektroničkim komunikacijama

Prema članku 1 Zakona o elektroničkim komunikacijama uređuje se „…područje elektroničkih komunikacija, i to korištenje elektroničkih komunikacijskih mreža i pružanje elektroničkih komunikacijskih usluga, pružanje univerzalnih usluga te zaštita prava korisnika usluga, gradnja, postavljanje, održavanje i korištenje elektroničke komunikacijske infrastrukture i povezane opreme, uvjeti tržišnog natjecanja te prava i obveze sudionika na tržištu elektroničkih komunikacijskih mreža i usluga, adresiranje, numeriranje i upravljanje radio frekvencijskim spektrom, digitalni radio i televizija, zaštita podataka i sigurnost elektroničkih komunikacija te obavljanje inspekcijskog i stručnog nadzora i kontrole u elektroničkim komunikacijama, kao i osnivanje nacionalnog regulatornog tijela za elektroničke komunikacije i poštanske usluge, njegovo ustrojstvo, djelokrug i nadležnosti te postupak donošenja odluka i rješavanja sporova u elektroničkim komunikacijama“ [50].

Ovim se zakonom uglavnom propisuju pravilnici koje operatori i HAKOM (Hrvatska regulatorna agencija za mrežne djelatnosti) moraju poštivati i provoditi ali za tematiku ovog rada najbitniji su:

1. Članak 100 – vezan za Tajnost elektroničkih komunikacija i
2. Članak 108 – vezan za Tajni nadzor elektroničkih komunikacijskih mreža i usluga [50].

Članak 100 Zakona o elektroničkim komunikacijama vezan uz Tajnost elektroničkih komunikacija tako glasi:

1. „U svrhu osiguravanja tajnosti elektroničkih komunikacija i pripadajućih prometnih podataka u javnim komunikacijskim mrežama i javno dostupnim komunikacijskim uslugama, zabranjeno je slušanje, prisluškivanje, pohranjivanje te svaki oblik presretanja ili nadzora elektroničkih komunikacija i pripadajućih prometnih podataka, osim u slučajevima iz članka 108. ovoga Zakona te u slučajevima utvrđenima posebnim zakonima.“

2. „Zabrana iz stavka 1. ovoga članka ne odnosi se na tehničku pohranu podataka koja je nužna za prijenos komunikacije, ne zadirući pritom u načela zaštite tajnosti podataka.“

3. „Odredbe stavka 1. i 2. ovoga članka ne odnose se na zakonski ovlašteno bilježenje komunikacija i pripadajućih prometnih podataka tijekom zakonitih poslovnih radnja u svrhu pružanja dokaza o trgovačkim transakcijama ili drugim poslovnim komunikacijama.“

4. „Korištenje elektroničkih komunikacijskih mreža za pohranu podataka ili za pristup podacima pohranjenim u terminalnoj opremi pretplatnika ili korisnika usluga dopušteno je samo u slučaju kada je taj pretplatnik ili korisnik usluga dobio jasnu i potpunu obavijest u skladu s posebnim propisima o zaštiti osobnih podataka, i to osobito o svrhama obrade podataka, te ako mu je osoba zadužena za nadzor podataka omogućila pravo odbijanja takve obrade podataka. Time se ne može spriječiti tehnička pohrana podataka ili pristup podacima isključivo u svrhu obavljanja ili olakšavanja prijenosa komunikacija putem elektroničke komunikacijske mreže, ili, ako je to nužno, radi pružanja usluga informacijskog društva na izričit zahtjev pretplatnika ili korisnika usluga“ [50].

