Kibernetička sigurnost IoT uređaja spojenih na cloud

Balent, Domagoj

SVEUČILIŠTE JOSIPA JURAJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARASTVA I INFORMACIJSKIH TEHNOLOGIJA

STRUČNI STUDIJ ELEKTROENERGETIKE

KIBERNETIČKA SIGURNOST IOT UREĐAJA SPOJENIH NA CLOUD

ZAVRŠNI RAD

DOMAGOJ BALENT

OSIJEK,2020

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac Z1S: Obrazac za imenovanje Povjerenstva za završni ispit na preddiplomskom stručnom studiju

Osijek, 29.09.2020.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za završni ispit na preddiplomskom stručnom studiju

Ime i prezime studenta:	Domagoj Balent
Studij, smjer:	Preddiplomski stručni studij Elektrotehnika, smjer Elektroenergetika
Mat. br. studenta, godina upisa:	A 4424, 20.09.2019.
OIB studenta:	50110981529
Mentor:	Mr.sc. Dražen Dorić
Sumentor:	
Sumentor iz tvrtke:	
Predsjednik Povjerenstva:	Dr. sc. Željko Špoljarić
Član Povjerenstva 1:	Mr.sc. Dražen Dorić
Član Povjerenstva 2:	Dr.sc. Venco Ćorluka
Naslov završnog rada:	Kibernetička sigurnost IoT uređaja spojenih na cloud
Znanstvena grana rada:	**Elektroenergetika (zn. polje elektrotehnika)**
Zadatak završnog rada	Problematika kibernetičke sigurnosti sustava tzv. Interneta stvari (engl. Internet-of-Things - IoT), telemetrijski spojenih na cloud poslužitelje postaje sve aktualnija uslijed trenda promjena poslovnih modela putem tzv. digitalne transformacije. U okviru završnog rada treba prikazati uobičajene IoT arhitekture, telemetrijske tehnologije te cloud poslužiteljska rješenja za prihvat i analizu prikupljenih informacija. Treba se osvrnuti na kibernetičke sigurnosne izazove i probleme s kojima se suočavaju IoT aplikacije.
Prijedlog ocjene pismenog dijela ispita (završnog rada):	Vrlo dobar (4)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 2 razina
Datum prijedloga ocjene mentora:	29.09.2020.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 23.10.2020.

Ime i prezime studenta:	Domagoj Balent
Studij:	Preddiplomski stručni studij Elektrotehnika, smjer Elektroenergetika
Mat. br. studenta, godina upisa:	A 4424, 20.09.2019.
Turnitin podudaranje [%]:	3

Ovom izjavom izjavljujem da je rad pod nazivom**: Kibernetička sigurnost IoT uređaja spojenih na cloud**

izrađen pod vodstvom mentora Mr.sc. Dražen Dorić

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

Sadržaj

1.UVOD……. 1

2.IoT…….. …2

2.1. Upravljanje IoT-a……..... 3

2.1.1. IoT Platforme za upravljanje uređajima…… 5

2.2. IoT arhitekture……... 7

2.2.1. Uređaji(Stvari, senzori i kontroleri)…… 7

2.2.2. IoT Gateways i prikupljanje podataka……... 8

2.2.3. Edge analitika…… 9

2.2.4. Baza podataka/Cloud platforma……. 9

2.3. Industrijska IoT……..9

3.TELEMETRIJSKE TEHNOLOGIJE…….. 11

3.1. Telemetrijske tehnologije u Hrvatskoj……..... 11

4.CLOUD POSLUŽITELJI…….. 13

4.1. Big Data…….. 13

5.KIBERNETIČKA SIGURNOST IoT UREĐAJA SPOJENIH NA CLOUD…… 15

5.1.Tehnike kibernetičkih napada…….. 16

5.1.1. Moderni kibernetički napadi…….. 16

5.2. Zaštita od kibernetičkih napada…….. 17

5.2.1. Cloud zaštita……. 20

ZAKLJUČAK…… 22

LITERATURA……... 23

SAŽETAK……... 25

ABSTRACT…….26

ŽIVOTOPIS…… 27

1. UVOD

IoT predstavlja napredak današnje tehnologije. Ogromna količina informacija se putem njega obrađuje i procesuira, a sve te informacije potrebno je negdje uskladištiti. Skladištenje se može vršiti lokalno ali veću prednost ipak donosi Cloud skladištenje. Stoga sav taj sustav mora raditi u skladu i bez većih poteškoća. Problem koji se javlja kod sustava IoT na Cloudu je sigurnost svih tih podataka. Veliki resursi se ulažu u zaštitu samog toga sustava od kibernetičkih napada.

1.1 Zadatak završnog rada

U ovome radu potrebno je objasniti kibernetičku zaštitu IoT uređaja spojenih na Cloud, načine zaštite, potencijalne prijetnje. Opisati IoT i Cloud kao zasebne sustave te kao cjelinu.

2. IOT

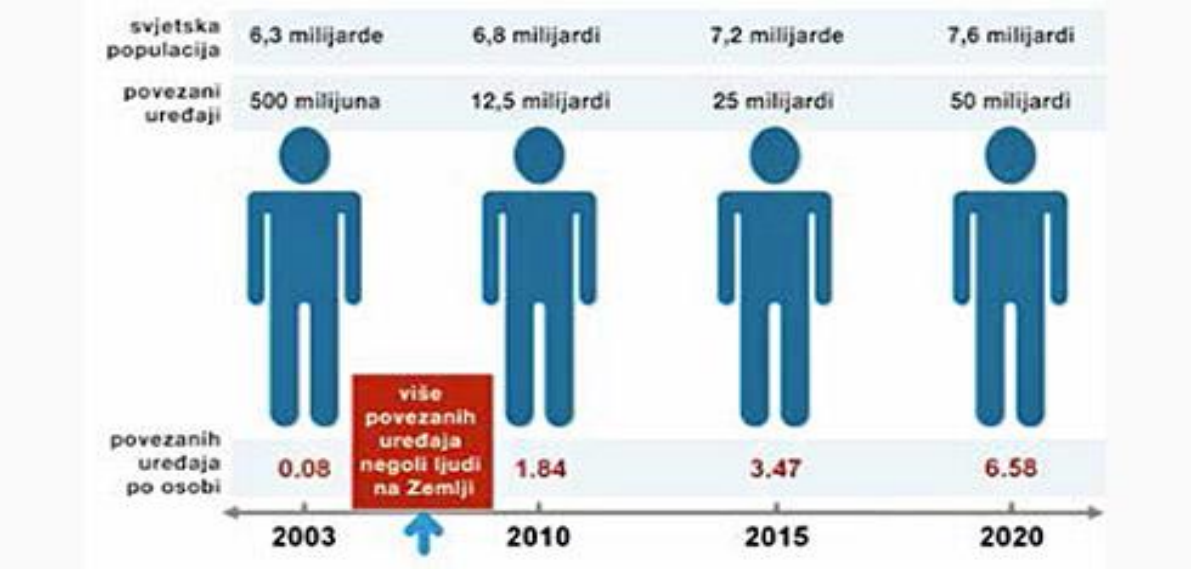
IoT odnosno Internet stvari predstavlja sljedeći logički napredak interneta koji povezuje pametne stvari. Dopušta poboljšanja i inovacije kroz korištenje raznih IoT podataka.. Pametni uređaji, razni senzori, uređaji za pohranu podataka aktivno sudjeluju u komunikaciji, sama komunikacija se vrši između korisnih podataka koje se same stvaraju.

