Zaštita od neovlaštenog prikupljanja osobnih podataka u IoT okruženju

Kos, Dino

Master's thesis / Diplomski rad

2022

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

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:816721

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Dino Kos

ZAŠTITA OD NEOVLAŠTENOG PRIKUPLJANJA OSOBNIH PODATAKA U IOT OKRUŽENJU

DIPLOMSKI RAD

Zagreb, 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 25. svibnja 2021.

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

DIPLOMSKI ZADATAK br. 6511

Pristupnik: **Dino Kos (0135224536)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Zaštita od neovlaštenog prikupljanja osobnih podataka u IoT okruženju**

Opis zadatka:

Danas se u mnogim područjima uvode različiti IoT uređaji od osobnih asistenata do raznih mjernih uređaja. Mnogi od tih uređaja prikupljaju vrlo širok opseg naših osobnih podataka, a često nisu na odgovarajući način zaštićeni. U radu je potrebno obrazložiti opasnosti za privatnost i osobne podatke od strane IoT uređaja, navesti tipične probleme i predložiti načine zaštite od neovlaštenog korištenja.

Mentor:

izv. prof. dr. sc. Goran Vojković

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

ZAŠTITA OD NEOVLAŠTENOG PRIKUPLJANJA OSOBNIH PODATAKA U IOT OKRUŽENJU

PROTECTION FROM UNAUTHORIZED PERSONAL DATA COLLECTION IN IOT ENVIRONMENT

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

Student: Dino Kos

JMBAG: 0135224536

Zagreb, veljača 2022.

SAŽETAK

Razvojem pametnih mobilnih uređaja te njihovim sve većim brojem i korištenjem, nailazi se na potrebu njihovog međusobnog povezivanja zbog velike količine podataka koja se na tim uređajima pohranjuje i obrađuje. Povezivanjem tih uređaja u cjelinu korisnicima se olakšava pristup podacima jer su samim time i podaci povezani u cjelinu. Tehnologija koja omogućava sve navedeno naziva se Internet stvari (Internet of Things).

Kao i svaki drugi veliki sustav, Internet stvari ima mnoštvo prednosti, ali i nedostataka od kojih je najveći mogućnost neautoriziranog pristupa podacima. Konstantno je potrebno poduzimanje određenih sigurnosnih koraka i usavršavanja sustava te edukacija korisnika kako bi se te mogućnosti smanjile. Neovlašteni pristup podacima može ozbiljno našteti fizičkoj ili pravnoj osobi stoga su neophodni sigurnosni sustavi zaštite.

Ova vrsta tehnologije se svakodnevno razvija, a s obzirom na to da je broj mobilnih terminalnih uređaja sve veći, može se reći da će biti u konstantnom razvoju. Prije same implementacije jednog ovakvog sustava potrebno je zadovoljiti određene pravne norme.

KLJUČNE RIJEČI

Internet stvari, mobilni uređaji, neautorizirani pristup, regulativa, uredba

SUMMARY

With the development of smart mobile devices and their increasing number and use, there is a need for their interconnection due to the large amount of data that is stored and processed on these devices. Connecting these devices as a whole makes it easier for users to access the data, because the data is connected as a whole. The technology that enables all of the above is called the Internet of Things.

Like any other large system, the Internet of Things has many advantages, but also disadvantages, the biggest of which is the possibility of unauthorized data access. It is constantly necessary to take certain security steps and improve the system and educate users in order to reduce these opportunities. Unauthorized data access can seriously harm a physical or legal person, so security protection systems are necessary.

This type of technology is evolving every day, and since the number of mobile terminal devices is increasing, it can be said that it will be in constant development. Before the implementation of such a system, it is necessary to meet certain legal norms.

KEYWORDS

Internet of Things, mobile devices, unauthorized access, regulation, law

Sadržaj:

1. Uvod……..1
2. Pitanja sigurnosti i zaštite podataka u IoT okruženju……3
3. Percepcija rizika u IoT okruženju……12
4. Upravljanje podacima u IoT okruženju……...19
    4.1. Tipovi podataka……..19
    4.2. Izvori podataka……...20
    4.3. Prikupljanje podataka…….22
    4.4. Administracija podataka…….22
    4.5. Obrada podataka…….23
    4.6. IoT aplikacije……..23
5. Potencijalni sigurnosni incidenti u IoT okruženju……...25
6. Usklađenost alata opće uredbe o zaštiti podataka za implementaciju IoTa…35
7. Zaključak…….41
Literatura…….43
Popis slika……47
Popis kratica……48

1. Uvod

Internet stvari (Internet of Things – IoT) je tehnologija koja je u sve većem porastu, a s kojom mnogi još uvijek nisu dovoljno upoznati. Ona predstavlja mrežnu infrastrukturu koja se sastoji od velikog broja uređaja međusobno povezanih putem Interneta te odatle dolazi i sami naziv tehnologije. Kao i kod svakog drugog oblika tehnologije, i ova tehnologija ima svoje prednosti i nedostatke, a uređaji, koji su povezani unutar nje, imaju podešene određene postavke. Zbog jako velikog broja uređaja i velike količine podataka koji su na njima pohranjeni, mogućnosti za neautorizirani pristup podacima su visoke. Iz tog razloga je potrebno takve podatke zaštititi na odgovarajuće načine i postići zahtijevanu razinu sigurnosti.

Svrha ovog rada je istraživanje problematike vezane uz neovlašteni pristup osobnim podacima u IoT okruženju. Cilj rada je, na temelju provedenog anketnog upitnika, koji je proveden putem društvenih mreža, uvidjeti osviještenost ljudi o samom IoT okruženju te osjećaj sigurnosti pojedinca dobiven određenim saznanjima o osobnim podacima koji su pohranjeni u njihovim uređajima te kojima je moguće neovlašteno pristupiti.

Rad se sastoji od sedam poglavlja, a to su redom:

1. Uvod,

2. Pitanja sigurnosti i zaštite podataka u IoT okruženju,

3. Percepcija rizika u IoT okruženju,

4. Upravljanje podacima u IoT okruženju,

5. Potencijalni sigurnosni incidenti u IoT okruženju,

6. Usklađenost alata opće uredbe o zaštiti podataka za implementaciju IoT-a te

7. Zaključak.

U prvom poglavlju objašnjen je sam pojam Interneta stvari te objašnjenje teme koja je obrađena. Definirani su svrha i cilj rada te su navedena obrađena poglavlja koja su ukratko opisana u nastavku.

U drugom poglavlju su definirana pitanja sigurnosti i zaštite podataka. Navedeni su mogući napadači na sustav te njihovi motivi napada. Dalje su analizirane prijetnje te kategorije

napada te su detaljno predstavljeni mehanizmi i sigurnosni okviri za detekciju napada te za prikupljanje informacija o sigurnosnim problemima koji se javljaju prilikom implementacije IoT okruženja.

Treće poglavlje govori o percepciji rizika u IoT okruženju te o pravnim zahtjevima s kojima se potrebno suočiti prilikom razvoja IoT tehnologije za čije su potrebe razvijene dvije važne metodologije, UPRAAM i DPIA. Metodologije su detaljno prikazane, objašnjen je princip njihovog rada te osnovni koraci od kojih se sastoje.

Upravljanje podacima u IoT okruženju je iduće poglavlje, a usmjereno je na izazove i probleme na koje se nailazi prilikom upravljanja podacima u IoT okruženju. Također, prikazani su tipovi podataka, izvori podataka, njihovo prikupljanje i administracija, obrada podataka te neke aplikacije koje se koriste u različitim granama društva koje su u srodnoj vezi s IoT okruženjem.

Peto poglavlje je usmjereno na potencijalne sigurnosne incidente u IoT okruženju. Prikazani su neki od incidenata koji su se dogodili u velikim organizacijama. Na temelju dosadašnjih istraživanja prikazani su neki ključni čimbenici koji se odnose na osviještenost korisnika te na njihovu uključenost u Internet stvari u svakodnevnom životu. Navedeni su mogući incidenti u slučaju zastarjelih softvera, opreme ili nemarnosti i neznanja korisnika. U svrhu ovog poglavlja je proveden i anketni upitnik kojim se htjelo uvidjeti u kojoj su količini korisnici osviješteni danas u odnosu na prijašnja istraživanja te u kojoj mjeri su sudionici IoT okruženja, a rezultati su prikazani pripadajućim dijagramima. Također će biti opisan utjecaj Covid-19 virusa na samo tržište i tehnologiju IoTa.

U šestom poglavlju su navedeni neki alati koji definiraju određene obveze organizacija koje moraju poštivati, a tiču se zaštite podataka. Navedeni su i određeni standardi, kao i određeni mehanizmi za certificiranje. U zaključku je prikazan osvrt na obrađenu temu te su iznesene određene činjenice i dobiveni rezultati.

2. Pitanja sigurnosti i zaštite podataka u IoT okruženju

Internet stvari je relativno novi pojam s kojim mnogi nisu upoznati, a označava povezivanje različitih uređaja putem Interneta i predstavlja mrežnu infrastrukturu u kojoj fizički uređaji komuniciraju s virtualnim. Internet stvari kombinira podatke, oblake, povezivost, analitiku i tehnologiju za stvaranje pametnog okruženja, onog u kojem su svi objekti implementirani s mogučnošću mrežnog povezivanja radi poboljšanja funkcionalnosti i interakcije. [1] Kao i svako drugo veliko okruženje, IoT okruženje pohranjuje veliku količinu podataka od kojih su neki od značajne važnosti (osobni podaci, podaci o kretanju, podaci o zdravstvenom stanju pojedinca). Svi pohranjeni podaci moraju biti sigurni te moraju biti zaštićeni na adekvatan način. S obzirom na to da se IoT okruženje sastoji od velikog broja međusobno povezanih uređaja koji pripadaju velikom broju korisnika, mogućnosti za neautorizirani pristup podacima su vrlo visoke i upravo iz tog razloga podaci moraju biti zaštićeni i sigurni. Samo neki od primjera IoT-a su povezani kućanski aparati, sigurnosni sustav pametnog doma, oprema pametnih tvornica, uređaji za nadzor zdravlja. Neautorozirani pristup je moguć od strane nekoliko vrsta napadača od kojih svaka vrsta ima svoju motivaciju. Napadači se dijele u četiri glavne skupine, a to su *cyber* kriminalci, nezadovoljni zaposlenici, *cyber* teroristi te nacionalne države koje su, uglavnom, usmjerene na *cyber* špijunažu. Mete *cyber* kriminalaca su bilo koji nezaštićeni sustavi, ali bez određene svrhe već s ciljem postizanja negativnih posljedica. Nezadovoljni ili nemarni zaposlenici napadaju sustav na način da instaliraju *malware* iz same unutrašnjosti sustava. Ovakvi napadi su vrlo teški za upravljanje i kontrolu jer napadač ima direktan pristup računalima i sustavu čak i ako je mreža fizički nepovezana s javnim Internetom. *Cyber* teroristi i grupe organiziranih kriminalaca posjeduju veliko znanje i vještine o sustavu i u mogućnosti su iskorištavati sve vrste ranjivosti. Najčešće su motivirani ekonomskim interesima koristeći ih za iznude ili za javno sramoćenje pojedinaca. [2]

Osnovni korak u borbi protiv napadača je analiza prijetnji. Prijetnju predstavlja bilo što što može dovesti do prekida, uplitanja ili uništenja usluga ili podataka unutar sustava. Analiza prijetnji predstavlja krucijalan korak u identificiranju vjerojatnosti terorističkog napada, a rezultira procjenom prijetnje. [3] Analiza vanjskih i unutarnjih podataka, udruženih s potencijalnim prijetnjama, predstavlja razliku između načina reakcije na napade i sprječavanja napada. Unutarnji podaci predstavljaju informacije generirane unutar kompanije, a pokrivaju

područja poput operacija, održavanja i financija, dok vanjski podaci pristižu s tržišta, a uključuju korisnike i natjecatelje. Vanjski podaci pomažu u boljem razumijevanju korisničke baze, a unutarnji podaci pomažu u vođenju posla i optimizaciji operacija. [4] Analiza prijetnji vrijednuje četiri dimenzije vezane uz potencijalne prijetnje:

1. Djelokrug: predstavlja zbirku uređaja, podataka i usluga koje prijetnje mogu vidjeti kao potencijalnu metu napada,

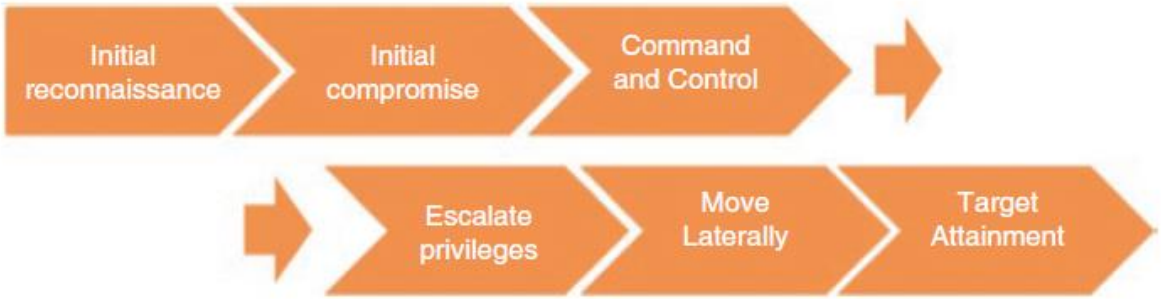
2. Zbirka podataka: predstavlja mogućnost prikupljanja podataka o *cyber* prijetnjama koje prijetnje koriste kao što su ranjivosti sustava, otvoreni portovi, popis *e-mail* adresa te IP[1] adrese sustava,

3. Analiza rizika: koristi se da bi se odredila razina izloženosti prijetnjama. Postiže se vrednovanjem postojećih mehanizama pomoću kojih IoT okruženje treba neutralizirati prijetnje u smislu dostupnosti, povjerljivosti te integriteta te

4. Smanjenje i predviđanje: izvedeni su na temelju ishoda prve, druge i treće dimenzije. Ova razina ima mogućnost dizajniranja mjera za smanjenje i sprečavanja sličnih napada u budućnosti. [2]

Valja i napomenuti da su sustavi koji se redovito ažuriraju manje ranjivi od onih sa zastarjelim softverom. To posebice predstavlja problem u IoT okruženju zbog velikog broja različitih uređaja pokretanih drugačijim operativnim sustavom ili izgrađenih drugačijim tehnologijama. Također, nisu svi sustavi jednako zanimljivi napadačima, već samo oni koji im mogu dati određenu vrijednost, odnosno, oni koji su vrijedni iskorištavanja njihovih ranjivosti. Uređaji koji su napadačima najzanimljiviji su sigurnosne kamere, povezani telefaks uređaji, pametni TV prijamnici, pametne žarulje, mikrofoni pametnih telefona pa čak i aparati za kavu. Uređaji koji su fizički nepovezani s javnom mrežom su manje ranjivi na *cyber* napade, dok su fizički zaštićeni uređaji manje ranjivi na napade petljom.