Članak 108 Zakona o elektroničkim komunikacijama vezan za Tajni nadzor elektroničkih komunikacijskih mreža i usluga glasi:

1. „Operatori javnih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga moraju o vlastitom trošku osigurati i održavati funkciju tajnog nadzora elektroničkih komunikacijskih mreža i usluga, kao i elektroničke komunikacijske vodove do operativno-tehničkog tijela nadležnog za nadzor elektroničkih komunikacija u skladu s posebnim zakonom kojim je uređeno područje nacionalne sigurnosti.“

2. „Obveze operatora javnih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga prema nadležnom tijelu iz stavka 1. ovoga članka i prema tijelima koja su ovlaštena za primjenu mjera tajnog nadzora elektroničkih komunikacijskih mreža i usluga, u skladu s posebnim zakonima iz područja nacionalne sigurnosti i kaznenog postupka, utvrđuju se

tim zakonima i posebnim propisom koji uređuje obveze operatora u području nacionalne sigurnosti.“

3. „Na obveze operatora javnih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga iz stavka 2. ovoga članka ne primjenjuju se odredbe članka 99. do 104. ovoga Zakona, niti odredbe posebnih propisa kojima je uređena zaštita osobnih podataka.“

4. „Operatori javnih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga moraju omogućiti nadležnim tijelima iz stavka 2. ovoga članka trenutačnu identifikaciju korisnika usluga“ [50].

6.3. Zakon o zaštiti osobnih podataka

Zakonom o zaštiti osobnih podataka uređuje zaštita osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka na području Republike Hrvatske. Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Zaštita osobnih podataka u Republici Hrvatskoj osigurava se svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište te neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama [51].

Ukoliko se izvršava postupak ekstrakcije podataka s nekog uređaja, vrši se obrada osobnih podataka. U skladu sa člankom 6. Zakona o zaštiti osobnih podataka, osobni podaci moraju se obrađivati pošteno i zakonito. Dakle podaci se mogu prikupljati u svrhu s kojom je fizička osoba upoznata te koja je u skladu sa Zakonom. Također se ne smije obrađivati više podataka nego što je to nužno. Jedna od najbitnijih stavki jest ta da, prije nego što se krene vršiti prikupljanje podataka, izvršitelj mora obavijestiti fizičku osobu da će se njegovi podaci prikupljati. Ovo se može ograničiti posebnim zakonima ako je riječ o nacionalnoj ili javnoj sigurnosti [51].

6.4. GDPR

Jedna od najbitnijih regulativa vezanih za zaštitu korisničkih podataka jest Opća uredba o zaštiti podataka (engl. General Data Protection Regulation) Europske Unije pod akronimom GDPR u kojima se definira na koji način su zaštićeni osobni podaci privatnih i pravnih osoba.

Prema članku 1 Opće uredbe o zaštiti podataka definirana je svrha uredbe kroz 3 točke: “

1. Utvrđuje pravila koja se odnose na zaštitu fizičkih osoba u pogledu obrade osobnih podataka i pravila koja se odnose na slobodno kretanje osobnih podataka.

2. Štiti temeljna prava i slobode fizičkih osoba, a posebno njihovo pravo na zaštitu osobnih podataka.

3. Slobodno kretanje osobnih podataka unutar Unije neće biti niti ograničeno niti zabranjeno iz razloga povezanih sa zaštitom fizičkih osoba u vezi s obradom osobnih podataka „ [52].

GDPR ne spominje eksplicitno IoT uređaje, a ne spominju ih niti nacionalni zakoni o primjeni. Međutim njihove uvodne izjave i odredbe odnose se na prikupljanje podataka putem IoT uređaja i pametnih kućnih uređaja. Tako se na primjer u uvodnoj izjavi br.6 Uredbe Europske komisije ,2016a, naglašava osviještenost postojećih i nadolazećih izazova u zaštiti osobnih podataka koji su nastali kao posljedica brzog globalnog tehnološkog razvoja. Naglašava se da je suvremena tehnologija promijenila ne samo neke segmente funkcioniranja gospodarstva nego i društveni život općenito omogućivši poslovnim subjektima baratanje osobnim podacima a fizičkoj osobi često nesmotrenu objavu osobnih podataka. Također se naglašava da osim blagodati koje nam pruža suvremena tehnologija ona bi morala osiguravati visoku razinu zaštite osobnih podataka [53].