IoT je otvorio nove mogućnosti rješavanja problema koje nisu bile omogućene prije ili su bile omogućene ali na ne isplative načine Stvari kao što su: pristup niskobudžetnoj tehnologiji senzora niske potrošnje, povezanost senzora na Cloudu koja je omogućila lakšu komunikaciju i izmjenu informacija između samih senzora i njihovu bolju povezanost, napredak strojnog učenja i analitike, zajedno sa pristupom raznovrsnim i ogromnim količinama podataka pohranjenih u oblaku kojima tvrtke mogu lakše i brže pristupiti.

Postoje mnoge definicije i objašnjenja što je zapravo Internet stvari ovisi o situacijama gdje se koristi ali u većini slučajeva sadrži spajanje različitih stvari na Internet, mjerenja, pohrana i analiziranje tih istih stvari odnosno informacija te njihova razmjena.

CISCO je još 2017.godine procijenio kako će se ukupan broj uređaja drastično povećati. Od 2017. do 2021 procijenjen je rast od 2,4 puta sa kojeg bi uređaji sa 5,8 milijardi došli do brojke od otprilike 13,7 milijardi uređaja. Ali taj broj je danas još veći. Takav veliki rast uređaja sa sobom donosi mnoge probleme i izazove. Samo neki od njih su upravljanje svim tim uređajima kao i stalna sigurnost uređaja i IoT sustava. Svrha samoga tog upravljanja uređajima je stalno praćenje samih uređaja koji se nalaze u sustavu kao i sustava u cjelini. Takvo stalno praćenje nam dopušta povrat ulaganja u svakom trenutku tih samih uređaja. Svaka dobra i kvalitetna IoT platforma trebala bi pojednostaviti i olakšati napredak IoT sustava uz minimalne ljudske napore i intervencije. [2]

Širok je raspon korištenja samog IoT. U pametnim kućama koriste se za pametnu rasvjetu kao i detektorima dima odnosno plina. Što se tiče prirode i okoline koriste se kod detekcije požara šuma, praćenja vremena, praćenja zagađenja bukom kao i praćenja zagađenja zraka. U industriji također pronalazi široku primjenu jer omogućava, praćenje objekata i automatizaciju procesa, dijagnostiku strojeva. Svoju svrhu pronalazi i u logistiki gdje se koristi kod nadgledanja pošiljki, daljinske dijagnostike vozila te generacija i zakazivanja ruta.



SL.2.1.Demonstracija rasta uređaja u svijetu [1]

Već 2008.godine ukupan broj uređaja premašio je ukupan broj ljudi na zemlji. IoT je već tada predstavljao svoj veliki porast, polako se uvlačio u svakodnevnicu i do danas dostigao velik broj ukupnih uređaja. Taj ogroman rast su uvidjele i velike kompanije kao što su Google, Amazon, Samsung, Apple kao i mnoge druge koje su počele ulagati u same uređaje i sustave IoT-a i time doprinijele rastu i razvoju IoT tehnologije. [2]

2.1. Upravljanje IoT-a

Upravljanje Internetom stvari provodi se u nekoliko koraka. A to su:1.uvođenje uređaja, 2.povezivanje uređaja, 3.nadgledanje uređaja, 4.nadzor i upravljanje rubnim uređajima, 5.upravljanje firmwarom, 6.konfiguracije preko zraka, 7.dijagnostike, 8.sunseting na uređaju. Svaki od ovih dijelova ima svoj zadatak kod upravljanja samog IoT.

Uvođenje uređaja predstavlja jedan od najranijih faza kod upravljanja IoT-a. Cilj ove faze je dovođenje uređaja odnosno implementacija uređaja u nultu konfiguraciju od strane korisnika. Sastoji se od tri ključna dijela: uspostave veze, osiguravanja pohrane te razmjene ključeva kako bi se osigurala sigurnost oba uređaja pri njihovom komuniciranju.

Prilikom povezivanja postoje različite mogućnosti povezivanja uređaja. Kod povezivanja problem je povezivanje starih uređaja s novima. Vrlo je lako napraviti IoT sistem jer su i uređaji i

ulazi proizvedeni od strane istog proizvođača ali problem je proizvesti nove uređaje za postojeće sustave jer je napredak i razvitak samih sustava vrlo brz i mijenja se iz dana u dan.

Nadgledanje uređaja je ključan faktor samog upravljanja IoT-a. Svaki uređaj koji se dodaje IoT-u dio je imovine nekoga pojedinca ili tvrtke. Dodavanje više uređaja doprinosi tome da imamo veću imovinu za sačuvati. Zato treba osigurati da je svaki od pojedinih uređaja u operativnom stanju kako bi osigurali povratak imovine. Kako bi se lakše zaštitio IoT sustav u njega se dodaje stalno nadgledanje uređaja od njegovog povezivanja do praćenja zdravlja samog tog uređaja. Sami proces nadgledanja ne bi trebao trošiti mnogo resursa jer bi time umanjili povrat ulaganja u samom sustavu IoT-a i takav sustav bi u konačnici bio ne isplativ. Različiti uređaji su doveli do toga da imamo različite spojeve i tako je u IoT sustav bilo neophodno uključiti Edge uređaje kako bi se te promjene mogle uskladiti.

Edge uređaji uvedeni su radi različitosti koje nalazimo prilikom spajanja različitih IoT uređaja. Oni su ti koji povezuju same uređaje sa Cloudom. Ali kao i većina dijelova IoT sustava i Edge uređaji također moraju biti stalno nadgledani i upravljani.

Upravljanje firmwarom uređaja odnosi se na upravljanje softvera IoT uređaja i rubnih uređaja. Problemi se javljaju sa pojavom i dodatkom više uređaja u sustav. Svaki od dodanih uređaja može doći sa svojim verzijom firmwara kojeg treba stalno ažurirati i konstantno upravljati njima. S vremena na vrijeme može doći do toga da isti uređaji mogu imati različite hardware iako dolaze od istog proizvođača. Stoga svaki taj uređaj ima različite firmware.