[1] Internet protocol



Slika 1. Životni ciklus *cyber* napada, [2]

Na slici 1. prikazan je životni ciklus *cyber* napada koji se sastoji od šest faza. Inicijalno izviđanje je prva faza, u toj fazi napadač proučava djelokrug napada vrednovanjem dostupnih zaštita sustava i njegovih potencijalnih ranjivosti. Druga faza je inicijalna opasnost u kojoj napadač ima mogućnost pristupanja sustavu iskorištavanjem određenih ranjivosti identificiranih u fazi izviđanja. U fazi naredbe i kontrole, napadač instalirava maliciozan softver kako bi ostvario mogućnost instantnog daljinskog pristupa sustavu u budućim napadima. U fazi eskaliranja privilegija, napadač pokušava eskalirati svoje privilegije prikupljanjem certifikata ili instalacijom *keylogger-a* za prikupljanje lozinki. U petoj fazi napadač skenira mrežnu unutrašnjost kako bi pronašao dodatne potencijalne mete. U zadnjoj fazi napadač dobiva pristup podacima te ima mogućnost brisanja podataka ili isključivanja i ponovnog postavljanja uređaja. [2]

Postoje četiri vrste obrazaca po kojima se napadi mogu kategorizirati, a to su:

1. Ciljani napadi: u ovoj vrsti napada, napadač unaprijed zna koji će sustav napasti, a najčešće je motiviran beneficijama koje će time postići,

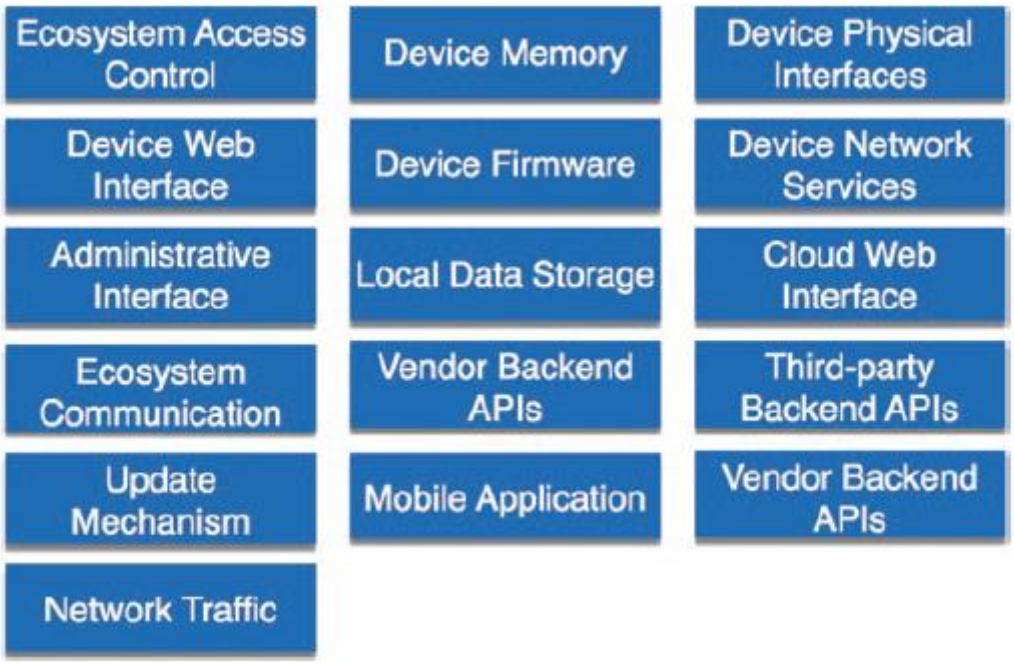
2. Rizik kolateralne štete: ovaj obrazac je povezan s ciljanim napadom, a događa se u situacijama kada napadači, u potrazi za glavnom metom napada, također kompromitiraju i inficiraju povezane čvorove iskorištavanjem njihovih ranjivosti te kompromitiranjem podataka upravljanim od strane povezanih čvorova,

3. Socijalni inženjering i *phishing*: mete napada su zaposlenici, koji predstavljaju najslabiju kariku u sigurnosnom lancu, a napad se izvodi na način da se zaposlenika navede da greškom otvori maliciozan sadržaj ili elektroničku poruku ili da instalira zlonamjerni softver te

4. Daljinski pristup: napadači, imajući prednost nad loše dizajniranim sigurnosnim mehanizmima, uzimaju pod kontrolu uređaje te ih koriste za izvođenje napada na daljinu. Veliki broj DDoS[2] napada prema poznatim pružateljima usluga se vodi ovim obrascem. Osim obrazaca, treba spomenuti i vrste napada na sustav, a najčešći od njih su *brute-force, malware* napadi te, već spomenuti, *phishing*. Kod *brute-force* metode, napadači pokušavaju pristupiti sustavu na način da isprobavaju sve moguće vrste lozinki dok ne otključaju korisnički profil. Lozinka im kasnije pomaže u pristupu određenim podacima ili *web* stranicama. *Malware* se definira kao zlonamjeran softver koji se preuzima na uređaj bez znanja korisnika, a primarni zadatak mu je krađa, enkripcija i brisanje osjetljivih podataka s uređaja. [5]

Kako bi se umanjile prijetnje, potrebno je poduzeti određene protumjere. Protumjere predstavljaju aktivnosti koje se izvršavaju kako bi se ublažio ili umanjio utjecaj druge aktivnosti ili situacije ili kako bi ih se učinilo bezopasnima. Prijetnje su neizbježne za svaki sustav, stoga ih je potrebno dizajnirati s pretpostavkama da će često biti mete napada. [2] Detekcija i oporavak od napada su glavne protumjere u slučajevima kad je napad bio uspješan. Kao glavni mehanizmi za detekciju napada koriste se alati za nadzor. Također, postoje i određeni sigurnosni okviri za identifikaciju i detekciju prijetnji. Prvi od njih je OWASP (The Open Web Application Security Project) IoT koji definira sigurnosni okvir za prikupljanje informacija o sigurnosnim problemima vezanim uz razvoj IoT okruženja i njegovu implementaciju. Glavni cilj ovog okvira jest pružiti pomoć, proizvođačima i korisnicima, u povećanju njihove pouzdanosti prema IoT okruženju. Također, OWASP predstavlja repozitorij svih *web,* aplikacijskih i sigurnosnih „stvari“ podržavanih od strane širokog znanja i iskustva. [6]

[2] Distributed Denial of Service



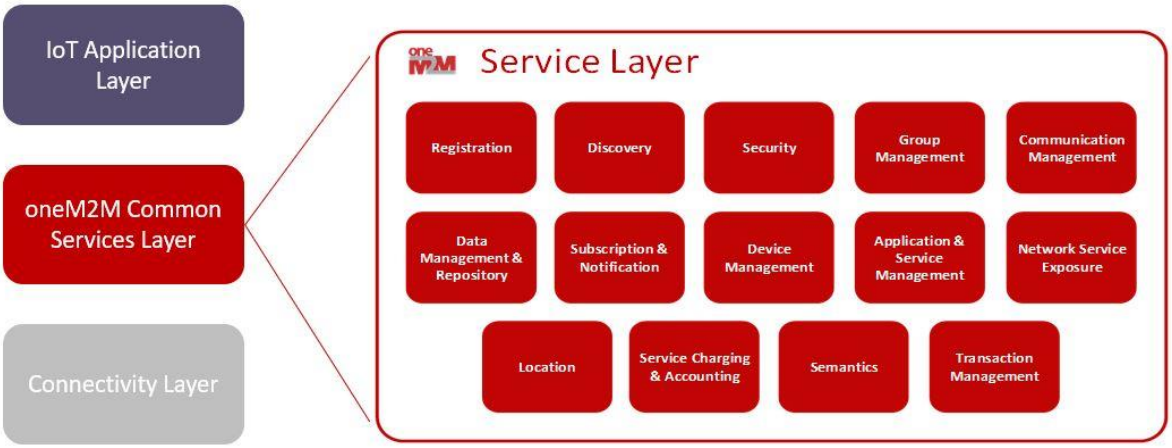
Slika 2. OWASP IoT područja, [2]

Na slici 2. prikazano je 17 područja IoT okruženja koja mogu biti podvrgnuta napadima, a u nastavku je navedeno deset ranjivosti najviše razine koje mogu biti identificirane među prikazanim područjima. Nesigurno mrežno sučelje predstavlja ranjivost jer bilo tko s omogućenim pristupom sustavu ima mogućnost izvođenja napada. Nedovoljna autentikacija se javlja u slučajevima kada se koriste loše zaporke ili kada su zaporke slabo zaštićene. Nesigurne mrežne usluge mogu biti osjetljive za napade preplavljivanjem ili za DoS napade. Manjak verifikacije integriteta ili enkripcije omogućava vidljivost podataka koji putuju lokalnom mrežom. Pitanja privatnosti uključuju manjak ispravnih zaštita prikupljenih osobnih podataka. Manjak akreditiva javlja se u nesigurnom *cloud* sučelju te u nesigurnom mobilnom sučelju. Do nedovoljne sigurnosne konfiguracije dolazi zbog manjka zrnatosti u konfiguracijskim postavkama, osobito za korisničke ovlasti. Nesiguran softver ili *firmware* sadrži osjetljive podatke ili nezaštićene mrežne konekcije za nadogradnje softvera ili *firmware-a*. Kao zadnja ranjivost navodi se loša fizička zaštita što znači da se USB[3] ili ostalim priključcima može lako pristupiti i zaobići konfiguracija ili određene ovlasti. Jedan od nesigurnih softvera kojima se

[3] Universal Serial Bus

služilo mnogo ljudi pa tako i autor ovog rada je Flash[4], koji se više ne koristi, a predstavljao je multimedijalni *player*.

Sljedeći, vrlo koristan, sigurnosni okvir je oneM2M koji definira sigurnosni okvir iz vlastitog modela arhitekture koji podržava M2M[5] usluge s kraja na kraj. oneM2M objedinjuje sve komponente složaja IoT rješenja te koristi postojeće tehnologijske komponente i standarde. [7] Ovaj okvir identificira četiri sigurnosne domene koje pružaju niz sigurnosnih mjera za identifikaciju prijetnji koje se mogu pojaviti unutar njega. Sigurnost aplikacijskih domena predstavlja set sigurnosnih mjera koje omogućavaju aplikacijske entitete i entitete zajedničkih usluga za sigurnu razmjenu podataka te zaštitu od napada. Sigurnost domene intra-zajedničkih usluga predstavlja niz sigurnosnih mjera koje omogućavaju funkcionalnosti zajedničkih usluga unutar njihovih entiteta za sigurnu razmjenu podataka te zaštitu od napada. Sigurnost domene inter-zajedničkih usluga predstavlja niz sigurnosnih mjera koje podacima omogućavaju sigurnu razmjenu između različitih entiteta zajedničkih usluga te zaštitu od napada. Mrežna sigurnost predstavlja niz sigurnosnih mjera koje omogućavaju entitetima zajedničkih usluga te uslugama mrežne sigurnosti sigurnu razmjenu podataka te zaštitu od napada.



Slika 3. oneM2M IoT arhitektura, [7]

Na slici 3. prikazana je arhitektura oneM2M sigurnosnog okvira po kojoj je vidljivo da se sastoji od tri sloja, a to su aplikacijski sloj, sloj oneM2M usluga te konekcijski sloj. [7] Osim

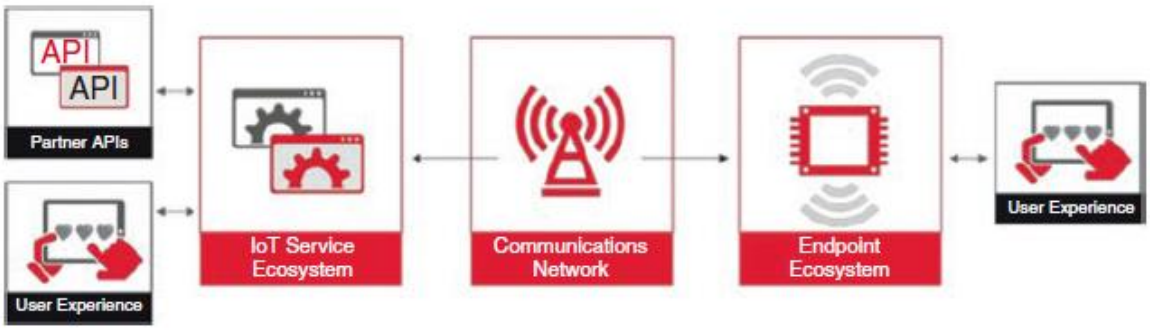
[4] Flash je bio računalni softver koji je služio za pregled sadržaja kreiranog na Adobe Flash platformi što uključuje multimedijalne sadržaje te igre, a pokretao se direktno s *web* preglednika ili na podržanim mobilnim uređajima
[5] Machine 2 Machine

navedenih, treba izdvojiti i dodatne slojeve oneM2M arhitekture. Prvi sloj je sloj sigurnosnih funkcija koji sadrži niz sigurnosnih funkcija koje mogu biti podijeljene u šest kategorija, a to su redom: identifikacija, autentikacija, autorizacija, sigurnosna asocijacija, rukovanje osjetljivim podacima te sigurnosna administracija. Drugi sloj predstavlja sloj sigurnosne okoline apstrakcije koji služi za implementaciju različitih sigurnosnih mogućnosti kao što su derivacija zaporki, enkripcija i dekripcija podataka, generacija i verifikacija potpisa, sigurnosni akreditivi te mnogi drugi. Ovaj sloj također pruža i fizički pristup sigurnosnom okruženju. Treći, i zadnji sloj, je sloj sigurnosnog okruženja koji sadrži jedan ili više sigurnosnih okruženja koja pružaju različite sigurnosne usluge usko povezane s pohranom osjetljivih podataka te s izvršenjem osjetljivih funkcija. Osjetljivi podaci uključuju sigurnosne zaporke, akreditive, identifikaciju informacija i mnoge druge, a osjetljive funkcije uključuju enkripciju i dekripciju podataka.

Ako se govori o nizu dokumenata sa sigurnosnim smjernicama koje djeluju kao podloga za sigurnosna pitanja IoT okruženja, tada je riječ o GSMA (Global System for Mobile Communications Association) IoT sigurnosnom okviru koji se odnosi na IoT entitete što uključuje pružatelje usluga, proizvođače uređaja, mrežne operatore i slično. GSMA IoT predstavlja inicijativu za pomoć operatorima u dodavanju vrijednosti i ubrzavanju dostavljanja novih povezanih uređaja i usluga unutar IoT-a što se postiže kolaboracijom industrije, odgovarajućom regulacijom te optimizacijom mreže, a sve to s ciljem pružanja podrške za rast IoT-a. [8] Ranije spomenute smjernice pružaju preporuke na tri razine, uslužni ekosustav, krajnji ekosustav te mrežni operatori. Sigurnosne smjernice predstavljaju niz praksa koje promoviraju sigurnosni dizajn s kraja na kraj te razvoj IoT rješenja. Organizacije koje usvajaju te smjernice uključuju IoT pružatelje usluga, IoT platforme te IoT uređaje. [9] GSMA IoT sigurnosni okvir ne pruža nove IoT standarde kao što to čini oneM2M, umjesto toga ukazuje na trenutno dostupna rješenja i standarde pomoću kojih je moguće što lakše odgovoriti sigurnosnim izazovima IoT okruženja. Kako bi se osigurala IoT dostupnost, jedna od mogućnosti je da se za mobilne komunikacije integriraju bežične tehnologije i protokoli koji pružaju usluge i rješenja za te komunikacije, a koji mogu zadovoljiti IoT potrebe. Druga mogućnost je osiguravanje identiteta IoT ekosustava, što znači osiguravanje od napada poput pasivnog presretanja podataka ili krađe identiteta. Za adresiranje privatnosti i sigurnosti, tehnologije poput 3G[6] i 4G[7] koriste zajedničke metode autentikacije za verifikaciju identiteta.

[6] Treća generacija mobilnih mreža
[7] Četvrta generacija mobilnih mreža

Također, s obzirom na to da su u uređajima pohranjene velike količine osobnih podataka, potrebno je osigurati sigurnost i privatnost.



Slika 4. Primjer modela GSM IoT okruženja, [9]

Na slici 4. prikazan je primjer modela GSM IoT okruženja na kojem se vide glavni sudionici tog okruženja s pripadajućim međusobnim odnosima, a to su API[8], korisničko iskustvo, ekosustav i komunikacijska mreža.