Općenitije, može se reći da GDPR postavlja sedam ključnih načela:

1. Zakonitost, pravednost i transparentnost.

2. Ograničenje svrhe.

3. Minimizacija podataka.
4. Točnost.
5. Ograničenje skladištenja.
6. Integritet i povjerljivost (sigurnost)
7. Odgovornost [54].

U preporuci Europske komisije 2017. godine za pripreme za uvođenje strategija pametnog mjerenja izložena su također pitanja zaštite podataka i pitanja sigurnosti. Zakoni o zaštiti podataka zahtijevaju nekoliko smjerova promatranja sigurnosti u kontekstu IoT uređaja primijenjenih u pametnim kućama poput privatnosti prema dizajnu i prema zadanim postavkama, odgovarajuće analize i tretmana rizika do prava i slobode ispitanika, obrada u skladu s načelima obrade i na utvrđenim i propisno ocijenjenim pravnim osnovama. Obzirom na zahtjevnost i kompliciranost infrastrukture pametnih kuća može se reći da je integriran sigurnosni pristup, identifikacija rizika i postupanje, kao i odgovorno ponašanje voditelja obrade podataka i drugih pružatelja usluga od najveće je važnosti [53].

7. ZAKLJUČAK

Internet stvari, ili IoT, je tehnologija koja omogućuje prikupljanje enormno velikih količina podataka o okruženjima unutar kojih su postavljeni. Na temelju tih podataka mogu se postići razne prednosti u usporedbi sa sustavima koji nisu uveli IoT u svoje poslovanje. Glavne prednosti koje se mogu postići su povećanje učinkovitosti sustava, smanjeni redovi čekanja, bolje korisničko iskustvo, postavljanje temelja za rudarenje podataka te uštede na vremenu i resursima sustava.

Jedan od sustava koji radi prve korake prema uvođenju IoT tehnologije u svoj sustav je sustav zdravstva. Zdravstvo bi moglo uvelike beneficirati od velike količine podataka koju je IoT može prikupiti. Od toga da je sa većim brojem podataka potencijalno lakše napraviti pojedinačne dijagnoze za svakog pacijenta do toga da sa digitalizacijom tolike količine podataka na globalnoj razini uz pomoć rudarenja podataka i umjetne inteligencije se otvaraju vrata novim otkrićima na području medicine. Uvođenjem IoT-a u zdravstvo, ali i mnoge druge sektore otvorit će se novi sektor poslova vezanih za obradu i analizu prikupljenih podataka.

Iako je IoT tehnologija po mnogo čemu korisna, trenutno ona ima i mane koje negativno utječu na sveukupni dojam o toj tehnologiji. Najveća mana ove tehnologije je što se opravdano dovodi u pitanje sigurnost podataka koji se prikupljaju pomoću nje te se istim podacima može manipulirati ili ih se može prodavati na ilegalnom tržištu

S obzirom da se kroz nedavnu povijest dogodilo nekoliko incidenata gdje se preko IoT tehnologije ostvario pristup cijeloj mreži (u radu spomenuti slučaj kasina ili slučaj Jeep Grand Cherokee) jasno je da je prosječna osoba vrlo skeptična prema implementaciji IoT tehnologije u sustav koji barata njihovim osobnim podacima. Posebno je ta osjetljivost izražena kad su u pitanju zdravstveni podaci prikupljeni s ciljem učinkovitijeg liječenja u sustavu zdravstva.

Kako bi se promijenila ta stigma ne samo kod prosječnih korisnika i laika nego i među stručnjacima potrebno je uložiti dodatne napore u razvoju IoT tehnologije po pitanju sigurnosnih standarda barem do razine koja se ostvarila na klasičnim komunikacijskim mrežama kroz godine rada na raznim standardima, propisima, regulativama i zakonima.