Kako bi smanjili troškove firmwara uvode se konfiguracije preko zraka. Iako se na prvu takva konfiguracija čini prilično jednostavna i laka za uspostaviti sama povezanost uređaja ne mora biti dosljedna pa konfiguracija preko zraka treba bit pažljivo uspostavljena. Ključna stvar je da pravi firmware ili konfiguracija budu dovedeni do pravog senzora jer ako je kriva verzija firmwara postavljena na inkompatibilan hardware može doći do uništenja samog uređaja, a takvi slučaji se ne mogu vratiti.

Upravljanje samim sustavom također zahtjeva postojanje dijagnostičkih programa koji će nadzirati stanja pojedinih uređaja unutar sustava. Stoga svaki IoT sustav trebao bi sadržavati neki od dijagnostičkih programa koji će javljati greške kako bi administrator mogao reagirati na njih i u što kraćem roku otkloniti greške.

Vremenom uređaji unutar sustava zastarijevaju i pojedini dijelovi će morati biti promijenjeni kako bi sustav mogao nastaviti sa radom. U tu svrhu potrebno je imati plan za zamjenu starih uređaja novim bez utjecaja na rad samog sustava.

2.1.1. IoT platforme za upravljanje uređajima

U svijetu postoje mnoge platforme koje pružaju upravljanje uređajima unutar IoT sustava. Neke od njih su: Amazon Web Services, Google Cloud IoT, Microsoft Azure IoT Suite, IBM Watson Suite i mnogi drugi.

Amazon Web Services pokriva velik dio stvari koji su nam potrebni kod upravljanja uređajima unutar IoT. Preko AWS IoT Cora uređaji se mogu povezati na Internet i međusobno razmjenjivati informacije, također omogućava komunikaciju uređaja različitih proizvođača i tipova. Također sadržava svoj upravljački uređaj koji nudi mogućnosti poput: rješavanja problema, praćenja i unaprjeđenja funkcionalnosti uređaja.

Google Cloud IoT sastoji se od mnogo manjih aplikacija koje pomažu u upravljanju samog IoT . Kao i kod Amazona i Google ima svoj Core koji prikuplja uređaje na jedno mjesto i između njih razmjenjuje informacije, sadrži i Pub/Sub aplikaciju koja obrađuje podatke i prikazuje stvarnu analitičku sliku informacija.

Azure IoT Suite sastavljen je od različitih situacija unutar sustava na koje ova platforma različito reagira. Za sad pruža četiri mogućnosti koje se mogu iskoristiti putem platforme. A to su: daljinski nadzor, povezane tvornice, predvidljivo održavanje, simulacije uređaja.

IBM Watson Suite je osmislio naziv za „Internet of Things“ kao Internet koji samostalno misli. IBM platforma podržava: učinkovitu daljinsku kontrolu uređaja, siguran prijenos i pohrana podataka u oblaku, razmjena podataka u stvarnom vremenu, mogućnost strojnog učenja zbog povezanosti sa AL tehnologijom.

SL.2.2. Poznate platforme za upravljanje IoT uređajima [3]

Puno je mogućnosti povezivanja uređaja unutar platformi. Tako razlikujemo žičano povezivanje i povezivanje bez žice odnosno wireless. Wireless povezivanje ima mnoge mogućnosti a neke od njih su Wi-Fi, Bluetooth, ZigBee, Sigfox te stanične veze kao što su: GSM, 3G, LTE, 5G. Također postoje povezivanje sa i bez rubnog uređaja.

Spremanje podataka se može podijeliti na dva načina: Sa SQL ili bez njega. SQL baza podataka se često naziva i „relacijska baza podataka“ dok je se bez SQL naziva „bez relacijska ili distribuirana baza podataka“ . Baze sa SQL imaju predefinirane sheme dok bez SQL ima dinamičku shemu za ne izgrađene podatke. Primjeri SQL baza su: Oracle, Sqlite, Postgres, MySql dok bez SQL baze su: MongoDB, BigTable, Cassandra, Redis. [5]

2.2. IoT Arhitekture

Kada se razmišlja o IoT taj sustav se čini dosta kompleksan i opširan. Stoga je bilo potrebno uvesti neku strukturu da se sav taj kompleksan svijet posložiti kao jedan uređen svijet sa svojim početkom i krajem. Kada se pričalo o IoT puno se pričalo o njegovom potencijalu i kako ga pravilno iskoristiti i od njega napraviti odličnu stvar. Znalo se da se njime može postići mnogo stvari i riješiti probleme koji su do tada postojali. Unatoč svim preprekama i problemima IoT se polako kroz godine razvija i pokazuje svoju iskoristivost. Veliki problem leži u tome što je velika razlika u IoT sustavima koji guše napredak i često stoje na putu do povezivanja svih stvari. Kao jedan od dva problema koja su stajali pred IoT fragmentacija je jedan od razloga zbog raznolike prirode stvari koje se žele povezati. Svaka implementacija IoT potrebna je čvrsta struktura kako bi mogla služiti svojoj zamišljenoj svrsi. Rezultat učinkovitosti i primjenjivosti sustava uvelike ovisi o kvaliteti određene infrastrukture. Tu dolazi arhitektura IoT koja je uspjela sav taj skup informacija i uređaja skupiti u jednu dobro po složenu cjelinu.