Za razvoj pouzdanih autonomnih sigurnosnih okvira koristi se okvir Anastacia koji dozvoljava testiranje, validaciju i optimizaciju sigurnosti od dizajna pa sve do razvoja i održavanja. Ovaj sigurnosni okvir uključuje:

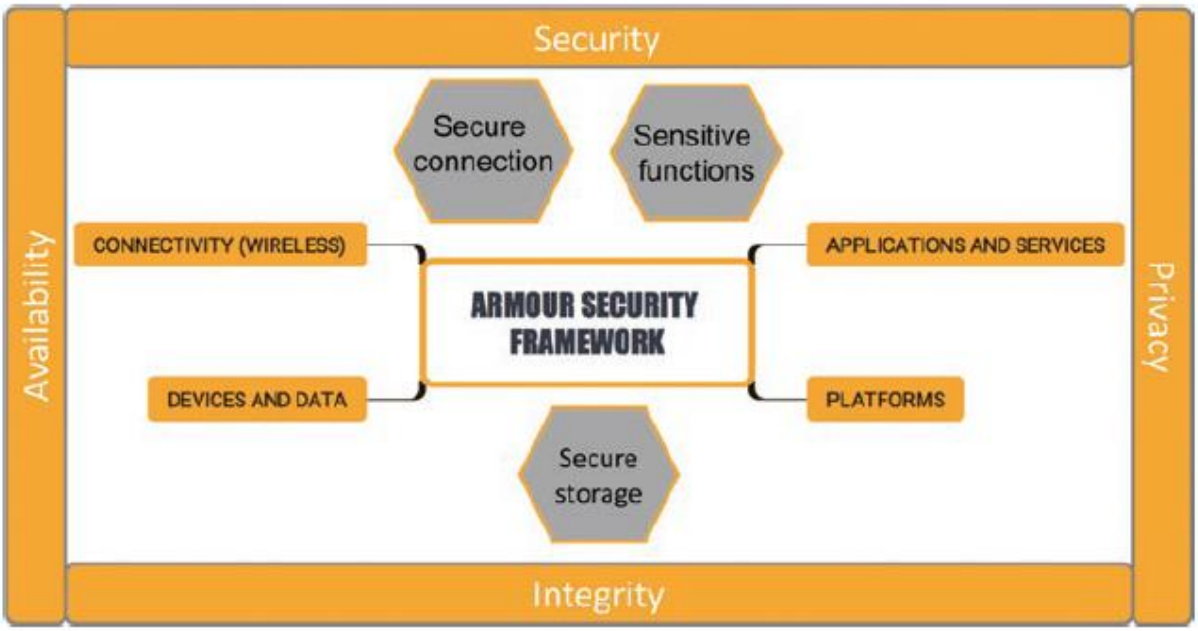
1. Paradigmu sigurnosnog razvoja baziranu na usklađenosti prakse i upotrebi sigurnosnih komponenti koja pruža sigurnosni dizajn i razvoj te osigurava njihovu sigurnost,

2. Složaj distributivnih i sigurnosnih komponenti sposobnih za razvoj sigurnosnih korisničkih politika i aktivnosti unutar IoT arhitekture koje dozvoljavaju adaptaciju sustava u smislu ublažavanja novih i neočekivanih sigurnosnih ranjivosti te

3. Kombinaciju standarda sigurnosti i privatnosti s nadzorom sustava u realnom vremenu i *online* testiranja koja pruža kvantitativne i kvalitativne evaluacije sigurnosnih razina i rizika privatnosti.

Zadnji u nizu sigurnosnih okvira je Armour, a njegova namjena je da služi kao sigurnosni vodič za segmente razvoja IoT okruženja.

[8] Application Programming Interface



Slika 5. Armour sigurnosni okvir, [10]

Na slici 5. prikazan je Armour sigurnosni okvir po kojoj je vidljivo da Armour definira četiri IoT segmenta IoT razvoja, a to su uređaji i podaci, bežična povezivost, platforme te aplikacije i usluge. Armour predlaže povezivanje OWASP okvira, oneM2M okvira i GSMA IoT okvira u Armour sigurnosni okvir te definira sigurnost u smislu dostupnosti, integriteta, privatnosti i sigurnosti, kao i smjernice za svaki od četiri segmenta s pripadajućim elementima.

3. Percepcija rizika u IoT okruženju

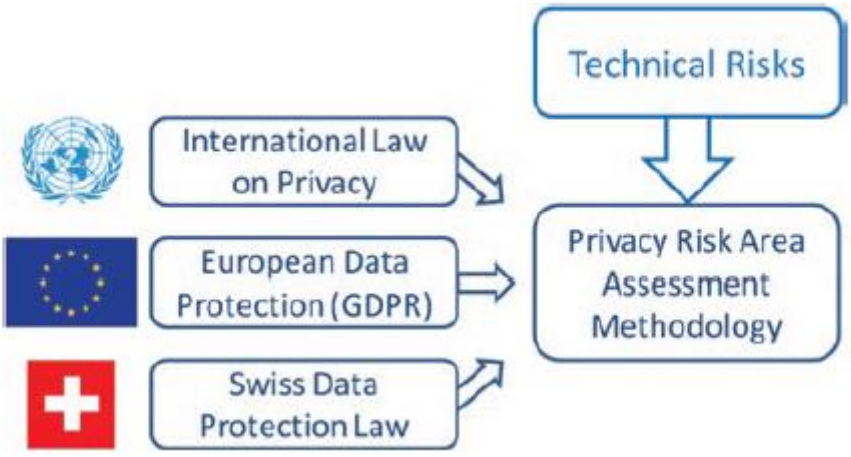
Prilikom razvoja bilo koje vrste tehnologije, pa tako i IoT tehnologije, potrebno je suočiti se s pravnim zahtjevima u smislu zaštite osobnih podataka. Za potrebe toga, u IoT području, razvijena je metodologija UPRAAM (Universal Privacy Risk Area Assessment Methodology). UPRAAM je dizajniran za procjenu usklađenosti IoT razvoja s GDPR (General Data Protection Regulation) regulacijom, ali se može primijeniti i za *web* stranice, aplikacije pametnih telefona te druge objekte. Alati koji građanima omogućavaju provjeru jesu li njihova prava kao podatkovni subjekti poštivana te alati i usluge koji poduzećima pomažu usklađivanje sa zahtjevima o zaštiti osobnih podataka, koriste metodologiju UPRAAM. [11]

Kako bi osigurao generičnost metodologije, UPRAAM je dizajniran kako bi zadovoljio dvije značajne svrhe upotrebe, a to su:

1. Jednostavna procjena usklađenosti razvoja IoT okruženja, *web* stranica i aplikacija za pametne telefone s redovnim krajnjim korisnicima te

2. Evaluacija usklađenosti zaštite podataka od strane stručnjaka. [2]

Zahtjevi koji su bili korišteni za vođenje i nadzor UPRAAM razvoja uključuju pouzdanost i vjerodostojnost, mogućnost sadržavanja legalnih i tehničkih rizika te sadržavanje regulacija. Razvoj UPRAAM-a je započeo identifikacijom i analiziranjem niza zakonskih obveza u smislu privatnosti i zaštite podataka.



Slika 6. UPRAAM zahtjevi, [12]

Na slici 6. prikazani su zakonski zahtjevi koji moraju biti zadovoljeni, zajedno s identificiranim tehničkim rizicima, prilikom razvoja UPRAAM metodologije kako bi se pružila ispravna evaluacija. UPRAAM metodologija je bazirana na provjerama i kontrolama, a to uključuje:

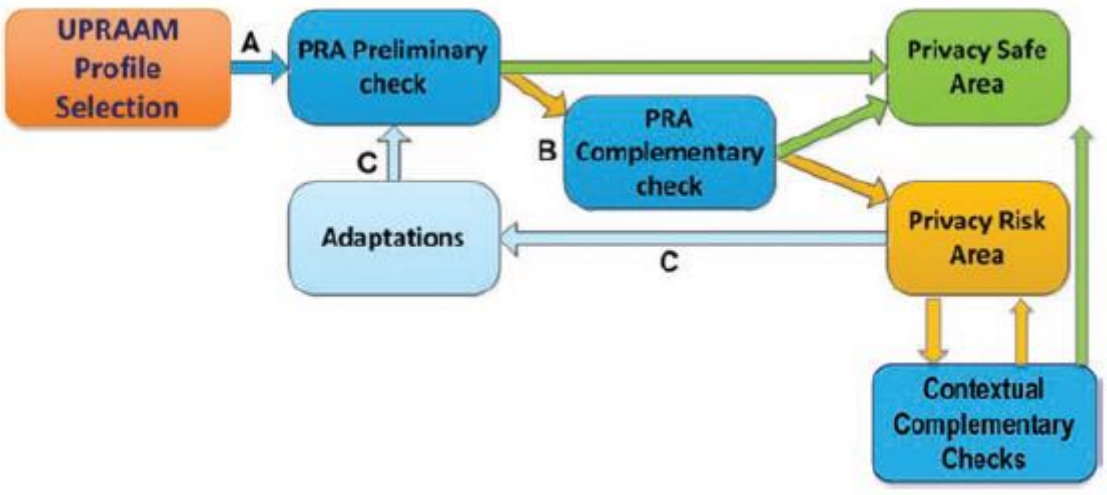
1. Preliminarni korak pod nazivom UPRAAM odabir profila: omogućava odabir i filtriranje pitanja prema kategoriji objekta. To se radi iz razloga što različiti objekti odgovaraju različitim profilima rizika. Ovaj korak omogućava bolji odabir pitanja i izbjegavanje onih nepotrebnih.

2. Prijedlog inicijalnih kontrola: u ovom koraku korisnik provjerava popis kriterija kako bi se utvrdilo jesu li osobni podaci izloženi riziku. Ako se zaključi da ne postoje podaci izloženi riziku, rezultat predstavlja sigurno područje privatnosti te se analiza zaustavlja. Ako se, s druge strane, zaključi da postoje podaci izloženi riziku, provode se dodatne provjere i predstavljaju korisniku te se time završava procjena.

3. Niz dodatnih provjera: dostavlja se korisniku prema podacima iz prethodnog koraka. Ovaj korak omogućava proširenje procesa dodatnim pitanjima za detaljniju analizu. Prema odgovorima korisnika, procjena se ažurira dok se ne postigne pouzdanost ili dok se podaci ne zateknu u sigurnom području privatnosti. U suprotnom, postoji visoka mogućnost da se podaci zateknu u rizičnom području privatnosti ili u sivoj zoni.

4. UPRAAM metodologija omogućava korisnicima fokusiranje na ključne faktore rizika. U slučaju nezadovoljavajućih rezultata nudi se iterativni proces u kojem korisnik ima mogućnost pregleda ključnih faktora koji su uzrokovali negativne rezultate te razmatranja adaptacija plana razvoja kako bi se ublažili rizici. Zatim se postupak ponavlja i ako rezultat ostane negativan, potrebna je detaljnija analiza i konzultacije sa stručnim osobljem.

Ono što još UPRAAM uključuje su informacije u realnom vremenu o tome je li *web* stranica usklađena s GDPR-om te jesu li instalirana aplikacija ili IoT razvoj u pametnom gradu usklađeni s GDPR-om, informacije o razvoju prijetnji za korisnike te vodič s bitnim izvorima o zaštiti privatnosti. [13] Na slici 7. prikazana je shema iterativnog procesa s opisana četiri koraka provjere i kontrole.



Slika 7. Shema UPRAAM iterativnog procesa, [14]

Kada se govori o pristupu informacijama, postoje dva modela UPRAAM metodologije. Prvi model se oslanja na informacije koje su dostupne javnosti i naziva se *Crowdsourcing* dok drugi model, onaj za detaljniju analizu, zahtijeva pristup većoj količini podataka koji sadrže informacije o mreži i povezivosti sa serverima, pohranama podataka, odnosima s procesorima i slično. Razina granularnosti evaluacije u oba modela ima utjecaj na razinu pouzdanosti rezultata, što znači da će rezultat biti pouzdaniji što je analiza sistematičnija. *Crowdsourcing* model uključuje informacije i mišljenja od velike skupine ljudi koji svoje podatke objavljuju putem Interneta, društvenih mreža i aplikacija na pametnim telefonima. Pojedinci uključeni u *crowdsourcing* mogu biti plaćeni zaposlenici ili volonteri. [15] *Crowdsourcing* također poboljšava kreativne procese i povećava produktivnost. Troškovi rada i istraživanja se smanjuju. S obzirom na to da se cijeli postupak temelji na Internetu, vrijeme provedeno u prikupljanju podataka putem fokus grupa ili u ručnom pretraživanju drastično se smanjuje. [16] Krajnji korisnik ima pet značajnih uloga, a te uloge su:

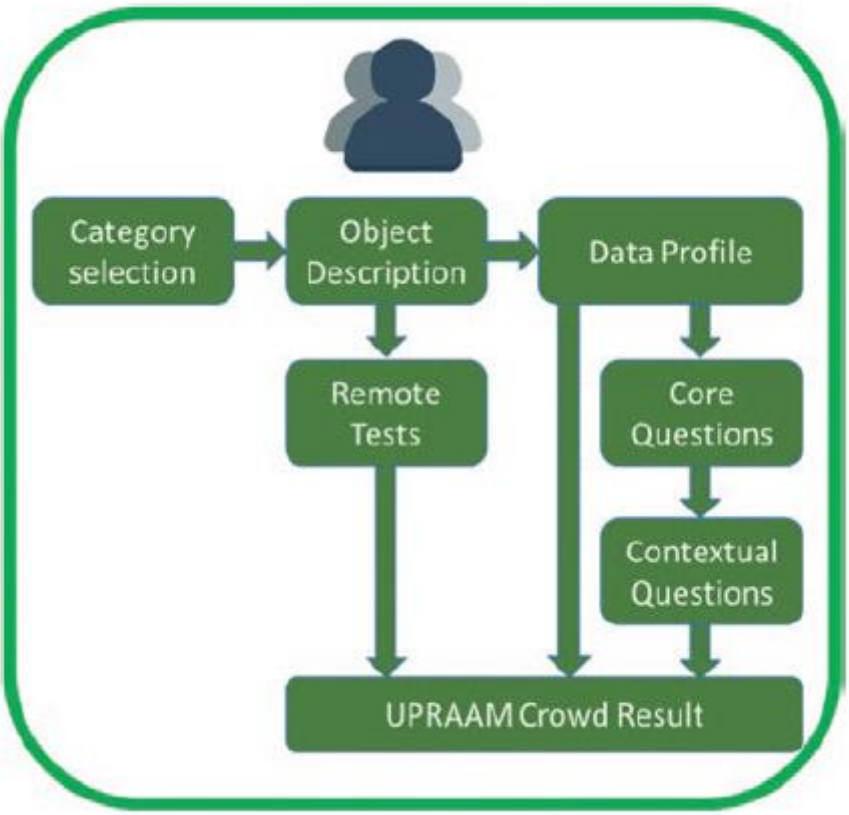
1. Uočavanje i identifikacija sumnjivog razvoja IoT okruženja, aplikacija za pametni telefon ili *web* stranice,

2. Omogućavanje automatskog rangiranja zadataka na temelju broja zahtjeva ili upozorenja od strane mnoštva,

3. Donošenje procjene objekata od značaja korištenjem UPRAAM metodologije,

4. Podjela zajedničkog znanja između mnoštva kreiranog od strane krajnjih korisnika u zajedničku bazu podataka te

5. Pridonošenje mnoštva dosezanju platformi i alata.



Slika 8. Evaluacija UPRAAM metodologije, [2]

Na slici 8. prikazana je evaluacija UPRAAM modela iz perspektive korisnika koja se sastoji od sedam koraka:

1. Odabir kategorije: ovaj korak uključuje odabir kategorije objekta koji će se procijenjivati, a tri najčešća odabira koja se predlažu su evaluacija *web* stranice, evaluacija aplikacija za pametne telefone i evaluacija IoT razvoja,

2. Opis objekta: u ovom koraku korisnik pruža informacije o objektu koji se procijenjuje, kao što su ime, inačica, kratki opis i slično,

3. Daljinski testovi: koriste se za razne provjere kao što je, primjerice, identifikacija kolačića,

4. Profiliranje podataka: korisnik identificira kategorije osobnih podataka koji su prikupljeni od strane aplikacija te koji će se procijenjivati. Ukoliko nema prikupljenih podataka, dolazi do situacije sigurnog područja, u suprotnom, proces se nastavlja ka sljedećem koraku,

5. Više pitanja: niz pitanja dostavlja se korisniku s ciljem procjene određenih rizika privatnosti,

6. Dodatna pitanja: dodatna pitanja se dostavljaju korisniku prema njegovim prethodnim naputcima te

7. Automatizirani rezultat: nakon što su odgovori na sva pitanja ponuđeni, sustav pruža evaluaciju razine rizika privatnosti.