LITERATURA

[1] F. Dian J; Vahidnia R; Rahmati A, Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey, Preuzeto sa: https://ieeexplore.ieee.org/document/9058658/references#references [Pristupljeno na datum: 10. kolovoz 2021.].

[2] Statista, Smartwatch unit sales worldwide from 2014 to 2017: https://www.statista.com/statistics/538237/global-smartwatch-unit-sales/ [Pristupljeno na datum: 10. kolovoz 2021.].

[3] Gillis A. S, What is internet of things (IoT)? https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT [Pristupljeno na datum: 10. kolovoz 2021.].

[4] Statista, Global spending on IoT in 2015 and 2020*, by industry sector https://www.statista.com/statistics/1095375/global-spending-on-iot-by-industry-sector/ [Pristupljeno na datum: 10. kolovoz 2021.].

[5] Statista, Annual value of the smart hospital market from 2018 to 2026 https://www.statista.com/statistics/1204318/smart-hospital-market-estimated-value-forecast/, [Pristupljeno na datum: 10. kolovoz 2021.]

[6] BehrTech, 6 Leading Types of IoT Wireless Tech and Their Best Use Cases https://behrtech.com/blog/6-leading-types-of-iot-wireless-tech-and-their-best-use-cases/, [Pristupljeno na datum: 10. kolovoz 2021.]

[7] BehrTech, What is LPWAN? https://behrtech.com/lpwan-technology/, [Pristupljeno na datum: 10. kolovoz 2021.]

[8] Leverege, IoT 101 An introduction to Internet of Things, Leverege LLC, 2018, Preuzeto sa: https://www.leverege.com/ebooks/iot-intro-ebook, [Pristupljeno 10. kolovoz 2021]

[9] Mekki K, Bajic E, Chaxel F, Meyer F, A comparative study of LPWAN technologies for large-scale IoT deployment, ICT Express, 2019, Preuzeto sa: https://doi.org/10.1016/j.icte.2017.12.005., [Pristupljeno na datum: 10. kolovoz 2021.]

[10] E-studnet: http://e-student.fpz.hr/Predmeti/O/Osnove_tehnologije_prometa/Materijali/Zadaci_s_vjezbi_iz_modula_Tehnologija_TK_prometa.pdf, [Pristupljeno na datum: 10. kolovoz 2021.]

[11] JT IoT blog, Top 5 Benefits of Cellular IoT https://blog.jtiot.com/top-5-benefits-of-cellular-iot, [Pristupljeno na datum: 10. kolovoz 2021.]

[12] Digi, Zigbee Wireless Mesh Networking https://www.digi.com/solutions/by-technology/zigbee-wireless-standard, [Pristupljeno na datum: 10. kolovoz 2021.]

[13] Zigbee alliance, Zigbee THE FULL-STACK SOLUTION INTERLACING ALL YOUR SMART DEVICES https://zigbeealliance.org/solution/zigbee/, [Pristupljeno na datum: 10. kolovoz 2021.]

[14] Terrell Hanna K, frequency-hopping spread spectrum (FHSS) https://searchnetworking.techtarget.com/definition/frequency-hopping-spread-spectrum, [Pristupljeno na datum 5. rujna 2021.]

[15] Gillis A. S, mesh network topology (mesh network), https://internetofthingsagenda.techtarget.com/definition/mesh-network-topology-mesh-network , [Pristupljeno na datum 9. rujan 2021]

[16] Link Labs, Bluetooth Vs. Bluetooth Low Energy: What's The Difference? https://www.link-labs.com/blog/bluetooth-vs-bluetooth-low-energy [Pristupljeno na datum: 10. kolovoz 2021.]

[17] Cisco, What Is Wi-Fi? https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html [Pristupljeno na datum: 10. kolovoz 2021.]