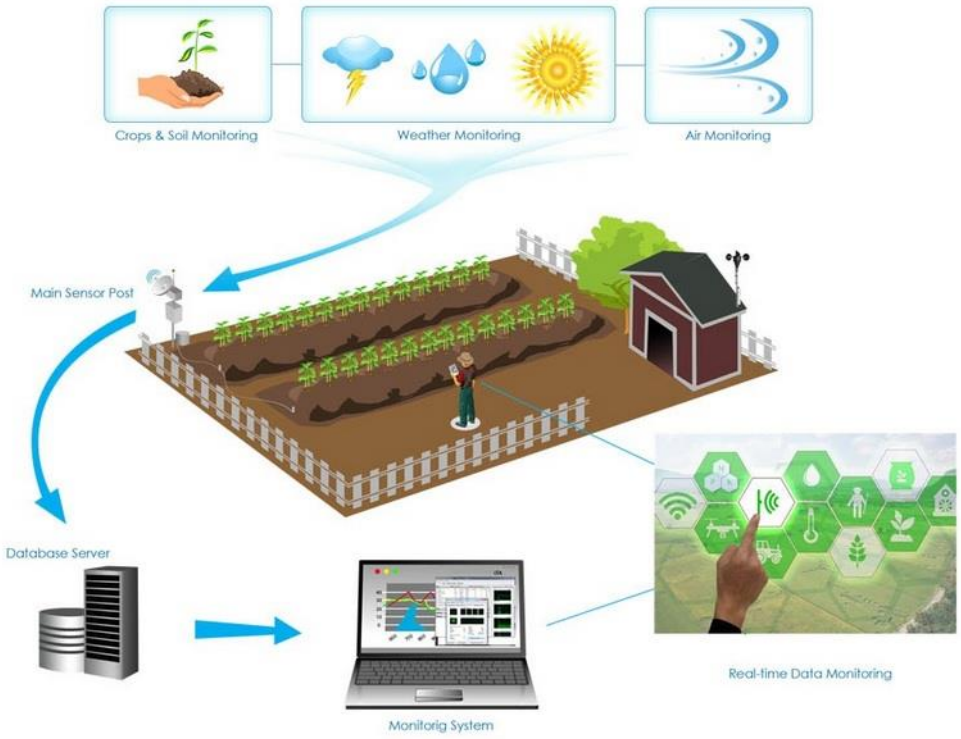
Iako je svaki IoT sustav drugačiji i ovisi koja dva sustava povezuje, temelji svake arhitekture IoT-a je u stvari jednak. Arhitektura se kao prvo sastoji od uređaja koji su spojeni na Internet , a to su senzori i pokretači koji mogu očitavati vrijednosti i podatke iz okoline. Prikupljene informacije tada se predaju IoT gateways. Sljedeća faza se sastoji od IoT sustava za prikupljanje podataka i pristupnika koji skupljaju veliku količinu neobrađenih podataka, oni ih pretvaraju u digitalne tokove, filtriraju i prerađuju tako da budu spremni za analizu. Treća faza sastoji se od edge uređaja koji služe za daljnju obradu podataka i unaprijeđenu analizu svih tih podataka. Nakon toga podatci se sele u baze podataka koje mogu biti ili kao Cloud ili instalirane lokalno. Tu se podatci spremaju, njima se upravlja i analizira njihova djelotvornost. [1]

2.2.1. Uređaji(Stvari, senzori i kontrolori)

Kao temelj svakog IoT sustava, povezani uređaji pružaju uvid u ključni pojam Interneta Stvari a to su informacije. Kako bi prikupili informacije iz okoline potrebni su nam senzori koji će informacije prihvatiti i očitati. Kao primjer možemo uzeti senzor u agrikulturi koji mjeri temperaturu i vlagu zraka, PH vrijednost tla i izlaganje usjeva suncu.

Drugi neizostavan element su pokretači. Oni usko surađuju sa senzorima i mogu pretvoriti informacije koje su prikupili pametni uređaji i pretvoriti ga u fizičku aktivnost. Kao primjer može se uzeti sustav navodnjavanja koji ima sve senzore postavljenje i programirane kako treba. Ovisno o vlažnosti tla senzori mogu pokupiti informacije kada je vlažnost tla niska i dati signal pokretačima za otvaranje ventila za vodu. Kada vlažnost tla poraste i dostigne željenu razinu senzor daje podatke odnosno signal pokretačima da je postignuta dovoljna količina vode i da može

zatvoriti dotok vode. Ono što je također važno je da povezani objekti ne bi trebali biti sposobni samo dvosmjerno komunicirati s njihovim odgovarajućim pristupnicima ili sustavima za prikupljanje podataka, već također biti u stanju prepoznati i razgovarati jedni s drugima kako bi prikupljali i dijelili informacije i surađivali u stvarnom vremenu kako bi se utjecalo na vrijednost cijele implementacije.



2.3. Primjer IoT u poljoprivredi [4]

2.2.2. IoT gateways i prikupljanje podataka

Iako usko surađuju sa senzorima i pokretačima ipak ih se mora odvojiti u posebnu fazu u IoT arhitekturi jer imaju važnu ulogu u prikupljanju podataka, filtriranju prikupljenih informacija i slanja tih podataka Edge uređajima pa kasnije preko njih i do Clouda na kojemu se ti podatci spremaju. Gateways su ti koji služe kao posrednici između povezanih stvari i Clouda i analitike, uz prikupljanje podataka služe kao točka poveznica koja povezuje ostale dijelove sustava.

Gateways olakšavaju komunikaciju između senzora i ostatka sustava pretvarajući podatke senzora koji su lako prenosivi i korisni za ostale komponente sustava. Pristupnici također mogu kontrolirati, upravljati i filtrirati podatke koji dolaze do Clouda, što pozitivno utječe na troškove prijenosa mreže i vrijeme povratka informacija. Još jedna pozitivna stvar pristupnika je sigurnost. Kako oni služe za prijenos informacija iz jednog smjera u drugi, uz pomoć dobro napisanih

programa zaštite lako se može spriječiti curenje informacija iz Clouda kao i smanjiti rizik od vanjskih napada na IoT uređajima.

2.2.3. Edge analitika

Uoči ograničene dostupnosti i brzine prijenosa podataka IoT cloud platformi, Edge sustav može pružiti brže vrijeme odziva i veću fleksibilnost u obradi i analizi IoT podataka. Kod nekih aplikacija brzina analize podataka je ključna u njihovoj izradi. Kod takvih aplikacija Edge analitika je dobila drastični porast u popularnosti među industrijskim ekosistemima IoT-a.

Minimiziranjem izloženosti mreži sigurnost se može značajno poboljšati, dok smanjena potrošnja energije i propusnosti doprinosi učinkovitijem iskorištavanju poslovnih resursa.

2.2.4. Baze podataka/Oblak platforma

Slikoviti prikaz arhitekture IoT opisuje senzore kao neurone, pristupnike kao kralježnicu, a baza podataka je mozak toga cijelog sustava. Baza podataka ili oblak platforma je osmišljena da pohranjuje, procesuira i analizira masivne količine podataka koristeći moćne motore koji čitaju podatke i mehanizme strojnog učenja koje rubni uređaj nikada ne bi mogao podržati. Računalstvo u oblaku doprinosi većim stopama proizvodnje, smanjenju neplaniranog zastoja i potrošnje energije.

Ako je opremljen odgovarajućim rješenjima za korisničke aplikacije, oblak može pružiti poslovne inteligencije i mogućnosti prezentacije koji pomažu ljudima da komunicira sa sustavom, kontrolira ga i nadzire te donosi informirane odluke na temelju izvještaja, nadzorne ploče i podataka pregledanih u stvarnom vremenu.