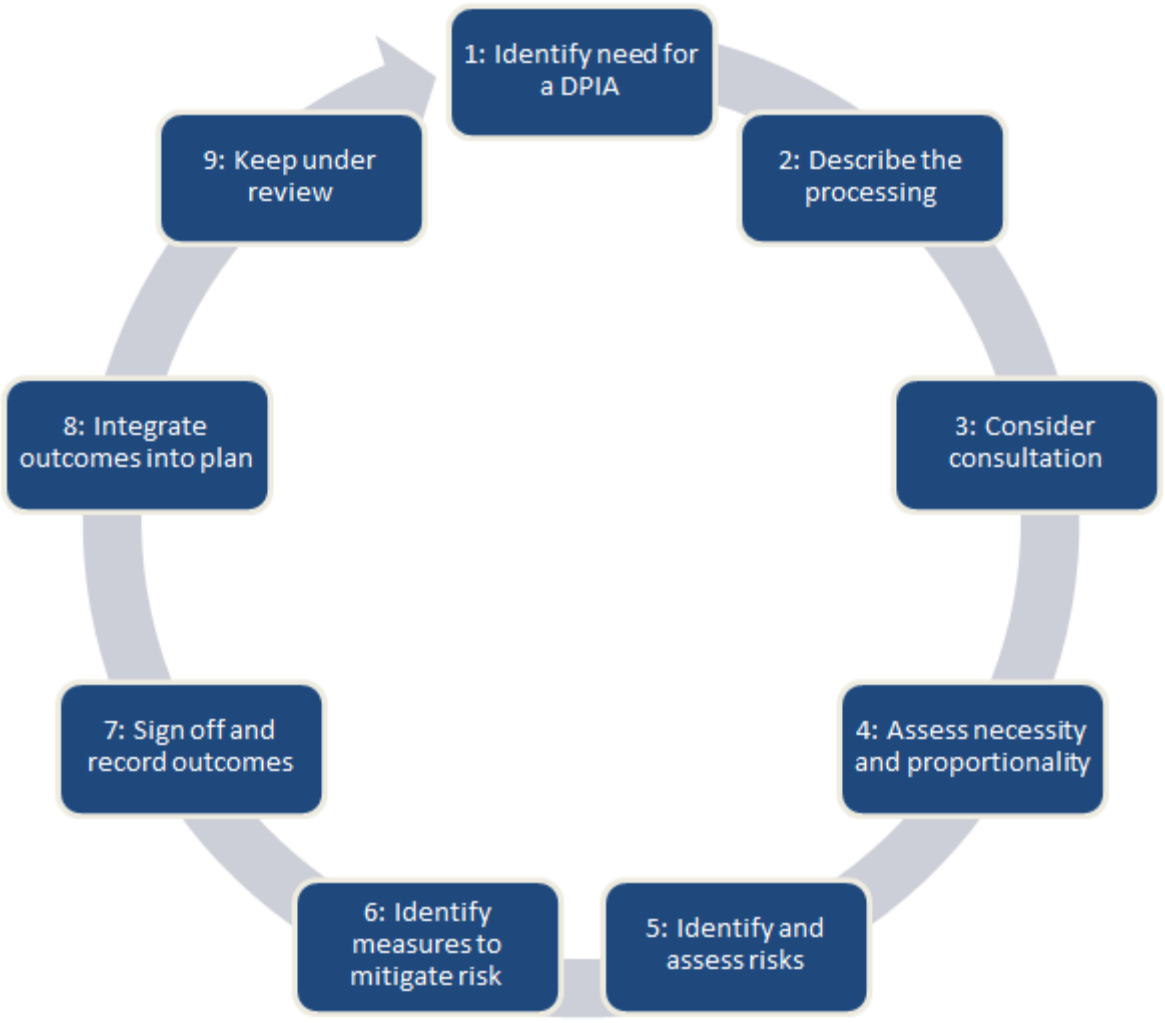
Za smenjenje rizika sustava prve mjere su identifikacija bilo kojeg potencijalnog nekonformizma, a proces smanjenja rizika moguće je odraditi kroz određene korake i akcije. Prvi korak uključuje identifikaciju regulacija na temelju lokacije razvoja IoT okruženja. Drugi korak je fokusiran na identifikaciju osobnih podataka koji mogu biti prikupljeni od strane sustava. Tamo gdje je moguće, točne informacije, koje će se obrađivati, moraju biti pružene. Također, trebala bi se provesti analiza praznine sustava od treće strane zbog identifikacije potencijalnih neusklađenosti s regulacijom za zaštitu podataka. Nakon što se sve neusklađenosti pohrane, razmatra se certifikacija. Proces se mora redovito ponavljati, kao i usklađenosti sustava.

Ono što je također bitno napomenuti jest to da je razumijevanje *cyber* prijetnji i ranjivosti osnovni i prvi korak za svako poduzeće. Prijetnje se sastoje od različitih vanjskih i unutarnjih krađa podataka, remećenja operacija ili neovlaštenog korištenja sredstava poduzeća. Ranjivosti pak definiraju slabosti unutar poduzeća koje mogu biti iskorištene u postizanju rezultata s negativnim posljedicama. [17] Pristup za smanjivanje rizika *cyber* sigurnosti, a koji se najčešće koristi, je saniranje ranjivosti unutar sustava te na taj način smanjivanje „površine“ napada dostupne napadačima.

Prijetnje i rizici su mogući i u pametnim domovima, a napadi koji su mogući u takvoj vrsti okruženja su *cyber* fizički napadi koji se razlikuju od tradicionlanih fizičkih napada kao što su provale i od *cyber* napada kao što je *malware*. Ovakve vrste napada su posebne zato što utječu na fizički prostor neovlaštenim pristupom u komunikacijsku infrastrukturu. Napadač kod

takvog napada može, primjerice, neovlašteno pristupiti sustavu pametnog doma i otključati vrata ili uključiti neki od kućanskih aparata što može dovesti do tradicionalne vrste napada poput provala ili požara. Ova vrsta napada predstavlja novi oblik rizika za stanovnike i percepcija korisnika je veoma bitna zbog samog razvoja pametnog doma.

Osim UPRAAM metodologije, postoji i metodologija DPIA (Data Protection Impact Assessment) koja se koristi u prvom od tri koraka transparentnog modela. DPIA je način za sistemsku i sveobuhvatnu analizu procesa, a pomaže u identificiranju i minimiziranju rizika zaštite podataka. [18] DPIA je potrebna kod bilo kojeg procesiranja čiji će rezultat vjerojatno završiti visokim rizikom za prava i slobode pojedinaca. Slučajevi u kojima bi DPIA uvijek trebala biti prisutna su sistematska i ekstenzivna evaluacija osobnih aspekata pojedinaca, procesiranje osjetljivih informacija te sustavski nadzor javnih mjesta. [19] Transparentni model sadrži jedanaest smjernica koje odgovaraju trima područjima, a to su principi upravljanja GDPR regulacijom, nejasnoće i neželjena ograničenja GDPR opskrbe važna za IoT okruženje te rizici privatnosti u IoT okruženju. Sa sve većim razvojem IoT tehnologija, DPIA postaje obavezna za većinu IoT uređaja dok će IoT razvijači morati procijenjivati rizike uređaja koje proizvode. Ukoliko njihova procjena pokaže visoke rizike privatnosti, morat će se provesti savjetovanje sa stručnjacima. Ova metoda pomaže u boljem razumijevanju potencijalnih rizika prilikom korištenja IoT proizvoda ili usluge. Proces DPIA metodologije prikazan je dijagramom na slici 9.



Slika 9. Iterativni proces DPIA metodologije, [18]

Drugi korak transparentnog modela uključuje ublažavanje rizika. Kod tog je koraka nužna procjena podrijetla podataka iz razloga što konzumenti mogu pružiti netočne podatke i mogu biti nesvjesni posljedica ukoliko je njihovo ponašanje konstantno nadzirano. Čak i kada su svjesni potencijalnih posljedica korištenja usluga ili proizvoda, promjene postavki mogu pružiti nepogodnosti ili oštećenja. Iz tog razloga implementiraju se organizacijske mjere koje garantiraju točnost i pouzdanost prikupljenih podataka. Treći korak ovog modela govori o zadanim postavkama te o postavkama po dizajnu. Cilj ovog koraka je povećati povjerenje i prihvaćanje tehnologije od strane korisnika te povećanje privatnosti korisnika. Riješavaju se i pitanja mjera u slučaju napada na sustav te pitanja ublažavanja negativnih posljedica uslijed „curenja“ podataka.

4. Upravljanje podacima u IoT okruženju

Jedan od ključnih čimbenika za uspješno IoT okruženje je tijek podataka koji je prisutan unutar tih tehnologija zbog različitih aspekata podataka poput izvora podataka, prikupljanja podataka, obrade podataka te transmisijskih uređaja. [20] U ovom poglavlju opisani su izazovi i problemi upravljanja podacima u smislu IoT okruženja, uključujući izvore podataka, prikupljanje podataka te obradu podataka. To su, u većini slučajeva, podaci vezani uz korisnike, određene transakcije i operacije velikih organizacija.

4.1. Tipovi podataka

U IoT okruženju postoje dvije skupine po kojima se podaci mogu razvrstati, a to su sirovi podaci niske razine i opći podaci visoke razine. [20]

1. Polimorfizam i heterogenost: aplikacije IoT okruženja uključuju različite tipove podataka iz različitih aplikacija. Podaci mogu biti fizičke prirode, biološke prirode i kemijske prirode. S porastom kompleksnosti aplikacija, dolazi do korelacije podataka iz različitih izvora. Podaci mogu biti numeričkog tipa, tekstualnog tipa te u XML[9] formatu, dok struktura podataka može predstavljati kombinaciju strukturiranih podataka, polustrukturiranih podataka te nestrukturiranih podataka.

2. Masivne skale: velika količina inteligentne opreme povezane s Internetom može prikupiti milijarde podataka u realnom vremenu. S obzirom na tako veliki broj podataka, potrebno je i veliko mjesto za pohranu te snažan sustav za obradu podataka.

3. Bogata semantika: uključuje prostorne podatke s informacijama o prostoru i vremenu kao što su GIS[10] podaci, a koriste se u zdravstvu, u sustavu za nadzor ulica te za transportna vozila.

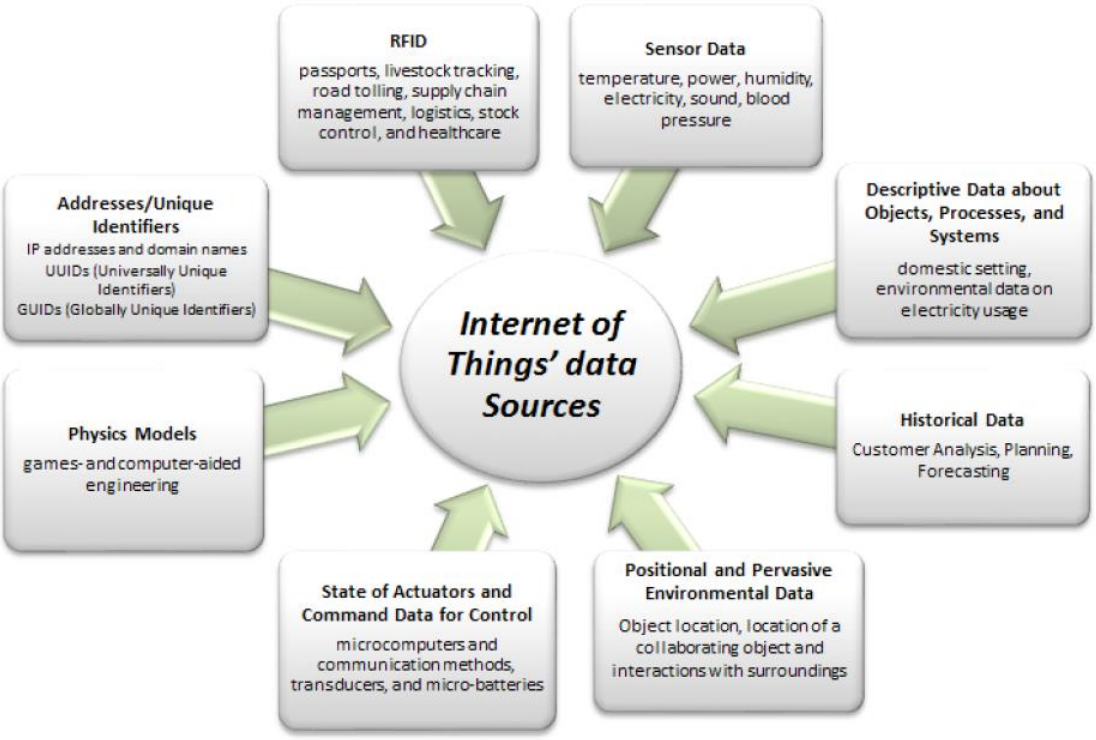
Osim navedenih, postoji i pet tipova podataka koji „pokreću“ IoT tehnologiju. Prvi od tih podataka su podaci koji se prikupljaju od strane IoT senzora unutar uređaja, a uključuju

[9] Extensible Markup Language
[10] Geoinformacijski sustavi

serijske brojeve objekata, temperaturu, lokaciju, vlažnost i slično. U iduću skupinu spadaju podaci koji se prikupljaju u repozitoriju koji se najčešće nalazi u oblaku. Ostala tri tipa uključuju prikupljanje podataka s velikog broja specijalnih IoT informacija, pružanje izvještaja te upotreba informacija pohranjenih u bazama podataka za pružanje napredne analitike. [21]

4.2. Izvori podataka

Podaci se u IoT okruženju prikupljaju s različitih senzora, a primarni izvori su „stvari“ ili interakcije s drugim „stvarima“ gdje se za pojam „stvari“ misli na uređaje unutar IoT okruženja. Ti uređaji mogu biti autonomni, poluautonomni ili neautonomni. S obzirom na ovisnost podataka o samim izvorima podataka, izvori se dijele na osam glavnih kategorija koje su prikazane na slici 10.



Slika 10. Izvori podataka s pripadajućim aplikacijama, [20]

1. RFID: RFID[11] tehnologija je lako prepoznatljiva i može biti implementirana u bilo koju vrstu objekta. RFID oznake interno pohranjuju informacije koje mogu biti emitirane u obliku radio valova putem čitača.

2. Unikatni identifikatori: objekti u IoT okruženju identificiraju se putem IP adrese. S porastom objekata, raste i broj IP adresa, a manjak adresnog prostora je pojavom IPv6[12] protokola prestao predstavljati problem.

3. Podaci o objektima, procesima i sustavu: podaci i metapodaci su ono što „pokreće“ IoT. Objekti koji proizvode takve podatke uključuju i procese i sustave koji se smatraju posebnim vrstama objekata.

4. Podaci o lokaciji i okolišu: podaci o lokaciji se prikupljaju s GPS sustava te s pozicija označenih objekata što uključuje satelite, Wi-Fi[13] pristupne točke i mobilne bazne stanice. Kolaboracija njihovih arhitektura omogućava praćenje pomičnih i nepomičnih komponenti.

5. Senzorski podaci: trenutna senzorska tehnologija omogućava prikupljanje velike količine podataka puno brže i s puno većom preciznošću.

6. Povijesni podaci: s prolaskom sve više vremena, podaci se počinju smatrati poviješću. Količina takvih podataka je velika i neophodna za donošenje poslovnih odluka te za poslovno planiranje i iz tog razloga zahtijeva pravilno upravljanje.

7. Fizički modeli: uključuje mikroračunala te napredne mikrobaterije. Karakteristike tih modela su snaga, svjetlost, zvuk i magnetizam, a koriste se u razvoju igara i u računalnom inženjeringu.

8. Podaci za kontrolu: nalaze se u daljinskim uređajima za kontrolu, a omogućavaju korisnicima pokretanje određenih aktivnosti u pametnom domu. Primjerice, korisnik želi, prije dolaska kući, uključiti neki uređaj kako bi si na vrijeme podesio ugodnost doma.