[18] Jia X, Feng Q, Fan T, Lei Q, RFID technology and its applications in Internet of Things (IoT). 2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012, Preuzeto sa: https://www.researchgate.net/publication/254032690_RFID_technology_and_its_applications_in_Internet_of_Things_IoT, [Pristupljeno na datum: 10. kolovoz 2021]

[19] Digiteum, The Role of RFID Technology and Internet of Things in Healthcare https://www.digiteum.com/rfid-technology-internet-of-things/ [Pristupljeno na datum: 10. kolovoz 2021.]

[20] Jurčević M, Autorizirana predavanja Tehnolgijski marketing i menadžment, Zagreb, 2009., Preuzeto sa: https://moodle.srce.hr/2020-2021/pluginfile.php/4416394/mod_resource/content/1/Skriptirana_predavanja.pdf, [Pristupljeno na datum: 10. kolovoz 2021.]

[21] Sheldon A, IoT in Healthcare: Benefits, Challenges and Applications https://www.valuecoders.com/blog/technology-and-apps/iot-in-healthcare-benefits-challenges-and-applications/#What_is_the_current_state_of_IoT_in_HealthCare, [Pristupljeno na datum: 10. kolovoz 2021.]

[22] Statista, Top benefits that companies realize through the use of data and analytics worldwide as of 2019 https://www.statista.com/statistics/895263/worldwide-barriers-effective-data-analytics-use/ [Pristupljeno na datum: 10. kolovoz 2021.]

[23] Wipro, What can IoT do for healthcare? https://www.wipro.com/business-process/what-can-iot-do-for-healthcare-/ [Pristupljeno na datum: 10. kolovoz 2021.]

[24] Pdfslide: https://pdfslide.net/documents/podvorbeni-sustavi.html [Pristupljeno na datum: 10. kolovoz 2021.]

[25] Borgini J, Top advantages and disadvantages of IoT in business: https://internetofthingsagenda.techtarget.com/tip/Top-advantages-and-disadvantages-of-IoT-in-business [Pristupljeno na datum: 10. kolovoz 2021.]

[26] Thales group, MedMinder makes Medication Smarter with IoT Connected Pill Box https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/customer-cases/smart-pill-dispenser [Pristupljeno na datum: 10. kolovoz 2021.]

[27] World Health Organization, Diabetes https://www.who.int/news-room/fact-sheets/detail/diabetes [Pristupljeno na datum: 10. kolovoz 2021.]

[28] Bauerfeind: https://cgm.hr/s7-easysense-cgm/ [Pristupljeno na datum: 10. kolovoz 2021.]

[29] Bauerfeind: https://cgm.hr/?gclid=Cj0KCQjwub-HBhCyARIsAPctr7w2-xAw7hB0nSIxJZ4a6Tjlr0RXEtbRhETLanUsmUkXRthnSrzbijcaArt4EALw_wcB [Pristupljeno na datum: 10. kolovoz 2021.]

[30] If world design guide, Samsung Health Monitor / Mobile blood pressure monitoring app https://ifworlddesignguide.com/entry/309576-samsung-health-monitor [Pristupljeno na datum: 10. kolovoz 2021.]

[31] Peraković D, Cvitić I, Nastavni materijali za kolegij: Sigurnost i zaštita informacijsko komunikacijskog sustava verzija dokumenta: 3.9.1, Sveučilište u Zagrebu Fakultet prometnih znanosti, Zagreb, 2020

[32] Cambridge Dictionary: https://dictionary.cambridge.org/dictionary/english/privacy [Pristupljeno na datum: 10. kolovoz 2021.]

[33] Investopedia, Strength, Weakness, Opportunity, and Threat (SWOT) Analysis https://www.investopedia.com/terms/s/swot.asp [Pristupljeno na datum: 10. kolovoz 2021.]

[34] Thales group, IOT SECURITY ISSUES IN 2021: A BUSINESS PERSPECTIVE https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats [Pristupljeno na datum: 10. kolovoz 2021.]

[35] Narodne novine: https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html [Pristupljeno na datum: 10. kolovoz 2021.]