2.3. Industrijska IoT

IIoT kratica je koja predstavlja industrijski Internet stvari koji se može definirati kao skup ljudi koji uz pomoć softverskih programa upravlja strojevima i uređajima u industriji. Kroz vrijeme razvila se tehnologija komunikacije stroja sa strojem(M2M) odnosno poslovi se vrše uz minimalne napore čovjeka dok poslove obavlja umjetna inteligencija koja razmjenjuje informacije kako bi došli do konačnog proizvoda. Cilj takve komunikacije je smanjenje ljudskih pogrešaka te povećanje korisnosti u samoj proizvodnji kroz smanjenje troškova novca ali i vremena.

U današnje vrijeme kada se IoT pokušava uvesti u industriju takav pomak ito vrijem naziva se 4 industrijska revolucija. Cilj revolucije je u industriju postaviti što više strojeva koji će stalno

biti nadzirani i koji će obrađivati poslove tražene od ljudi uz pomoć IoT-a. Ova revolucija je još uvijek u tijeku i polako se pokušava uvesti u današnju industriju.

Auto industrija je dobila veliki doprinos putem IoT. IoT je omogućio automatizaciju u procesu proizvodnje vozila. Proces se velikim djelom ubrzao, operateri imaju potpuni pregled same proizvodnje i pomoću komunikacije IoT mogu mijenjati proizvodnju ovisno o potrebama. Potencijalne greške su također minimalizirane a i potreban je manji broj ljudi u samoj proizvodnji.

Slika 2.4. Implementacija IoT u auto industriju

3. TELEMETRIJSKE TEHNOLOGIJE

Telemetrija je tehnologija prikupljanja i primanja podataka s udaljenih senzora ili sustava za prikupljanje podataka. S novim telemetrijskim sustavima u obliku uređaja Interneta stvari(IoT) tržište ekspresno raste, a milijarde uređaja se šire po svijetu. Neki od primjera telemetrija u svijetu su: uređaji za praćenje životinja, automobilski senzori za razinu goriva, toplinu motora i brzinu vozila, monitor srca(EKG), nosivi uređaji za praćenje zdravlja. Telemetrija nam nudi mogućnost pristupa podatcima s udaljenih mjesta.

IoT uređaji komuniciraju putem nekoliko mrežnih protokola. IoT uređaji koji se koriste za telemetriju kao što su daljinski senzori imaju sljedeće zahtjeve:1.mala snaga-većina uređaja se napaja iz ugrađene baterije,2.otisak niskog koda-ovo zahtijeva lagane protokole koji ne trebaju velike zahtjeve za računalom,3.malu propusnost-veći prijenos propusne širine zahtjeva veću snagu i dodatne hardverske otiske,4.lokalni inteligentni IoT prolazi-što je sustav bliži IoT uređaju, to je niža snaga potrebna za prijenos.

IoT telemetrijska komunikacija između uređaja i sustava prijema obavlja se s nekoliko protokola. Svaki protokol ima prednosti i mane. Ti protokoli su: MQTT(The Message Queuing Telemetry Transport), CoAP(Constrained Application Protocol), HTTP, HTTPS. [5]

3.1. Telemetrijske tehnologije u Hrvatskoj

1.Sigfox IoTNET-vodeća globalna komunikacijska platforma za IoT uređaje, koja je svoje proizvode plasirala i na hrvatsko tržište. Sigfoxova mreža koji koristi nisko pojasni radio signal koji je kvalitetniji i brži signal od mobilnih mreža. Spojeni uređaji koriste dugotrajne baterije koje traju godinama i postiže veću energetsku učinkovitost. Učinkovitost se također održava i slanjem podataka na precizan i brz način. Time se štedi energija jer se smanjuje energija njihovog stalnog slanja. Sigfoxova tehnologija je primijenjena u raznim životnim situacijama od pametnih gradova, pametne poljoprivrede i pametnog zdravstva pa sve do pametnog turizma, pametne industrije i pametnog mjerenja. Neki od njihovih proizvoda su: HummBox Rain gauge-spojeni senzor pluviometara koji služi za kontinuirano praćenje oborina, ProximaBox koji je zamišljen za bilo koju aplikaciju potrebnu za ljudsku interakciju, a opremljen je i NFC i senzorom temperature, Capturs koji služi kao GPS lokator za ljude koji se bave sportom.

2.NB-IoT(Narrowband Internet of Things)-mreža Interneta stvari tvrtke Hrvatski Telekom. Prednosti nove NB-IoT tehnologije očituju se prije svega u niskim troškovima te jednostavnom komunikacijskom modulu koji omogućuje izravno povezivanje senzora i drugih IoT uređaja na mobilnu mrežu (nije potrebna instalacija i održavanje lokalnih mreža).

Nakon uspješno završenog testiranja NB-IoT mreže u gradu Koprivnici tijekom 2017. godine, NB-IoT mreža je komercijalno dostupna od 2. svibnja 2018.godine. Mreža je bazirana na 3GPP industrijskom standardu koji se koristi u licenciranom spektru. Mrežu odlikuje: odlična prodornost signala u zatvorene prostore, niska potrošnja energije, visoka sigurnost, mala količina podataka, svjetski standard, jednostavnost primjene.

3.LoraWAN-baziran je na oblaku koji upravlja srednjim pristupom , ali djeluje uglavnom kao protokol mrežnog sloja za upravljanje komunikacijom između LPWAN pristupnika i uređaja krajnjih čvorova kao protokol usmjeravanja, koji održava LoRa Alliance.

LoRaWAN definira komunikacijski protokol i arhitekturu sustava za mrežu, dok fizički sloj LoRa omogućuje komunikacijsku vezu dugog dosega Uređaji u mreži su asinkroni i odašilju se kad imaju podatke za slanje. Podaci koji prenose uređaj krajnjeg čvora primaju više gateway-a koji pakete podataka prosljeđuju na centralizirani mrežni poslužitelj. Mrežni poslužitelj filtrira duplicirane pakete, vrši sigurnosne provjere i upravlja mrežom. Podaci se zatim prosljeđuju aplikacijskim poslužiteljima. Tehnologija pokazuje visoku pouzdanost za umjereno opterećenje, no ima nekih poteškoća s performansama koje se odnose na slanje priznanja.

4. CLOUD POSLUŽITELJI

Cloud poslužitelji su moćna fizička ili virtualna infrastruktura koja izvodi pohranu za obradu aplikacija i informacija. Cloud poslužitelji stvoreni su pomoću softvera za virtualizaciju za podjelu fizičkog poslužitelja na više virtualnih poslužitelja. Funkcijama virtualnog poslužitelja može se pristupiti daljinski putem internetskog sučelja. Resursi, aplikacije i informacije koje su dijeljene u cloudu dostupne su i drugim uređajima i računalima preko Interneta. Cloud i Internet su tehnologije koje imaju vrlo različite karakteristike, ali nas okružuju u svakome smislu. Cloud je postao važan faktor kod poslovanja kompanija, analizu podataka i aplikacija dodatno su pomogle razvoju IT tehnologija. Spajanjem ta dva svijeta dobili smo pojam CloudIoT koja predstavlja spoj odnosno integraciju Cloud u IoT. Aplikacijama i podatcima spremljenim na Cloud moguće je pristupiti Internetom, odnosno korištenjem jednog od internetskih poslužitelja.