[11] Radio Frequency Identification
[12] Internet protocol version 6
[13] Wireless Fidelity

4.3. Prikupljanje podataka

Uređaji koji imaju mogućnost pristupa različitim izvorima podataka su RFID, GPS[14], NFC[15], pametni telefoni i različiti oblici senzora. RFID uređaji se najviše koriste u zdravstvu, hospitalizaciji i u upravljanju katastrofama. Noviji pametni telefoni opremljeni su senzorima koji imaju mogućnost kreiranja M2M ili V2V[16] mreža za nadzor uvjeta i stanja na cestama. Također, praćenje lokacije uređaja moguće je sve dok se baterija uređaja ne isprazni, čak i bez uključene lokacije samog uređaja. Postoje tri prepreke u postupku prikupljanja podataka koje utječu na kvalitetu i efikasnost uređaja za prikupljanje podataka te na njihovu sigurnost. Prva od tih prepreka predstavlja slijepe točke u IoT uređajima koje uzrokuju smanjenje mogućnosti čitanja podataka u određenim uvjetima. Primjerice, kod RFID tehnologije, tagovi su postavljeni na udaljenosti od 5 do 20 metara od čitača, a ako je udaljenost veća, dolazi do smanjenja signala i nemogućnosti čitanja podataka. [20] Tipovi podataka su tekstualni ili numerički podaci te audio i video zapisi. Bilo kakva promjena u zapisu podatka može dovesti do posljedice da su podaci neupotrebljivi što predstavlja drugu prepreku. Trećom preprekom se smatraju sigurnost i privatnost podataka koji se prenose između IoT uređaja i spremišta podataka, a mogu biti mete napada pa bi se iz tog razloga trebali koristiti od strane autoriziranog osoblja, pohranjeni u autoriziranim serverima i s ograničenom mogučnošću pristupa.

4.4. Administracija podataka

Kao klasičan pristup administraciji IoT podataka koristi se relacijska baza podataka, dokumentno orijentirana baza podataka ili baza znanja s određenim rješenjima. [20] Za analizu velikih repozitorija koriste se procesi koji su opisani u nastavku.

1. Čišćenje: čišćenje podataka je proces koji se koristi za detekciju i uklanjanje pogrešaka i nedosljednosti podataka s ciljem unaprijeđivanja kvalitete podataka. Za IoT je specifično da se podaci u realnom vremenu neprekidno generiraju s velikog broja različitih

[14] Global Positioning System
[15] Near-Field Communication
[16] Vehicle 2 Vehicle

izvora te je stoga potrebno efektivno čišćenje podataka kako bi bila postignuta kvaliteta podataka.

2. Model fleksibilne baze podataka: spremišta podataka u IoT okruženju identificiraju se kao SQL[17] i NoSQL[18]. SQL je programski jezik korišten u relacijskim modelima u kojima su podaci organizirani kao relacije. NoSQL je posebno izgrađena baza podataka za specifične modele podataka i ima fleksibilne rasporede za izgradnju modernih aplikacija, a razlika u odnosu na SQL je u tome što NoSQL ne dijeli podatke u relacije niti se koristi SQL za komunikaciju s bazom podataka.

4.5. Obrada podataka

Ovaj korak zahtijeva mnogo računanja te se za njega koriste različite tehnologije. Sastoji se od nekoliko ključnih tehnika koje pomažu u rukovanju sa sučeljima i interoperabilnošću podataka. Jedna od tih tehnika je upravljanje pristupom, a odnosi se, uglavnom, na zahtijevanje prikupljanja podataka u realnom vremenu za svrhe nadzora ili za uvid u podatke pohranjene unutar sustava. Druga tehnika je agregacija podataka koja se koristi u senzorskim mrežama za bežično usmjeravanje. Ideja ove tehnike je kombiniranje podataka pristiglih iz različitih izvora eliminacijom redundancije i minimizacijom broja transmisija. Smatra se ključnim mehanizmom za emitiranje podataka za strujanje. Glavni zadatak ovog mehanizma jest prikupljanje najkritičnijih podataka s različitih senzora te učiniti te podatke dostupnima s minimalnim kašnjenjem. [21]

4.6. IoT aplikacije

IoT je sve više prihvaćen od strane velikog broja organizacija i ustanova, a jedan od glavnih faktora su aplikacije u IoT okruženju koje su usko vezane uz ljudske dnevne rutine. [20]

[17] Structured Query Language
[18] Not only SQL

1. Zdravstvena njega: sa sve većim pružanjem pažnje ljudi na njihove zdravstvene probleme, IoT postaje sve primjenjiviji u tom području. Jedan od primjera je beskontaktni sustav za nadzor zdravlja koji prati korisničke izraze lica, tjelesne poze i zvukove bez utjecaja na svakodnevni život korisnika. Aplikacija predstavlja koncept detekcije emocija s drugim ljudskim faktorima te na taj način korisnik može biti dijagnosticiran bez tjelesnog kontakta. Na temelju analize trenutnih informacija, moguće je prosuditi treba li korisniku zdravstvena njega. Pristup zdravstvenoj njezi ljudi koji žive u ruralnim područjima može biti otežan. Zdravstveni centar zahtijeva da svaka registrirana osoba nosi jedan aktivni RFID senzor. Bilo koja promjena parametara upozorava pacijenta i doktora koji potom trebaju pristupiti ustanovi kako bi pružili njegu ukoliko je potrebna.

2. Hospitalizacija: u slučaju nužde, vozač kola hitne medicinske pomoći će odabrati rutu vodeći se svojim osobnim iskustvom. U velikim gradovima prometna je zagušenja nekad nemoguće izbjeći. Jedno od predloženih rješenja su ambulantna kola opremljena RFID oznakama koje služe kao prijenosni sustav prikupljanja podataka i kao lokacijski sustav. Prometni uvjeti s bežičnih senzora pozicioniranih na cestama se mogu poslati kontrolnom centru bolnice te se na temelju toga može odrediti optimalni put koji bi pružio najbržu rutu.

3. Logistika: logistički procesi zbog internacionalizacije opskrbnih lanaca postaju sve kompleksniji. [20] Korištenjem IoT tehnologije moguće je savladavanje tih izazova. Jedno od rješenja je upotreba robota za manevriranje pokućstvom. Robot i oznaka su opremljeni RFID oznakom radi sinkronizacije navigacije robota prema objektima. Kako bi se robotima omogućila navigacija prema objektima i manipulacija istima, koristi se radiofrekvencijski kompas razvijen kao sustav na RFID radu. Proces je moguć bez kompleksnog algoritma strojnog učenja.

4. Proizvodnja: za pametnu proizvodnju, također, je usvajanje IoT tehnologije bitan element. Faktori s kojima se mnogi proizvođači susreću su nove sigurnosne direktive, zaštita okoliša, nadzor proizvodnje i odnosi s klijentima itd. Proizvodnja odjeće se suočava s faktorima poput otpada, nedovoljnih količina proizvoda, odnosa s kupcima i poslijeprodajnih usluga. Jedno od rješenja je sustav dizajniran s podrškom *online* kupovine i individualnog odijevanja. RFID oznake se koriste za praćenje svakog koraka proizvodnje. Korisnici imaju uvid u bitne informacije u smislu virtualnog dizajna i praćenja statusa pošiljke.

5. Potencijalni sigurnosni incidenti u IoT okruženju

U zadnjih nekoliko godina razvoj IoT tehnologija je u znatnom porastu. Prema dosadašnjim istraživanjima, s porastom razvoja IoT tehnologije, raste i osviještenost građana o samom IoT okruženju, rizicima, ranjivostima te potencijalnim napadima i incidentima. Pojam koji je usko vezan uz IoT pojam jest pametni dom koji predstavlja mnoštvo uređaja unutar jednog kućanstva koji su međusobno povezani kao što su igraće konzole, monitori za nadzor djeteta, pametni TV prijemnici te bežični nadzorni sustav. Jako veliki broj takvih uređaja se prodaje bez ugrađenih sigurnosnih alata i s operacijskim sustavima koji ne podržavaju instalaciju sigurnosnih softvera. [22] Prosječan broj pametnih uređaja unutar jednog doma u SAD-u u 2018. godini iznosio je 11, a najčešće korišteni uređaji su pametni telefoni (91%), pametni TV prijemnici (73%) te tableti (72%).

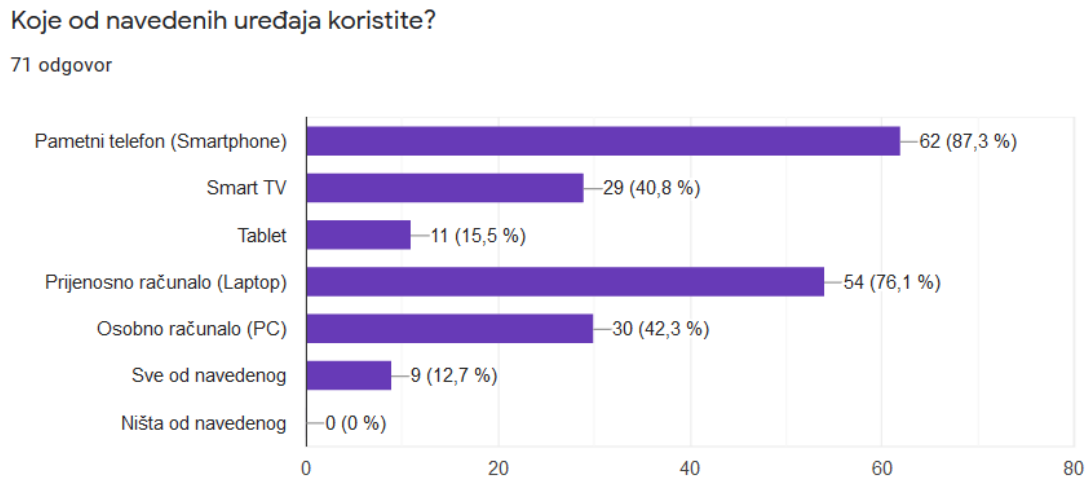
Postoji veliki broj propusta od strane korisnika koji napadačima omogućavaju vrlo laki pristup njihovim pametnim uređajima te samim time i pristup bankovnim informacijama, fotografijama i video zapisima, e-porukama te sigurnosnim postavkama, a najčešće su to loše lozinke, nemarno pretraživanje *web* sadržaja i neadekvatno ažurirana oprema. Također, pristupanjem sumnjivim i malicioznim *web* stranicama, što svakako uključuje i *web* stranice koje nisu podržane od strane HTTPS[19] protokola, korisnici se izlažu *phishing* napadima i prevarama. Prema istraživanjima, samo 50% korisnika redovito ažurira aplikacije na svom pametnom TV prijemniku, dok samo 60% korisnika koristi različite lozinke za sve pametne uređaje. S druge strane, broj korisnika koji koriste samo jednu lozinku za sve uređaje iznosi samo 10% te ih samo 20% ima nekoliko lozinki koje koriste naizmjenično. Promjenu lozinke više od 3 mjeseca nije napravilo 70% korisnika pametnih telefona i tableta, a 50% korisnika pametnog TV prijemnika nikad nije promijenilo lozinku. [22]

S porastom nekriptiranih konekcija i iskorištavanjem ranjivosti, podaci za prijavu često budu izloženi, a posljedica toga jest da osobni podaci više nisu sigurni. Velika količina podataka se svakodnevno objavljuje na društvenim mrežama i svi ti podaci mogu biti zloupotrijebljeni ukoliko nisu sigurni. Prema istraživanjima, 61% korisnika pohranjuje privatne i osjetljive informacije na osobnom ili prijenosnom računalu, dok 68% korisnika u dobi od 18 do 22 godine takve podatke pohranjuju isključivo na svojim telefonima. Kada je riječ o zabrinutosti korisnika

[19] Hyper Text Transfer Protocol Secured

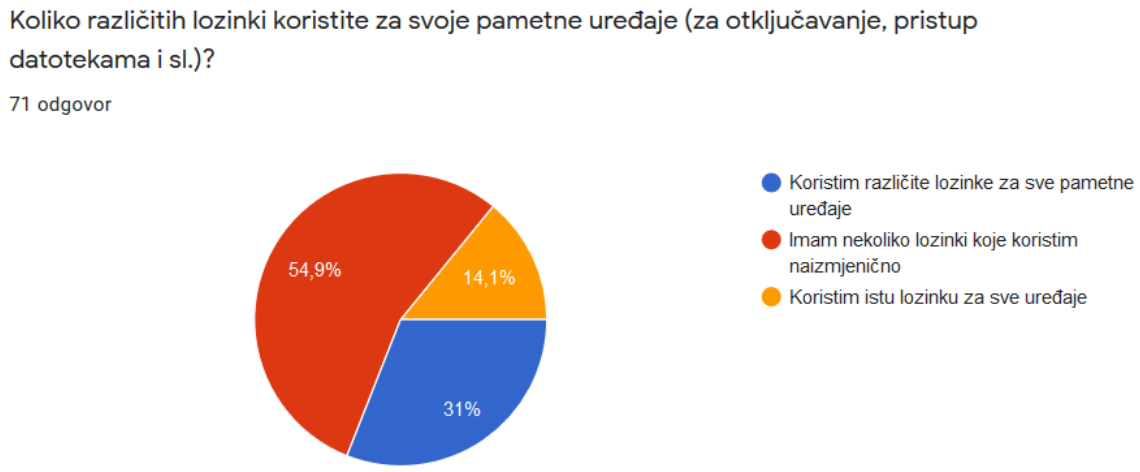
zbog neautoriziranog pristupa informacijama, najviše ih je zabrinuto zbog krađe identiteta, njih 58%, 56% ih je zabrinuto zbog zloupotrebe osjetljivih informacija, a 55% ih je zabrinuto zbog mogućnosti inficiranja uređaja zlonamjernim softverom. Samo 10% korisnika nije zabrinuto ni zbog koje od navedenih mogućnosti, što znači da je osvještenost korisnika 2018. godine bila vrlo niska. Istim istraživanjem htjelo se ustanoviti i u kolikoj količini se koriste slabe i jake lozinke te na kojim uređajima se najčešće nalaze takve lozinke. Tako je ustanovljeno da polovica svih pisača u pametnim domovima ima vrlo slabe lozinke, dok su IP kamere uređaji s najmanje slabih lozinki kojih ima samo 5%. Od sveukupnog broja uređaja unutar jednog pametnog doma, najslabije lozinke su detektirane na pametnim telefonima, pisačima i računalima, a najsnažnije lozinke su detektirane na platformama za izradu prototipova kao što je Arduino, usmjerivačima i kamerama. Najčešće identificirane ranjivosti i izloženosti su DoS napadi i preplavljivanje, a najčešći tipovi napada su nepovjerljive *web* stranice, *phishing* napadi i maliciozni programi. Najranjiviji uređaji unutar IoT okruženja su usmjerivači, računala i pisači, a najmanje ranjivi su pametni TV prijemnici, platforme za izradu prototipova te prijamnici.

U sklopu ovog rada provedena je i anketa kojom se htjelo utvrditi u kolikoj mjeri se danas koriste IoT uređaji te koliko su zapravo korisnici osviješteni o opasnostima i sigurnosnim incidentima s kojima se u istom tom okruženju mogu susresti. Anketa je provedena nad 71 osobom u dobi od 19 do 58 godina.



Slika 11. Prikaz korištenih uređaja

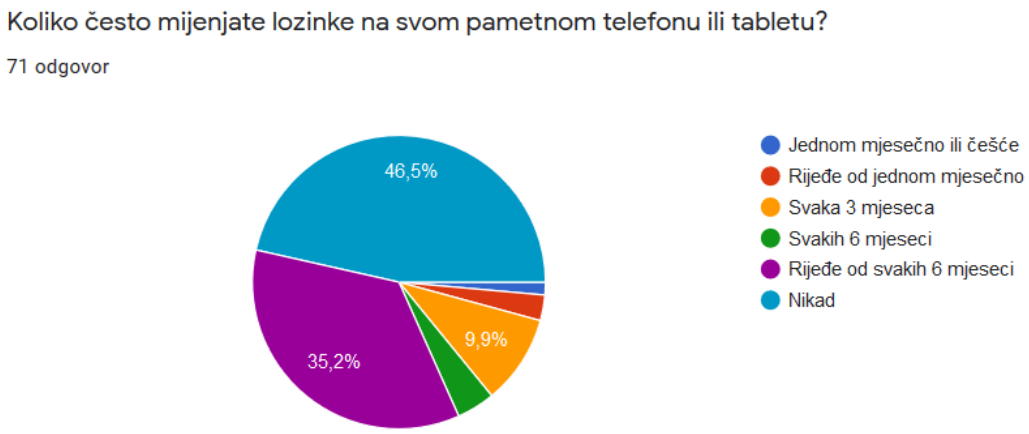
Prema slici 11. vidljivo je da gotovo svi ispitanici koriste pametni telefon, njih 87%, dok ih samo 13% koristi sve od ponuđenih uređaja, a to su, osim pametnog telefona, pametni TV prijemnik, tablet, prijenosno računalo te osobno računalo. Nitko od ispitanika ne koristi nijedan uređaj, a najviše ih koristi, po njih 12, pametni telefon i laptop te pametni telefon, pametni TV prijemnik te prijenosno i osobno računalo. Gotovo 40% ispitanika je odgovorilo da nije upoznato s pojmom Internet stvari kao ni njegovim okruženjem iako su njegovi redoviti korisnici, dok su samo 2 korisnika odgovorila da nisu upoznati s pojmom krađe identiteta. Od polovine ispitanika, koja koristi pametni TV prijemnik, samo 4% njih ažurira softverske aplikacije unutar uređaja nakon više od mjesec dana. Usporedimo li to s istraživanjem iz 2018. godine u SAD-u, razlika je velika jer ih tada 50% nije redovito ažuriralo aplikacije što je otprilike deseterostruko više korisnika. Prema tom podatku se može zaključiti da korisnici redovito ažuriraju aplikacije na pametnim TV prijemnicima što je dobar podatak jer i zastarjele aplikacije mogu biti uzročnici određenih opasnosti.