[36] Republika Hrvatska, Ured vijeća za nacionalnu sigurnost: https://www.uvns.hr/hr/sto-su-to-mjere-i-standardi-informacijske-sigurnosti [Pristupljeno na datum: 10. kolovoz 2021.]

[37] Intellectsoft, Top 10 Biggest IoT Security Issues https://www.intellectsoft.net/blog/biggest-iot-security-issues/ [Pristupljeno na datum: 10. kolovoz 2021.]

[38] OWASP: https://owasp.org/www-project-mobile-top-10/2016-risks/m3-insecure-communication [Pristupljeno na datum: 10. kolovoz 2021.]

[39] Slide to doc, MEDIA TRANSMISI Secara garis besar ada dua kategori https://slidetodoc.com/media-transmisi-secara-garis-besar-ada-dua-kategori/[Pristupljeno na datum: 5. rujan 2021.]

[40] Kaspersky, Cryptography Definition https://www.kaspersky.com/resource-center/definitions/what-is-cryptography [Pristupljeno na datum: 10. kolovoz 2021.]

[41] Salad, Why Do Antivirus Programs Block Miners? https://salad.com/blog/why-do-antivirus-programs-block-miners/ [Pristupljeno na datum: 10. kolovoz 2021.]

[42] Statista, Internet of things (IoT) security threats and concerns worldwide as of late 2019, https://www.statista.com/statistics/1202640/internet-of-things-security-concerns/, [Pristupljeno na datum: 10. kolovoz 2021.]

[43] CIS: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-05-265.pdf [Pristupljeno na datum: 10. kolovoz 2021.]

[44] McMillen D, Internet of Threats: IoT Botnets Drive Surge in Network Attacks https://securityintelligence.com/posts/internet-of-threats-iot-botnets-network-attacks/ [Pristupljeno na datum: 10. kolovoz 2021.]

[45] Toybuzz, My Friend Cayla Doll Banned in Germany https://toybuzz.org/my-friend-cayla-doll-banned-in-germany/ [Pristupljeno na datum: 10. kolovoz 2021.]

[46] Kaspersky, Black Hat USA 2015: The full story of how that Jeep was hacked https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/ [Pristupljeno na datum: 10. kolovoz 2021.]

[47] IoT for all, The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities [Pristupljeno na datum: 20. prosinca 2020.].

[48] Davis J, Healthcare IT news, FDA to patients with St. Jude pacemakers: Update needed to keep hackers out of devices https://www.healthcareitnews.com/news/fda-patients-st-jude-pacemakers-update-needed-keep-hackers-out-devices [Pristupljeno na datum: 10. kolovoz 2021.]

[49] Narodne novine : https://narodne-novine.nn.hr/clanci/sluzbeni/2011_11_125_2498.html [Pristupljeno na datum: 2. kolovoz 2020.].

[50] Narodne novine: https://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html [Pristupljeno na datum: 10. kolovoz 2021.].

[51] Narodne novine: https://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html [Pristupljeno na datum: 5. kolovoz 2021.].

[52] GDPR: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32016R0679 [Pristupljeno na datum: 10. kolovoz 2021.]

[53] Vojkovic G, Milenkovic M, Katulić T. IoT and Smart Home Data Breach Risks from the Perspective of Croatian Data Protection and Information Security Law, 2019, Preuzeto sa: https://www.researchgate.net/publication/335828354_IoT_and_Smart_Home_Data_Breach_Risks_from_the_Perspective_of_Croatian_Data_Protection_and_Information_Security_Law, [Pristupljeno na datum: 10. kolovoz 2021.]

[54] Information Commissioner Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ [Pristupljeno na datum: 10. kolovoz 2021.]