Cloud infrastruktura se sastoji od skupine servera na kojima se nalaze određeni servisi. Cloud je svojom pojavom donio promjenu u korištenju Interneta ali i pohranjivanja podataka. Glavni poslužitelji Cloud usluge u svijetu su: Google, Microsoft, Saleforce, HP, Amazon. Najveće društvene mreže poput Facebooka i Twittera jednim dijelom se nalaze na Cloudu.

Cloud se sastoji od prednjih i stražnjih slojeva. Prednji sloj je dio koji vidi korisnik i koji se pojavljuje kada korisnik želi priči jednom djelu Clouda. Stražnji sloj se sastoji od hardverskog i softverskog dijela koji se pokreće kad korisnik pristupi sučelju. Cloud je konfiguriran da odgovara za svakog korisnika onako kako on traži, njegova izvedba može biti pomoću rada jednog računala ili više njih ovisno o potrebi korisnika. Također svoju potrošnju i prijenos podataka također prilagođava korisniku ako je prijenos podataka bit će veća potrošnja dok kod manjeg prijenosa će smanjiti potrošnju jer će uvidjeti da prijenos pojedinih podataka nije potreban.

4.1 Big Data

Tehnologija koja prikuplja i analizira velike količine podataka u realnom vremenu naziva se Big Data. Jedna od definicija Big Date je pomoću kratice „3V“. Volume – velika količina podataka koji se prikupljaju, obrađuju i stavljaju na raspolaganje za analizu. Velocity – kontinuirano prikupljanje velike količine podataka u realnom vremenu. Variety – podaci su dostupni u različitim oblicima i izvorima, a zapravo su najčešće nestrukturirani.

Big Data i Internet Stvari su usko povezani jer milijuni uređaja i senzora koji su spojeni na Internet stvaraju i procesuiraju velike količine podataka. Prema procjenama količina podataka koja se stvori udvostruči se svakih dvije godine, neovisno o podatcima Internet Stvari. U svijetu je prema podatcima u 2013.godini bilo proizvedeno 4,4 ZB(zetabajta) podataka, od čega su 2,9ZB stvorili korisnici, a ostalih 1,5ZB su stvorile tvrtke. Procjenjuje se da će u 2020. godini količina

podataka dostići brojku od 50ZB. Većina stvari prikupljena od strane Internet Stvari su maleni skupovi podataka odnosno Small Data, a to su podatci koji sadrže specifična svojstva koja opisuju trenutna stanja. Small Data zna što određena stvar radi dok Big Data zna zašto to radi. Big Data nije nužno potreban u svim situacijama Internet Stvari nekada je potreban samo mali dio podataka tada taj dio obavlja Small Data i tako tvrtke ali i sami korisnici mogu uštedjeti. [7]

SL 4.1.Big Dana [7]

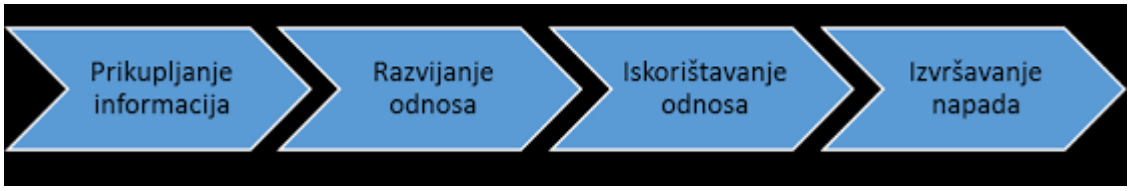
Problem koji se javljaju kod Big Date ali i Internet stvari općenito su sigurnost i privatnost samih tih podataka. Sigurnost je problematična zbog raznolike i široke primjene samih Internet Stvari. Svaki dio Interneta Stvari zahtjeva drugačiji tretman odnosno ima drugačije zahtjeve za brzinom i obradom podataka. Količine podataka koje dolaze od strane Internet Stvari će biti kontinuirane i skokovite pa će velike količine podataka dovesti u pitanje stabilnost infrastrukturu i podatkovni centar. Najbolji način je da tvrtke koje proizvode veliku količinu podataka prebace svoje podatke i tako se dodatno osiguraju svoje podatke.

5.KIBERNETIČKA SIGURNOST IOT UREĐAJA SPOJENIH NA CLOUD

Kibernetička sigurnost predstavlja praksu zaštite sustava, mreža i programa od digitalnih napada. Ti kibernetički napadi obično su sumjereni na pristup, promjenu ili uništavanje osjetljivih podataka informacija koje iznuđuju novac od korisnika ili prekid normalnih poslovnih procesa. Dugo godina unazad ljudi koji su se koristili kibernetičkim napadima često puta kada bi naletjeli na bilo koji sustav zaštite korisnika ili tvrtke, jednostavno bi ga zaobišli i zaključili kako treba naći lakšu metu. U današnje vrijeme to nije slučaj, današnji kibernetički kriminalci su dobro organizirani pojedinci ili organizacije koje su dobro financirane od strane kriminalnih organizacija ili nacionalnih država. Te organizacije su mnogo više strpljive i upornije u ulasku u sustav i krađi podataka određene organizacije ili pojedinca. U današnje vrijeme meta može biti svatko, ciljane su sve vrste organizacija i podataka.

Primjer nekih od kibernetičkih napada: Sony Pictures-u studenom 2014.godine napadači su putem interneta objavili neobjavljene filmove kao i osjetljive informacije o samim zaposlenicima. Kasnije se ispostavilo da su to bili Ruski i Ukrajinski kriminalci koji su doveli do toga da se veliki do filmova morao odgoditi ali je i javno osramotio dio radnika Sony Picturesa. Anthem Blue Cross-u veljači 2015.godine je druga najveća tvrtka za zdravstveno osiguranje u Sjedinjenim Američkim Državama objavila je da su hakeri provalili u njihov sustav i ukrali oko 80 milijuna korisničkih podataka koji su sadržavali osobne podatke ali i brojeve osiguranja. Hakiranje se dogodilo uz pomoć državnog poticaja Kine koja je putem malwara iskoristila slabosti Adobe Flasha i tako naštetiti tvrtki Anthem Blue Cross.