Slika 12. Prikaz broja korištenih lozinki na pametnim uređajima

Sa slike 12. može se iščitati da 55% korisnika posjeduje određeni broj lozinki koje koriste za svoje pametne uređaje. Prema starom istraživanju, taj broj je bio svega 20% no varijacije su moguće ovisno o lokacijama i navikama korisnika. Samo 30% korisnika koristi različite lozinke za sve uređaje dok je ranije taj broj iznosio 60% što je dvostruko veća razlika. Istu lozinku za sve uređaje koristi otprilike jednak broj korisnika, njih 10%. S obzirom na to da je napadačima puno lakše neovlašteno pristupiti određenim uređajima kada se koristi samo

jedna lozinka, poželjno je da je taj broj što niži, gotovo nepostojeći, što je slučaj u obje situacije, što je pokazano i istraživanjima provedenim 2019. godine od strane kompanije Bitdefender, 2018. godine od strane kompanije Gartner pod nazivom 2018 IoT Security te 2020. godine od strane kompanije IDC pod nazivom European IoT Survey 2020: Vertical Overview.



Slika 13. Prikaz učestalosti promjene lozinke na pametnom telefonu

Pomalo zabrinjavajuć podatak je taj da gotovo polovina ispitanika nikad ne mijenja lozinku na svom pametnom telefonu ili tabletu što je vidljivo i po slici 13., a prema starom istraživanju takvih je korisnika bilo 70%. Prema tom podatku se može zaključiti da je osvještenost korisnika, što se tiče mogućih opasnosti koje vrebaju iza zastarjelih lozinki, u bitnom porastu, ali je ta osvještenost i dalje nedovoljna. Također, ono što je usko povezano s prethodnim podatkom jest činjenica da polovina korisnika pohranjuje osjetljive informacije na svojim pametnim uređajima, što je također vrlo zabrinjavajuće jer su takvi uređaji vrlo ugroženi. Nedostaci kao što su pohranjene osjetljive informacije te istovremeno korištenje jedne lozinke dugi vremenski period napadačima predstavljaju glavnu prednost. Ono što je ovim anketnim upitnikom također ispitano jest koji od sigurnosnih potencijalnih incidenata korisnicima predstavlja najveću prijetnju. 45% ispitanika se odlučilo za krađu identiteta nakon čega, s približno jednakim postotkom, slijede pristup osjetljivim informacijama i inficiranje uređaja zlonamjernim programom. S obzirom na veliki broj ispitanika s neažurnim lozinkama, a s druge strane pak svjesnost mogućnosti krađe identiteta ili podataka, ostaje pitanje iz kojeg razloga ispitanici ne ažuriraju svoje lozinke. Provjereno je i koji od neautoriziranih pristupa unutar pametnog doma bi im predstavljao najveću prijetnju kada je u pitanju njihov osjećaj

sigurnosti te se gotovo 80% korisnika odlučilo za pristup IP kameri. Nakon toga slijede pristup garažnim vratima i monitoru za nadzor djece, a samo jedan ispitanik se odlučio za neovlašteni pristup svjetlima. Navedeno je i vidljivo na slici 14.

Slika 14. Prikaz neovlaštenih pristupa prema razinama opasnosti

Ranjivosti sigurnosnih kamera mogu dozvoliti napadačima daljinski pristup kameri, slušanje audio izlaza te korištenje inficiranog uređaja za DDoS napade. Sigurnosne ranjivosti otkrivene u faks uređajima omogućavaju napadačima krađu podataka kroz mrežu tvrtke korištenjem samo telefonske linije i broja faksa. Napadaći šalju posebno kreirane *malware* datoteke u ciljane mreže. Ranjivosti faks uređaja omogućavaju dekodiranje tih datoteka i postavljanje istih u memoriju što im omogućava pristup osjetljivim informacijama. Ranjivosti pametnih TV prijemnika omogućavaju napadačima akcije koje nisu opasne poput mijenjanja TV kanala ili podešavanja glasnoće te akcije koje predstavljaju opasnost, a to su praćenje kretanja i razgovora putem integriranih kamera i mikrofona. Ranjive su čak i pametne žarulje koje koriste infracrvenu komunikaciju. U tim situacijama napadači šalju naredbe korištenjem infracrvenih nevidljiviih svjetala emitiranih iz žarulja kako bi otkrili ostale povezane IoT uređaje na kućnu mrežu. Pametni aparati za kavu koji su povezani na mrežu putem posebnih aplikacija također mogu biti mete napadačima jer s njih mogu pristupiti podacima s bankovnih kartica. Postoji još veliki broj uređaja koji mogu biti mete napadačima, a samo neki od njih su pisači, pametni zvučnici pa čak i benzinske postaje.

Osim navedenih pametnih terminalnih uređaja, postoje i druga IoT rješenja koja, također, mogu biti ranjiva. Jedan od primjera je pametna električna mreža koja se sastoji od nadzora potrošnje električne energije, pametnih uređaja i obnovljivih izvora energije poput solarnih ploča. Važna komponenta ovakvih rješenja jest instalacija pametnih mjerača koji pružaju dinamičke cijene i dvosmjerni tijek struje između domova i veće mreže. S poboljšanjem, mjerači dobivaju mogućnost mjerenja potrošnje električne energije u najbitnijim vremenskim skalama. Trenutno rješenje, proizvedeno u Kanadi, podržava čitanja mjerača u intervalima od 5 do 60 minuta, dok bi se ti intervali, kod budućih generacija, smanjili na minutu ili manje. [23] Razvoj pametnih mjerača ima velik utjecaj na privatnost korisnika s obzirom na to da nenamjerno čitaju detaljne informacije o aktivnostima unutar doma. Primjerice, ako nije bilo nikakvih događaja tijekom noći koji uključuju potrošnju električne energije barem šest sati, tada se može zaključiti da su svi ukućani spavali ili ako je TV prijemnik bio aktivan na određenom TV kanalu, može se zaključiti koji je TV sadržaj osoba pratila. Takve informacije predstavljaju temelj za dizajniranje određenog analitičkog alata za predviđanje ponašanja, a koje mogu biti zloupotrijebljene od strane određenih tvrtki i kriminalaca.

Prema autorima Molina-Markham A, Shenoy P, Fu K, Cecchet E i Irwin D [23], provedeno je istraživanje o potrošnji električne energije unutar tri doma u periodu od dva mjeseca. Za prikupljanje podataka, korištena je posebna oprema koja je bilježila potrošnju električne energije svaku sekundu. Podaci su se prenosili u kreirani *web* preglednik te su se, pomoću posebnog računala, podaci preuzimali svakih sat vremena i pohranjivali u repozitorij za analizu. Analiza se sastojala od četiri koraka, predprocesiranje potrošnje energije korištenjem algoritma za identifikaciju i označavanje sličnih tipova potrošnje energije, označavanje svake potrošnje energije s jednom ili više karakteristika, filtriranje automatiziranih uređaja promatranjem njihovog ponašanja tijekom perioda niske potrošnje energije te preslikavanje oznaka na događaje iz stvarnog života korištenjem male količine prikupljenih vanjskih podataka. Na kraju, entitet, koji je imao pristup velikoj količini podataka, je klasificirao događaje na temelju prethodnih saznanja. Iz perspektive električnih uređaja, pametni mjerači bi trebali zadovoljavati četiri kriterija:

1. omogućavanje kritičnog vrha naplate i pružanje podrške dinamičkim cijenama,
2. podržavanje alarma za neovlaštenu krađu energije,
3. podržavanje obavijesti o prekidu napajanja i obnavljanju te

4. podržavanje odgovora na zahtjev za automatizaciju kućanstva.

U jedan od načina neautoriziranog pristupa informacijama svakako pripada i socijalni inženjering. Socijalni inženjering predstavlja iskorištavanje ljudskih mana radi postizanja zlonamjernog cilja. Napadači probijaju zaštitu sustava radi pristupa povjerljivim informacijama, a glavne žrtve su im osobe koje imaju puno povjerenja. Napadači takve osobe navode da prekrše sigurnosne protokole te na taj način pristupaju informacijama, a u mnogim slučajevima žrtve budu izmanipulirane kako bi nehotice sami zarazili ili sabotirali sustav. Socijalni inženjering se dijeli u dvije kategorije, a to su *hunting* i *farming*. *Hunting* pristup nastoji izvršiti napad s minimalnom interakcijom s metom. [24] Jednom, kada se postigne zadani cilj i postigne narušavanje sigurnosti, izgledno je da će komunikacija biti prekinuta. Ovo je najčešće korištena metodologija kao podrška *cyber* napadima. *Farming* metodologija se ne koristi često, ali, bez obzira na to, može se koristiti u određenim situacijskim prilikama. Cilj napadača je uspostaviti vezu sa žrtvom kako bi izvukao informacije na dulji vremenski period. Tijekom samog procesa, interakcija se može promijeniti, žrtva može shvatiti da je riječ o prevari te napadač, u tom slučaju, može pokušati podmititi ili ucijeniti žrtvu. Kako bi se postigao zadani cilj, napad se može provesti kroz samo jednu fazu ili kroz čitavi niz operacija. U slučaju kada je riječ o skupini operacija, to uključuje istraživanje, mamac, realizaciju i izlaz. Faza istraživanja uključuje izviđanje, proučavanje i prikupljanje što je moguće više informacija o ljudima i poslovima povezanim s metom napada. U fazi mamca, napadač uspostavlja komunikaciju s potencijalnom žrtvom. Kroz razgovor sa žrtvom gradi razinu povjerenja i preuzima kontrolu interakcije. U fazi realizacije cilj je ostvariti svrhu napada koja može biti izvlačenje informacija ili manipulacija mete kako bi ugrozio sustav svojim postupcima. U zadnjoj fazi, fazi izlaza, napadač finalizira interakciju sa žrtvom nastojeći ne pobuditi nikakve sumnje. Nakon zadnje faze, najčešće je napadača vrlo teško pronaći. Osim navedenih faza, postoji i određeni broj pristupa kojima se napad može realizirati. *Phishing* napadi imaju za cilj pristupiti osobnim prepoznatljivim podacima digitalnim putem, kao što su maliciozne e-poruke koje izgledaju kao da su primljene od strane legitimnih i povjerljivih izvora i *web* stranica. *Phishing* napadi ciljaju velike skupine kako bi se pristupilo što većem broju žrtava. *Baiting* napadi su fizički napadi u kojima napadač postavlja zlonamjerni program u neki oblik medija za pohranu podataka te ga ostavlja na vidljivom mjestu kako bi ga žrtva možda priključila na sustav. Jedan od najnaprednijih napada jest *watering hole* koji zahtijeva visoko tehničko znanje, a predstavlja napad u kojem napadač kompromitira određenu grupu korisnika inficiranjem *web*

stranica za koje napadač zna da ih korisnici posjećuju. Cilj ovog napada je inficiranje korisničkog računala i time ostvarivanje pristupa mreži na radnom mjestu korisnika.

S obzirom na jako veliki broj IoT uređaja koji su povezani međusobno, a samim time i sve veći broj podataka koji su izloženi, zahtjevi za sigurnošću podataka i samih IoT okruženja postaju sve veći. U nastavku će biti ukratko opisani neki od IoT incidenata koji se odnose na narušavanje privatnosti korisnika i krađu podataka, a koji su se dogodili u nekim od vodećih tvrtki svijeta. Jedan od takvih slučajeva pojavio se u Arizoni pod nazivom Facepalm. Korisnik je dodavao prijatelja u grupni razgovor nakon čega je mogao čuti sve njegove razgovore na iPhone-u. Korisnik je slučaj prijavio Apple-u koji je reagirao unutar tjedan dana i pristupio slučaju ozbiljno pustivši nadogradnju softvera te je na taj način uklonio pogrešku. U drugom slučaju, jedan od najpopularnijih Wi-Fi čipseta je bio izložen ranjivosti koja je mogla biti aktivirana bez ikakve korisničke interakcije, a događala se u situacijama kada bi čipset bio povezan s igračim konzolama te s pametnim telefonima. Kasnije je ustanovljeno da je greška bila u *firmware-u* aplikacije te je ubrzo bila uklonjena. *Malware* pod nazivom Silex je narušavao pohranu IoT uređaja, uklanjao mrežnu konfiguraciju, ometao rad vatrozida i zaustavljao uređaj, a raširio se na preko 1500 uređaja. Za oporavak uređaja, vlasnici su morali ručno ponovno instalirati kompletan *firmware* uređaja. Ono što je iznenađujuće je da je napadač imao samo četrnaest godina. Jedan od napada dogodio se putem Bluetooth komunikacije, a uzrokovao je izlaganje uređaja te mogućnost praćenja korisnika i pristupima njihovim osobnim dokumentima što se koristilo za špijuniranje korisnika bez obzira na razinu zaštite operacijskog sustava. Ranjivosti su otkrivene i u pametnim sustavima za zaključavanje kod kojih su napadači daljinski otključavali vrata i ulazili u domove. Od strane proizvođača pametnih brava su puštene zakrpe za preuzimanje. U drugom slučaju, također su postojale ranjivosti u pametnim bravama, ali ovaj put su napadačima omogućavale virtualno otključavanje jer su napadači imali uvid u lokaciju uređaja s kojeg je inače provođeno otključavanje. Pametne igračke su još jedan u nizu incidenata gdje su napadači iskoristili ranjivosti sustava. Nedostajale su određene autentikacije te enkripcije za povezane *online* račune. Glavni povodi su bili napadi na igre i online knjige, praćenje uređaja, slanje poruka djeci te provođenje *man-in-the-middle* napada.

Kako bi se u velikim kompanijama spriječilo probijanje sigurnosnih zaštita i neautorizirani pristupi sustavu potrebno je suočiti se sa slabostima na razini uređaja. [25] Također, potrebno je prilagoditi upute za edukaciju koje se daju zaposlenicima kako bi ih se pravilno educiralo i kako bi im se pružile adekvatne instrukcije o tome kako da izbjegavaju pogreške koje vode do izlaganja podataka. IoT obuhvaća sve veći broj povezanih uređaja, od

sigurnosnih kamera do pametnih termostata. Mnoga poslovanja koriste IoT uređaje na razini poduzeća kako bi radnicima pomogli da što efikasnije obavljaju svoje zadatke ili kako bi se zadovoljile potrebe upravljanja objektima. [25]

Početkom 2020. godine svijet je zahvatila pandemija uzrokovana Covid-19 virusom koja je, kako i na sva ostala područja u svijetu, djelovala i na IoT područje. Veliki broj organizacija bio je prisiljen promijeniti poslovnu politiku na način da se kompletan rad odrađuje na daljinu, iz doma zaposlenika, ne bi li se kontakt među zaposlenicima smanjio. To je za određene zaposlenike počelo predstavljati problem iz razloga što su upoznati isključivo s alatima i onim dijelovima opreme koji su im neophodni za uspješno obavljanje posla. Radom od kuće, na neki se način, smanjuje računalna i Internet sigurnost zbog toga što zaposlenici nisu s njima dovoljno upoznati te oni predstavljaju dodatne potencijalne mete napadačima. Naglim izbijanjem virusa, pojavio se i novi val *cyber* kriminala, a napadači su, uglavnom, motivirani naglim porastom mogućih površina napada prelaskom radne snage na rad od kuće. Osim broja napada, također su se povećali i njihova brzina i razmjeri. [26] Jedan od glavnih problema je taj što kompanije nemaju dovoljan broj računala i opreme te su zaposlenici prisiljeni koristiti osobna računala kako bi pristupili korporativnom Intranetu, a tu se pojavljuju i neke radnje koje zaposlenici ranije nisu obavljali od kuće, kao što su društvene mreže ili *online* kupovina. S obzirom na to da većina tih uređaja ima lošu zaštitu, puno su ranjiviji na *malware* napade.