POPIS KRATICA

IoT	Internet of Things, uređaji koji prikupljaju podatke iz svoje okoline i dijele ih sa svojom mrežom
LPWAN	širokopojasne mreže male snage
BLE	Bluetooth Low Energy, komunikacijski standard
RFID	Radio-frequency identification, komunikacijski standard
LoRa	Long Range, modifikacija LPWAN tehnologije
NB-IoT	Uskopojasni Internet stvari, modifikacija LPWAN tehnologije
NMT	Nordic Mobile Telephone, prva generacija mobilnih mreža
GSM	Global System for Mobile Communications, druga generacija mobilnih mreža
UMTS	The Universal Mobile Telecommunications System, treća generacija mobilnih mreža
LTE	Long Term Evolution, četvrta generacija mobilnih mreža
SIM	subscriber identification module (hrv. identifikacijski modul pretplatnika)
M2M	Machine to machine, komunikacija stroja sa strojem
QoS	Quality of Service (hrv. Razina kvalitete usluge)
VPN	Virtual Private Network (hrv. Virtualna privatna mreža)
APN	Access Point Name (hrv. Naziv pristupne točke)
IEEE	Institute of Electrical and Electronics Engineers (hrv. Institut inženjera elektrotehnike i elektronike)

RF	Radio frequency (hrv. Radio frekvencija)
IP	Internet Protocol (hrv. Internet protokol)
LAN	local area network (hrv. lokalna mreža)
WAN	wide-area network (hrv. Mreža širokog područja)
Mb/s	megabit per second (hrv. megabit po sekundi)
WiFi HEW	High-Efficiency WLAN (hrv. WLAN visoke učinkovitosti)
CT	protokol stabla interferencije
CO_2	ugljikov dioksid
FIFO	first in first out (hrv. prvi unutra prvi van)
SPT	Shrotest Processing Time (hrv. Najkraće vrijeme posluživanja)
mHealth	mobile Health (hrv. Mobilno zdravstvo)
HIPAA	Health Insurance Portability and Accountability Act (hrv. Zakon o prenosivosti i odgovornosti zdravstvenog osiguranja)
EKG	elektrokardiogram
SWOT analiza	analiza snaga (engl Strengths), slabosti (engl. Weaknesses), mogućnosti (engl. Opportunities) i prijetnji (engl. Threats)
HVAC	Heating, ventilation, and air conditioning (hrv. grijanje, ventilacija i klimatizacija)
IoMT	Internet of Medical Things (hrv. Internet medicinskih stvari)
FOTA	Firmware Over-The-Air (hrv. Firmware preko zraka)
API	Application Programming Interface (hrv. Sučelje za programiranje aplikacija)

ENISA	European Union Agency for Cybersecurity (hrv. Agencija Europske unije za kibernetičku sigurnost)
NIST	National Institute of Standards and Technology (hrv. Nacionalni institut za standarde i tehnologiju), nacionalni institut Sjedinjenih Američkih Država
NFC	Near-Field Communication, komunikacijski standard
SMS	Short Message Service (hrv. Usluga kratkih poruka)
TLS	Transport Layer Security, (hrv. Sigurnost transportnog sloja)
IT	Information technology, (hrv. Informacijske tehnologije)
VLAN	virtual LAN (hrv. Virtualni LAN)
FDA	Food and Drug Administration, Američka savezna agencija za hranu i lijekove
Q4	četvrto tromjesečje
Q3	treće tromjesečje
H1	prva polovica
PLC	programmable logic controller (hrv. Programabilni logički upravljač)
BYOD	Bring your own device (hrv. Ponesi vlastiti uređaj)
CPU	central processing unit (hrv. centralna procesorska jedinica)
GPU	graphics processing unit (hrv. grafička procesorska jedinica)
DDoS	distributed denial-of-service (hrv. distribuirano uskraćivanje usluge)
GB	Gigabyte
CNN	Cable News Network, multinacionalni televizijski kanal temeljen na vijestima

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

POPIS SLIKA

POPIS TABLICA

POPIS GRAFIKONA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako 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 diplomskog rada pod naslovom **Sigurnosni i regulatorni izazovi IoT-a u sustavu zdravstva**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 10.9.2021

E. Vojvodić
(potpis)