Problem su i ti što su se kibernetički kriminalci razvili u prave profesionalce. Prije su o njima razmišljalo kao o „djeci koja sjede u podrumima“ i izvode probleme poznavajući osjetljivost mreže ali i programski kod. Današnji kriminalci su potaknuti novcem i sponzoriranjem od dobro financijski održivih organizacija ali i samih država. Glavne odlike takvih kriminalaca su: velika količina resursa koje posjeduje za izvođenje napada, ima veću tehničku dubinu i fokus, dobro su financirani i bolje organizirani.



Slika 5.1 Tijek kibernetičkog napada [8]

5.1. Tehnike kibernetičkih napada

Korištenjem naprednog malwara. Malwari su u principu zlonamjerni softveri ili koji obično oštećuje ili onemogućuje, preuzima kontrolu nad ili krade informacije iz računalnog sustava. Malwari uglavnom sadrže adware, bootkits, trojanske konje, crve i mnoge druge. Napredni malware ključna je komponenta ciljanih, sofisticiranih i neprekidnih napada. Korištenjem njega pomoću zaražene točke u sustavu može se doći do krađe podataka za ulazak u za prijavu kako bi se dobio pristup zaštićenom sustavu. U većini slučajeva ovaj malware je ne uočljiv od strane standardnih antivirusnih programa za zaštitu. Oni predstavljaju jednu od najopasnijih opasnosti za organizacije jer zaobilaze zaštitu i ublažavaju ranjivost i slabost ciljane organizacije. Ovaj vid napada najčešće napada tvrtkine najveće i najvrijednije informacije i zbog toga je jedan od najopasnijih vrsta napada.

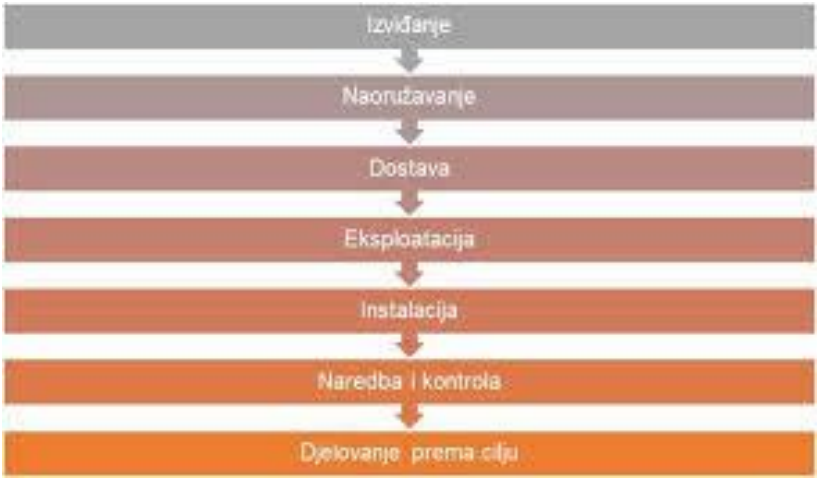
Botovi, DoS i DDoS- botovi predstavljaju individualne zaražene krajnje točke i jedan su od čestih načina napada kibernetičkih kriminalaca. Često se koriste u distribuiranim napadima odbacivanja usluge odnosno DDoS-u. Cilj takvog napada je da se preplavi ciljani poslužitelj ili mreža s prometom velikog broja botova, u takvim napadima botovi sami nisu meta napada. Obično je za takve napade potrebna vojska botova poznatija kao botnetovi. Napadači koristi veliki broj botova kako bi stvorio promet koji preplavljuje mrežne i poslužiteljske objekte cilja. Takvi napadi često ciljaju kompanije iz osobnih ili političkih razloga ili pak zbog iznuđivanja novca

Napredne uporne prijetnje(APTs) je tehnika prijetnje koja koristi kombinaciju malwara i botova kako bi stvorila još opasniji i razarajuće napade. Odlike ovih napada mogu se obrazložiti iz samog imena: Napredna(Advance)- uz sami malware i botnetove napadači razvijaju vještine za razvoj dodatnih alata i tehnika eksploatacije te mogu imati pristup naprednoj tehnologiji elektronički nadzor, satelitsku snimku i ljudskim obavještajnim resursima. Uporni(Persistent)- APT može postojati kroz više godina u sustavu, napadači slijede određene ciljeve i koriste se niskim i sporim pristupom kao bi izbjegli otkrivanje. Prijetnja(Threat)- APT je namjerna i usmjerena te može prouzrokovati ozbiljne štete.

5.1.1. Moderni kibernetički napadi

Pored izravnih napada na poslužitelja i imovinu, današnji napadi razvili su se u strpljive, na više stupnjeva podijeljen i prikriveni postupak koji kombinira eksplotaciju, malware i utaje u koordiranom napadu. Sastoji se od više stupnjeva a oni su:1.Izviđanje- kibernetički kriminalci duže vremena proučavaju cilj svoga napada kako bi uvidjeli moguće propuste u zaštiti ali i sami plan napada na sustav. 2.Oružje i dostava-slijedeći korak je utvrđivanje koje oprema će se koristiti u napadu i kojom metodom će se sami napad izvršiti. 3.Eksplotacija- dvije su moguće opcije

eksplotacije a to su: društveni inženjering koji je vrlo jednostavna tehnika da se netko privuče da klikne lošu vezu ili otvori zlonamjernu datoteku, a druga opcija je softversko ubacivanje koji radi na principu da varaju operativni sistem, Internet preglednik ili neki treći program da pokrene napadački kod. 4.Instalacija-jednom kada je cilj infiltriran, napadač mora osigurati postojanost koda odnosno njegovu otpornost ili održivost. 5.Komanda i kontrola(CnC)- komunikacija je ključni uvjet svakog uspješnog napada. Napadači moraju biti u mogućnosti komunicirati sa zaraženim sustavima kako bi se omogućilo zapovijedanje i kontrola te izvlačili ukradene podatke iz ciljanog sustava ili mreže. Komunikacija mora biti neprimjetna i ne smije izazvati nikakvu sumnju. 6.Radnje na cilju-Napadači imaju mnogo različitih motiva za napad, uključujući krađu podataka, uništavanje kritične infrastrukture. Posljednja faza napada često traje mjesecima ili čak godinama, posebno kad je cilj krađa podataka, jer napadač koristi strategiju slabog i sporog napada kako bi izbjegao otkrivanje. [8]



5.2.Životni ciklus kibernetičkog napada [8]

5.2. Zaštita od kibernetičkih napada

Osnovne stvari koje su tu da se promatraju kao bi se zaštitili od napada: Komunikacija je životna linija koja drži napad, većina napada se izvršava preko sustava kojim se komunicira, ako se komunikacija prekine ili do nje ne može doći napad neće bit uspješan. Pošto se napad odvija u više koraka postoje mnoge mogućnosti kada se može otkriti napad i spriječiti njegovo širenje. Manje je vrijedno što napad radi kad ima kontrolu, bitno je spriječiti da dođe u kontrolu u prvom

redu. Organizacije moraju proširiti svoj krug vidljivosti i prema van organizacije ali i prema unutra kako bi organizacija bila sigurnija.