Neka istraživanja pokazuju da su određene kompanije, za vrijeme pandemije, ostvarile samo 50% prihoda radi „zamrzavanja“ budžeta, dok je 60% kompanija, koje su uvele nove pametne uređaje, navelo kako im je situacija pomogla da postignu prednosti na tržištu. S druge strane, očekuje se da će do 2026. godine vrijednost globalnog IoT tržišta porasti na 1386 milijardi dolara s trenutne vrijednosti od 761 milijarde dolara. Također, prema istraživanju Gartnera, 47% organizacija je investiralo u IoT tehnologiju na bilo koji način.

Prema poduzeću Global Sign [27] dronovi su postali jako korisni za vrijeme pandemije. U Kini je sustav dronova dostavio medicinski pribor u više od 300 individualnih letova. Mnoge države koriste dronove za nadzor i kontrolu javnih mjesta te su također korišteni i za prijenos važnih informacija. Neke od tehnologija postale su veoma bitne za poduzeća, a neke od njih su infrastruktura potrebna za rad na daljinu, alati koji omogućavaju *online* suradnju, sigurnosni softveri i slično. Softver koji je doživio najveći uspjeh za vrijeme pandemije je Zoom, a zabilježeno je da je broj korisnika porastao s 19 milijuna na više od 200 milijuna u samo tri mjeseca. Područje IoT tehnologije koje također bilježi veliki rast su zdravstvene aplikacije. Jedan od primjera dolazi iz Stanforda iz dječje bolnice gdje je zabilježeno 620 telezdravstvenih

konzultacija dnevno, dok je taj broj ranije iznosio samo 20. U Kini se čak koriste i roboti za sanitaciju i dezinfekciju bolnica i za opskrbu lijekovima. Osim robota i dronova, implementirana su i određena rješenja koja pružaju pomoć, a koriste se ovisno o tome je li osoba preboljela bolest ili nije pa se tako mogu podijeliti na ona koja se koriste u fazi dijagnoze, odnosno prije bolesti, u fazi karantene te u fazi oporavka. Neka od tih rješenja su pametni termometri, pametne kacige, pametne naočale te određene aplikacije za pametne telefone kao što su, primjerice, Social Monitoring i Selfie App. Social Monitoring je razvijen u Rusiji od strane vlade za praćenje pacijenata koji boluju od Covid-19 bolesti i moraju biti u samoizolaciji. Pacijenti moraju zatražiti QR[20] kod svaki put kad žele napustitit svoj dom. Selfie App je razvijen u Poljskoj sa sličnom funkcijom kao i Social Monitoring. Integrirana je s geo-lokacijom i tehnologijom za prepoznavanje lica kako bi se pratili pacijenti koji moraju biti u samoizolaciji 14 dana. Pacijenti mogu odbiti instalaciju aplikacije, ali na taj način riskiraju nenajavljene posjete ovlaštenog osoblja. Korištenjem aplikacije, od pacijenta se zahtijeva slanje vlastitih slika, u bilo kojem dijelu dana, kao dokaz o poštivanju mjera.

Još jedno područje IoT tehnologije na koju je pandemija imala utjecaj su pametne zgrade i to na način da je promijenjen način na koji se očekuje da se zgradama upravlja, a to uključuje socijalnu distancu, praćenje zauzetosti, pametno grijanje, ventilacijske i klimatizacijske sustave te strože mjere prilikom održavanja i čišćenja. To je značajno povećalo važnost i potražnju IoT tehnologije u zgradama jer pametne zgrade mogu omogućiti učinkovitije upravljanje objektima i pružiti podršku za sigurno i zdravo okruženje.

Zbog navedenih razloga i problematike glede Covid-19 pandemije, ova je tema postala još i važnija u periodu od zadnjih godinu i pol dana te se može sve više očekivati veliki porast broja korištenih pametnih uređaja koji je i u dosadašnjem periodu zabilježen. Samim će time korisnicima pametnih uređaja prijeći u naviku da koriste više uređaja nego ranije, a očekuje se da će isti taj broj uređaja koristiti i nakon pandemije, iako im neki od njih možda neće ni biti potrebni.

[20] Quick Response kod

6. Usklađenost alata opće uredbe o zaštiti podataka za implementaciju IoTa

Prije pojave Opće uredbe o zaštiti podataka (GDPR) [28] velika količina podataka, osobnih i poslovnih, bila je javna te se njima moglo lako pristupiti. Nastupanjem GDPR uredbe na snagu građanima se, na neki način, vraća nadzor nad njihovim osobnim podacima, a uredba regulira zaštitu podataka i privatnost osoba unutar Europske unije. Prema portalu Sales Seek [29] postojala su tri najvažnija pitanja o samoj uredbi prije njezinog stupanja na snagu, a to su privatna mišljenja i stajališta pojedinaca, utjecaj javno dostupnih informacija na usklađenost uredbe te na koji način se „zaboravljaju“ korisnici koji više nisu aktivni pretplatnici određene usluge, a na neki način moraju biti u evidenciji odjavljenih korisnika. Glavni cilj regulative je zaštita i regulacija privatnosti podataka te se odnosi na bilo koju organizaciju koja obrađuje ili posjeduje podatke o građanima Europske Unije bez obzira na njihovo sjedište. Ovom se Uredbom utvrđuju pravila povezana sa zaštitom pojedinaca u pogledu obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka. [30]

Jedno od glavnih obilježja regulative danas su uređaji IoT okruženja. S velikim brojem senzora koji bilježe svaku informaciju iz okoline o tome tko smo, gdje smo i što radimo, raste i zabrinutost zbog povrede privatnosti i podataka koja je sve više i više vitalna, a senzori postaju potencijalna točka napada za napadače. IoT uređaji djeluju kroz senzore prikupljajući podatke koji se kasnije koriste od strane kompanija za poboljšavanje svojih usluga koje se, nakon toga, nude korisniku zauzvrat. U slučaju povrede privatnosti ili podataka, to može imati značajan utjecaj na živote ljudi ovisno o osjetljivosti samih podataka. Bastos et. al. navode kako je GDPR najvažnija promjena u regulaciji privatnosti podataka u posljednjih dvadeset godina i kako bi se razumjelo samu regulativu, potrebno je biti upoznat s pojmovima osobnih podataka, osjetljivih podataka, anonimnih podataka, procesiranja i povrede podataka. Samo neki od podataka koje prikupljaju senzori su slike, audio i video zapisi, lokacije, temperatura, vlažnost, tlak, akceleracija i otkucaji srca.

Prema članku 4. GDPR regulative, u IoT okruženju nailazi se na mnoštvo izazova. Prvi od tih izazova je pristanak. Taj izazov govori o tome može li se kontrolirati koji podaci se prikupljaju o kome i koji se podaci uopće prikupljaju. (čl. 4., st. 11. „privola“ ispitanika znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose). [28] Kad je riječ o IoT sustavima, tu se nailazi na problem koji se odnosi na

podatke koji se mogu prikupljati o korisnicima, a za koje se korisnici nužno i ne bi složili da se o njima prikupljaju kao što su podaci o kretanju ili podaci o zdravstvenom statusu. Jedno od mogućih rješenja je, da se prilikom svake privole koju su korisnici dužni prihvatiti, točno kategoriziraju skupine podataka koje bi se prikupljale te da im se time donekle omogući da sami odaberu koje su podatke voljni dijeliti, a da se automatizmom prikupljaju samo oni koji su nužni za te svrhe. Trenutni IoT sustavi nastoje pružiti takvu vrstu kontrole, dok se M2M komunikacije baziraju na činjenici da ljudska interakcija nije važna kako bi sustav funkcionirao. Glavni problem predstavlja povećanje neravnoteže snage između podataka i upravitelja podataka, što znači da pojedinac može biti u nemogućnosti pristati ili odbiti procesirane svojih podataka. *Online* usluge obično imaju politiku privatnosti u kojoj se iznosi koji se podaci prikupljaju i u koju svrhu i prihvaćanje te politike je obavezno ukoliko se želi nastaviti s korištenjem usluge. Drugi problem je taj što u IoT okruženju osoba nije uvijek aktivni korisnik te u tom slučaju osoba nije pružila svoju privolu i može biti potpuno nesvjesna da se njezini osobni podaci prikupljaju. Trenutno je jedino rješenje isključivanje senzora što može narušiti rad sustava.

Drugi izazov je princip minimizacije podataka. U okruženju pametnog doma aktivni senzori mogu prikupljati podatke od visoke privatnosti. Implementacijom odgovarajućih tehničkih i organizacijskih mjera zaštite podataka, u svim fazama razvoja pametnih uređaja, sigurnosne mjere i minimizacija podataka imaju značajnu ulogu. Uređaji pametnog doma pružaju benefite kako konzumentima, tako i kompanijama. 2017. godine ukupna tržišna vrijednost tih uređaja iznosila je 84 milijarde dolara, čak 16% više u odnosu na 2016. godinu. [32] Upravitelji podataka smiju koristiti samo one podatke koji su adekvatni, bitni i ograničeni što je nužno u odnosu sa svrhom za koju su procesirani. Također, moraju osigurati da su prikupljeni podaci neophodni za njihovo procesiranje i da se drugi podaci neće prikupljati izvan tog okvira te moraju osigurati da su prikupljeni podaci nužni za dostavu njihovim proizvodima i uslugama. Ograničavanje prikupljanja podataka je nužno za usluge za koje su ti podaci procesirani. Primjerice, audio i video zapisi su prikupljeni u sirovom obliku i jedini način da se ograniči prikupljanje podataka jest njihovo cenzuriranje odmah nakon prikupljanja, a to vodi do idućeg izazova, a to je transparentno procesiranje i pravo na zaborav. Razmotri li se da je korisnik prihvatio politiku privatnosti i da je svjestan koji se podaci prikupljaju, dozvoljava li mu trenutna usluga da vidi kako se podacima rukuje, primjerice, koliko puta dnevno se prikuplja određena informacija, gdje se šalje i kojim putem je tamo poslana. To je veoma važno za GDPR s obzirom na to da se podaci o europskim državljanima trebaju pohranjivati unutar Europske Unije. Alat DSAR (The Data Subject Access Request) omogućava pojedincima da zatraže

pristup podacima koje određena kompanija ima pohranjene o njima. Alatu može pristupiti bilo koja osoba čije osobne podatke određena kompanija procesira. Pri tome pojedinci nisu nužni navoditi razlog pristupa podacima i u bilo kojem trenutku mogu zatražiti kopiju svojih podataka. Pravo na zaborav je europsko pravo pri kojem kompanija mora obrisati sve podatke o pojedincu ukoliko on to zatraži. U IoT okruženju, i transparentno procesiranje i pravo na zaborav, su kompleksniji, počevši s činjenicom da će se podaci vjerojatno prebacivati između uređaja, mnogo više puta nego inače, prije nego stignu do odredišta. Iz tog je razloga kompanijama teško pratiti gdje se nalazi koji dio podatka. Mnoge aktivnosti obrade podataka uključene u rad IoT-a spadaju u materijalni opseg Opće uredbe o zaštiti podataka, s obzirom na to da IoT uređaji teže obrađuju osobne podatke. Zbog toga bi zaštita podataka trebala biti ugrađena u svako IoT rješenje od samog početka i tijekom životnog ciklusa razvoja. [32]

Prijavljivanje povrede podataka je idući od izazova. GDPR kompanijama definira rok od 72 sata (prema čl. 33., st. 1.) za prijavu povrede podataka vlastima nakon što postanu svjesni da je do istih došlo. To se može pokazati prilično izazovnim s obzirom na to da je procjenjivanje veličine i posljedica povrede podataka teško. U IoT okruženju pronalazak i procjena povrede podataka među velikim brojem uređaja postaju još komplesniji i teži. (čl. 4., st. 12. „povreda osobnih podataka“ znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani). [28]

Posljednji od izazova je zadana privatnost i sigurnost podataka (čl. 32., st. 1.). GDPR za upravljače podataka zahtijeva implementaciju efektivnih i dokazivih mjera za garanciju korisničke privatnosti i povjerljivosti. S obzirom na ograničene konfiguracije sustava i hardvera IoT uređaja, razvoj naprednih i efektivnih sigurnosnih mehanizama je težak.

Standard ISO 27001 predstavlja shemu za upravljanje *cyber* sigurnošću u organizacijama i s njegovom implementacijom organizacije imaju sustav za upravljanje informacijskom sigurnošću koji pruža usklađenost s GDPR regulativom. S obzirom na nedostatak uspostavljenih strategija za sigurnost, upravljanje i ažuriranje IoT uređaja, za IoT razvoj, GDPR predstavlja veliki izazov. ISO 27001 omogućava organizacijama upravljanje financijskim informacijama, intelektualnim vlasništvom te podacima o zaposlenicima.

Jedno od područja koja uključuje GDPR je i *blockchain*. *Blockchain* uključuje nekoliko računala koja se nalaze u različitim državama svijeta, a predstavlja repliciranu, odnosno preslikanu, dijeljenu i sinkroniziranu digitalnu strukturu podataka održavane od strane

odgovarajućeg algoritma proširenu na više lokacija, država ili institucija. Digitalno zabilježeni podaci su pohranjeni u paketima zvanim blokovi koji su međusobno povezani kronološkim redom. Tehnički je vrlo teško promijeniti redoslijed blokova. Kako bi bio legalan, GDPR zahtijeva da je upravitelj podacima u skladu prilikom implementacije projekata koji uključuju procesiranje osobnih podataka korisnika, zaposlenika ili trećih strana. Čiji su osobni podaci uključeni, koje će se vrste osobnih podataka procesirati, tko upravlja podacima, jesu li uključene treće strane u procesiranje podacima, koja vrsta *blockchain* tehnologije će se korstiti samo su neka od pitanja koja treba razmotriti prije nego se *blockchain* tehnologija koristi za procesiranje osobnih podataka. [33]

Od velike je važnosti osigurati da je razvoj IoT rješenja u skladu s regulativom. Na temelju toga, moguće je definirati tri seta zahtjeva, a to su potreba za identifikacijom, procjenom i minimizacijom rizika, potreba za izražavanjem volje kompanije za usklađivanje s GDPR regulativom te potreba za demonstracijom GDPR usklađenosti. Prva mjera za smanjivanje pravnih i financijskih rizika je pravilna identifikacija bilo kojih potencijalnih nesukladnosti. Taj je proces moguće izvesti mobilizirajući ured za usklađenost unutar kompanije ili zapošljavanjem eksperata. Potrebno je slijediti određene korake kako bi se smanjili rizici.

1. Prvi korak se sastoji od identifikacije primjenjivih regulacija na temelju lokacije IoT razvoja i procesiranja podataka,

2. Drugi korak ima za cilj identificirati sve one osobne podatke koji mogu biti prikupljeni ili procesirani od strane razvojnog sustava, a to uključuje IP adrese, video strujanja, registarske oznake automobila te geolokacije mobilnih uređaja i vozila,

3. Gdje je moguće, potrebno je pružiti informacije o procesiranju podataka te o kontaktima odgovornih osoba,

4. Preporuča se provedba DPIA metode koja ima za cilj procijeniti potencijalne rizike te bi se trebala izvesti prije prikupljanja bilo koje vrste podataka, a također može služiti i kao dokaz za demonstraciju pouzdanosti upravitelja podacima,

5. Peti korak je analiza sustavskih praznina koja bi se trebala izvoditi od strane treće strane, a služi za identifikaciju potencijalnih nesukladnosti s regulativom za zaštitu podataka,

6. Sve identificirane nesukladnosti bi se trebale sustavno adresirati s aktivnom podrškom menadžmenta i, gdje je moguće, s pravnim i tehničkim ekspertima,

7. Nakon što se otklone sve nesukladnosti, može se razmatrati evaluacija i certifikacija treće strane te

8. Proces provjere usklađenosti bi se trebao redovito provoditi.

Od strane tvrtke Archimede Solutions razvijena je shema certificiranja te za procjenu GDPR usklađenosti pod naivom EuroPrivacy, a temelji se na UPRAAM metodologiji. [34] Ovaj alat je dizajniran za adresiranje svih obaveza regulacije za zaštitu podataka s fokusom na GDPR regulativu. Evaluacijski proces sadrži nekoliko stotina kontrolnih točaka koje se odabiru i primjenjuju ovisno o objektu koji se procjenjuje. Redovito se ažuriraju na temelju prakse i razvoja obaveza kako bi se osigurala sveobuhvatna procjena usklađenosti. Tvrtka također omogućava analizu sustavskih praznina, certificiranje te zaštitu podataka korištenjem DPIA metode.

Jedan od rizika za tvrtke, koje sudjeluju u razvoju IoT usluga, je mogučnost isključivanja s europskog tržišta. Europski upravitelji podacima imaju obavezu odabrati procesore podataka koji su obvezani poštivati GDPR regulativu. Upravitelji podacima moraju osigurati da su svi procesori, locirani izvan Europe, obvezani poštivati GDPR načela prije međusobnog dijeljenja osobnih podataka. Za pružatelje IoT usluga izvan Europe, a koji žele biti aktivni na europskom tržištu, može biti važno da demonstriraju svoju obvezanost poštivanja GDPR regulative. Za te potrebe je razvijen Privacy Pact mehanizam koji im omogućava dobrovoljno i ugovorno obvezivanje prema poštivanju GDPR regulative. Mehanizam je usmjeren na razmjenu podataka između upravitelja podataka i procesora na europskom području s procesorima koji se nalaze izvan Europe. Također, nadjačava set ugovornih standarda izdanih od strane Europske komisije. Alat je implementiran i dostupan kao mrežna ugovorna platforma. Platforma objavljuje popis organizacija koje su elektronički potpisale ugovor s pravnim efektima. To uključuje detalje organizacije kako bi bili vidljivi javnosti i prepoznatljivi za one strane čiji se podaci procesiraju. Digitalnim potpisivanjem ugovora, on postaje važeći u periodu od dvanaest mjeseci nakon čega kompanija može obnoviti ugovor. Također, kompanija u bilo kojem trenutku može povući ugovor koji se potom uklanja s popisa za javnost. Shema certificiranja je dizajnirana na način da na odgovarajući način obuhvaća rastuće tehnologije s naglaskom na IoT tehnologiju, kao i na druge rastuće tehnologije poput velikih podataka ili umjetne inteligencije. Glavne prednosti ove sheme su isplativost, pouzdanost i vjerodostojnost. Shema je dizajnirana tako da obuhvaća nekoliko zadataka, a to su dizajniranje metodologije koja omogućava učinkovitu i visoko pouzdanu evaluaciju GDPR usklađenosti, obuhvaćanje specifičnih rastućih tehnologija povezanih s rizikom, poput IoT

tehnologije i umjetne inteligencije, povećanje pouzdanosti rezultata provođenjem sistematičnijih analiza i smanjivanjem dimenzija evaluacije, razvoj metodologije koja pruža certifikacijsku shemu koja obuhvaća razne regulacije za zaštitu podataka te optimizacija troškova povećanjem učinkovitosti procesa. Od evaluacije se očekuje da se izvodi kroz aktivnu kolaboraciju s upraviteljem podataka, kako bi se efektivno procijenila njihova usklađenost s regulacijama za zaštitu podataka. Evaluacija GDPR usklađenosti zahtijeva duboku, sustavnu i sveobuhvatnu analizu kako bi bila pouzdana i smislena. Važan dio rada je usredotočen na identificiranje i prikupljanje svih relevantnih zakonskih i normativnih obaveza kako bi se osiguralo sveobuhvatno certificiranje o zaštiti podataka. Shema je također osmišljena kako bi se olakšala integracija komplementarnih međunarodnih i nacionalnih propisa. Klijent i certifikacijsko tijelo mogu odlučiti proširiti opseg certificiranja na dodatne zahtjeve za zaštitu podataka. To tvrtkama omogućava izbjegavanje dvostrukih postupaka i troškova certificiranja.

Prema čl. 25., st. 3. GDPR regulativa ističe da se sljedeći zahtjevi mogu dokazati pomoću mehanizama za certificiranje:

1. Usklađenost s načelima privatnosti prema dizajnu i prema zadanim postavkama,

2. Jamstva koja pruža procesor,

3. Usklađenost sa zahtjevima za sigurnost procesiranja te

4. Postojanost odgovarajućih sigurnosti za prijenos osobnih podataka trećim stranama ili međunarodnim organizacijama od upravitelja ili procesora.

7. Zaključak

Internet stvari je još uvijek nepoznanica velikom broju ljudi, bez obzira na njegov sve brži rast i razvoj. Za sami razvoj IoT tehnologija potrebno je zadovoljiti određene norme i standarde za čije potrebe su dizajnirane određene metodologije čijim korištenjem se postiže usklađenost razvoja IoT okruženja s GDPR propisima.

Jako veliki broj uređaja unutar IoT okruženja radi s lošim konfiguracijskim postavkama i s neažuriranim softverima ili lozinkama te takvi uređaji postaju glavne mete za napadače i kroz njih napadači najlakše pristupaju sustavu. Velika količina podataka je pohranjena na takvim uređajima te njihovim kompromitiranjem mogu nastati ozbiljne financijske, materijalne ili druge negativne posljedice za organizacije i kompanije, ali i za pojedince. Napadači, osim u same IoT uređaje, mogu neovlašteno pristupati i u određene sustave pri čemu vrlo često koriste ljude, odnosno, zaposlenike kao glavne mete prema kojima razviju određenu razinu povjerenja i na taj način si olakšaju pristup sustavu.

Puno tipova i izvora podataka je u sklopu IoT tehnologija, a koji se prikupljaju, pohranjuju, obrađuju i administriraju prema određenim propisma i stanardima. Tehnologije koje se koriste u IoT okruženjima, a uvelike pridonose prikupljanju podataka i ugrađuju se u velik broj objekata su RFID, BlueTooth, Wi-Fi pristupne točke i GPS.

Dosadašnja istraživanja pokazuju da je razina ljudske osviještenosti prema opasnostima unutar IoT okruženja i dalje nedovoljno visoka i da se velika količina propusta, napada i sigurnosnih incidenata događa svakodnevno. Očekuje se da će daljnjim porastom razvoja IoT tehnologija te adekvatnim i redovitim edukacijama ljudi rasti i ljudska svijest i pravilno održavanje i rukovanje uređajima i sustavima te da će se smanjivati i broj sigurnosnih ranjivosti i incidenata.

S obzirom na sve veću rasprostranjenost IoT tehnologije, a samim time i veći broj uređaja unutar nje i podataka pohranjenih na njima, nužno je da, prvenstveno, zaposlenici svih vrsta organizacija i korporacija, osobito onih jako velikih, redovito pohađaju edukacijske i seminarske tečajeve o sigurnosnim propisima i protokolima unutar same organizacie kako bi se vanjskim prijetnjama pružila što manja mogućnost neovlaštenog pristupa putem ljudskog faktora. Nužno je da se educira i ostatak ljudske populacije kako bi svoju sigurnost povećali jer bi ona trebala biti na prvom mjestu svakog pojedinca.

Autor ovog djela smatra kako bi se, nakon samog razvoja određenog sigurnosnog sustava, trebala provesti detaljna testiranja od strane profesionalaca ne bi li se uočili bilo kakvi sigurnosni propusti i da bi se tek nakon detaljnog ispitivanja i analize, sustav trebao smatrati adekvatnim i odgovarajućim za primjenu. Također bi se svaki takav sustav trebao redovito ažurirati i održavati te bi se konstanto trebala provoditi testiranja istoga ne bi li se uočile neke nove greške ili propusti, kako bi bio u koraku s rastućom tehnologijom i u mogućnosti obrane od vanjskih prijetnji koje su također rastuće i napredne.

Literatura

[1] Zanni T. Risk or reward: What lurks within your IoT?. Švicarska; 2017.

[2] Ziegler S. Internet of Things Security and Data Protection. Springer; 2019.

[3] IoTOne. Threat Analysis. Preuzeto sa: https://www.iotone.com/term/threat-analysis/t685 [Pristupljeno: veljača 2022.]

[4] Whortwhile. 3 Keys to Managing Data and Maximizing Business Intelligence. Preuzeto sa: https://worthwhile.com/insights/2017/02/20/data-business-intelligence/ [Pristupljeno: veljača 2022.]

[5] EC-Council. Cyber Security Certification Programs. Preuzeto sa: https://blog.eccouncil.org/4-types-of-cyberattacks-that-youre-most-likely-to-face/ [Pristupljeno: veljača 2022.]

[6] Synopsys. Open Web Application Security Project Top 10 (OWASP Top 10). Preuzeto sa: https://www.synopsys.com/glossary/what-is-owasp-top-10.html [Pristupljeno: veljača 2022.]

[7] OneM2M. Benefits of oneM2M. Preuzeto sa: https://www.onem2m.org/using-onem2m/what-is-onem2m [Pristupljeno: veljača 2022.]

[8] GSMA. Internet of Things. Preuzeto sa: https://www.gsma.com/iot/ [Pristupljeno: veljača 2022.]

[9] Palindrome Tech. GSMA IoT Security Assessment. Preuzeto sa: https://www.palindrometech.com/gsma-iot-security-assessment/ [Pristupljeno: veljača 2022.]

[10] Ahmad A, Baldini G, Cousin P, Matheu S N, Skarmeta A, Fourneret E, Legeard B. Large Scale IoT Security Testing, Benchmarking and Certification. Université de Bourgogne Franche-Comté, France; 2020.

[11] Privacy Flag. The Privacy Flag project. Preuzeto sa: https://privacyflag.eu/ [Pristupljeno: veljača 2022.]

[12] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the

Internal Market (“Directive on electronic commerce”), Službeni list Europske unije, L 178. Preuzeto sa: https://eur-lex.europa.eu/ [Pristupljeno: veljača 2022.]
[13] Digital Strategy. Shaping Europe's digital future. Preuzeto sa: https://digital-strategy.ec.europa.eu/en/news/privacy-flag-project-presents-new-tools-and-privacy-certification-scheme-iot-week-2017 [Pristupljeno: veljača 2022.]
[14] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (“Directive on privacy and electronic communications”). Preuzeto sa: https://eur-lex.europa.eu/ [Pristupljeno: veljača 2022.]
[15] Investopedia. Crowdsourcing. Preuzeto sa: https://www.investopedia.com/terms/c/crowdsourcing.asp [Pristupljeno: veljača 2022.]
[16] Outsource Force. What is Crowdsourcing and How Important is it. Preuzeto sa: https://www.outsource-force.com/blog/what-is-crowdsourcing-and-how-important-is-it/ [Pristupljeno: veljača 2022.]
[17] KPMG. How Secure is Your Enterprise. Preuzeto sa: https://home.kpmg/xx/en/home/insights/2017/04/how-secure-is-your-enterprise.html [Pristupljeno: veljača 2022.]
[18] ICO. Data Protection Impact Assessments. Preuzeto sa: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ [Pristupljeno: veljača 2022.]

[19] When is a Data Protection Impact Assessment (DPIA) required?, European Commission. Preuzeto sa: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en [Pristupljeno: veljača 2022.]

[20] Smanchat S, Vongsingthong S. A Review of Data Management in Internet of Things. Bangkok; 2015.

[21] Barcoding. The 5 Types of Data That Power the Internet of Things. Preuzeto sa: https://www.barcoding.com/blog/the-5-types-of-data-that-powers-the-internet-of-things [Pristupljeno: veljača 2022.]

[22] Pascu L. The IoT Threat Landscape and Top Smart Home Vulnerabilities in 2018. Bitdefender; 2015.

[23] Molina-Markham A, Shenoy P, Fu K, Cecchet E, Irwin D. Private Memoirs of a Smart Meter. University of Massachusetts Amherst; 2010.

[24] Hacking the human operating system: The role of social engineering within cybersecurity. Technical report. Intel Security; 2015.

[25] Information Age. Enterprise IoT and Data Breaches: what you need to know. Preuzeto sa: https://www.information-age.com/iot-and-data-breaches-123483531/ [Pristupljeno: veljača 2022.]

[26] Fortinet. Understanding the Impact of COVID-19 on IoT Security. Preuzeto sa: https://www.fortinet.com/blog/industry-trends/understanding-the-impact-of-covid-19-on-iot-security [Pristupljeno: veljača 2022.]

[27] Global Sign. Hands-Free Everything? The Coronavirus Impact on IoT. Preuzeto sa: https://www.globalsign.com/en/blog/hands-free-everything-coronavirus-impact-iot [Pristupljeno: veljača 2022.]

[28] Zakon o provedbi Opće uredbe o zaštiti podataka, NN 42/2018 (805) [Pristupljeno: veljača 2022.]

[29] Sales Seek. 3 Critical Unanswered Questions About GDPR. Preuzeto sa: https://blog.salesseek.com/3-unanswered-gdpr-questions/ [Pristupljeno: veljača 2022.]

[30] EUR-Lex. 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). Preuzeto sa: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 [Pristupljeno: veljača 2022.]

[31] Bastos D, Giubilo F, Shackleton M, El-Moussa F. GDPR Privacy Implications for Internet of Things. London; 2018.

[32] PwC. The Internet of Things: Is it just about GDPR?. Preuzeto sa: https://www.pwc.co.uk/services/risk/technology-data-analytics/data-protection/insights/the-internet-of-things-is-it-just-about-gdpr.html [Pristupljeno: veljača 2022.]

[33] Squire Patton Boggs. Blockchain and GDPR – Many Open Questions to be Addressed and Solved! Preuzeto sa: https://www.securityprivacybytes.com/2017/12/blockchain-and-gdpr-many-open-questions-to-be-addressed-and-solved/ [Pristupljeno: veljača 2022.]

[34] Euro Privacy. Audit and Certification in Data Protection. Preuzeto sa: https://www.europrivacy.org/ [Pristupljeno: veljača 2022.]

Popis slika

Slika 1. Životni ciklus *cyber* napada……5

Slika 2. OWASP IoT područja…….7

Slika 3. oneM2M IoT arhitektura……..…….8

Slika 4. Primjer modela GSM IoT okruženja…….10

Slika 5. Armour sigurnosni okvir……...11

Slika 6. UPRAAM zahtjevi……...12

Slika 7. Shema UPRAAM iterativnog procesa…….14

Slika 8. Evaluacija UPRAAM metodologije…….15

Slika 9. Iterativni proces DPIA metodologije……18

Slika 10. Izvori podataka s pripadajućim aplikacijama…….20

Slika 11. Prikaz korištenih uređaja……26

Slika 12. Prikaz broja korištenih lozinki na pametnim uređajima……....27

Slika 13. Prikaz učestalosti promjene lozinke na pametnom telefonu……28

Slika 14. Prikaz neovlaštenih pristupa prema razinama opasnosti…….29

Popis kratica

IP (Internet Protocol) Internet protokol

DDOS (Distributed Denial of Service) Distribuirano uskraćivanje usluga

USB (Universial Serial Bus) Univerzalna serijska sabirnica

M2M (Machine-to-Machine) Stroj-stroj komunikacija

3G (3rd Generation) Treća generacija mobilnih mreža

4G (4th Generation) Četvrta generacija mobilnih mreža

API (Application Programming Interface) Sučelje aplikacijskog programiranja

XML (Extensible Markup Language) Proširivi jezik označavanja

GIS (Geoinformation Systems) Geoinformacijski sustavi

RFID (Radio Frequency Identification) Identifikacija radio frekvencije

IPv6 (Internet Protocol version 6) Internet protokol verzija 6

WiFi (Wireless Fidelity) Bežična povezivost

GPS (Global Positioning System) Globalni sustav pozicioniranja

NFC (Near Field Communication) Komunikacija u blizini polja

V2V (Vehicle-to-Vehicle) Vozilo-vozilo komunikacija

SQL (Structured Query Language) Strukturirani jezik upita

NoSQL (Not Only SQL) Nije samo SQL

HTTPS (Hyper Text Transfer Protocol Secured) Siguran protokol za prijenos hiperteksta

QR (Quick Response) Brzi odgovor

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 **Zaštita od neovlaštenog prikupljanja osobnih podataka u IoT okruženju** na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 3/2/2022

(potpis)