Tradicionalne metode zaštite imaju jako mali utjecaj kod kibernetičkih napada. Tradicionalni firewalls i IPS rješenja klasificiraju promet, firewall dopušta ili blokira promet, a IPS određuje koji se potpisi trebaju primijeniti, a sve se temelje na luci. Kao rezultat toga, prijetnja koja izbjegava i dinamično, poput naprednog malwara, može jednostavno odskočiti u neočekivani port, dobiti pristup mreži i izbjeći otkrivanje.

Firewalls služe kao prva linija obrane, služi za filtriranje prometa i segmentiranje mreže u različite zone zaštićene lozinkom. Većina firewalls ima problema jer ne mogu imaju male mogućnosti pronalaska i identificiranja malwara. Dodavanjem antimalware mogućnosti na firewall poboljšava se zaštita ali oni pate od slabe točnosti i ozbiljnije degradacije performansi.

Sprječavanje prodora vode ka pravom rješenju jer za razliku od vatrozida ulaze u mrežu i štite ju iznutra od napada malwara. Učinkoviti IPS-ovi koriste kombinaciju potpisa zasnovanih na eksploataciji, koji se mogu brzo proizvesti, ali osiguravaju ograničeno pokrivanje i potpise na temelju ranjivosti, za što je potrebno duže vrijeme, ali osiguravaju pokrivenost širokim rasponom iskorištavanja. U većini slučajeva IPS-ovi pružaju privremenu ili dugoročnu zaštitu ranjivim poslužiteljima.

Proxies su još jedan oblik zaštite praćenjem mreže. Oni pate od problema jer vide samo dio aplikacija ili samo dio mrežnog protokola kojeg treba nadgledati. Punomoćnici trebaju oponašati aplikacije koje prate pa pate s ažuriranjem postojećih i novih aplikacija. Kao rezultat, iako proxy poslužitelji razumiju nekoliko protokola u dubini, obično im nedostaje širina protokolarne podrške potrebne za kontrolu tunela i protokola unutar protokola koje hakeri koriste da sakriju svoj pravi promet.

Zaštita krajnje točke- krajnje točke su često mete napada jer su relativno ranjive zbog ogromne raznolikosti i verzija koje pokreću te stoga mogu pružiti ulaznu točku u mrežu i pristup podatcima koje napadač želi. Naslijeđena zaštita krajnjih točaka, poput antivirusnog softvera utemeljenog na domaćinu, ima iste slabosti kao i ostala naslijeđena tehnologija koja se temelji na potpisu jer mogu otkriti samo poznati već malware- i potpuno su neučinkoviti za otkrivanje novih, modificiranih ili nepoznatih malwara. Uz to, krajnje točke kao što su prijenosna računala i mobilni uređaji često nisu zaštićene zaštitnim zidovima ili IPS-om ako nisu povezani s mrežom organizacije, otvarajući ih za napad kada ih zaposlenici koriste daljinski.

Moderne zaštite od kibernetičkih napada idu u pravome smjeru i vode do nekih pravih rješenja. Jedan od rješenja je postavljanje kontrole same komunikacije unutar zaštićene stvari. Odnosno postavljanje i dopuštanje samo komunikacija koje su potrebne u samom procesu unutar

IoT. Time mi izbacujemo sve nepotrebne komunikacije između određenih komponenti. Problem je što sami hakeri žele svoj napad izvesti tako što će ubaciti program koji će krasti informacije i koji ne će remetiti rad same komunikacije između uređaja. Tu dolazi do nemogućnosti pronalaska rješenja za takve probleme. Testiranja samih nepoznatih informacija i mapa u kojima se nalaze također je jedan od tipova moderne zaštite podataka. Svaka nepotrebna komunikacija treba se zabilježiti i pomno pratiti. Treba postaviti i stalno ažurirati zaštitu jer se napadači iz dana u dan mijenjaju svoj način rada i pronalaze nove načine ulaska u sustav.

Moderna zaštita također se temelji i na različitim vrstama kontrole koje se moraju uzeti u obzir u sigurnosnim politikama organizacije. Svrha samih tih sigurnosnih politika je smanjiti rizik od zaraze odnosno smanjiti prijetnje koje dolaze. Čak i najzaštićenije organizacije moraju biti oprezne i moraju imati na umu da mogu biti komprimirane i moraju biti spremne na takve slučajeve. Stvaranje učinkovitih sigurnosnih politika zahtijeva dobro razumijevanje rizika koje predstavljaju razne aplikacije i značajke koje se koriste u mreži, poslovne potrebe organizacije i radni zahtjevi korisnika. IT(eng. Internet Technology) mora igrati aktivnu ulogu u definiranju pametnih politika koje omogućavaju korisnike organizacije i umanjuju rizik, ali važno je da IT ne bude jedini vlasnik tih pravila - vidljiva podrška izvršne uprave je presudna. Usvajanje novih aplikacija u organizacijama obično započinje od samih korisnika, a ne od pravila.

Upravljanje aplikacijama obično uključuje ograničavanje upotrebe nepotrebnih visoko rizičnih aplikacija uz istodobno upravljanje dopuštenim aplikacijama kako bi se smanjili svojstveni rizici koje mogu sa sobom donijeti. Uspostavljanje učinkovitih politika zahtijeva otvoreni dijalog između korisnika, IT-a i uprave kako bi se istinski razumjelo koje aplikacije imaju legitimnu radnu uporabu i vrijednost. Poznato je da su određene aplikacije kanali za zlonamjerni softver, kako u smislu zaraze, tako i u pogledu trajnog upravljanja. Peer-to-peer aplikacije, poput BitTorrenta, pravi su primjeri takvih aplikacija.

Također na današnjem tržištu postoje aplikacije koje su spoj i dobrog i lošega. Takve aplikacije mogu imati veliku vrijednost samim organizacijama ali i uz to nositi veliki rizik. Kontroliranje trebalo bi biti cilj ovih aplikacija. U ovom slučaju, aplikacije mogu biti dopuštene, ali ograničene na dopuštanje samo potrebnih značajki uz blokiranje značajki s većim rizikom .Primjer toga je organizacija može omogućiti aplikaciju za web sastanke, ali ne dopustiti mogućnost udaljene radne površine koja daljinskom napadaču može omogućiti da preuzme kontrolu nad strojem.

Dokumentirane politike zaposlenika i obuka krajnjeg korisnika moraju biti ključni dijelovi za kontrolu aplikacija, ali kontrole zaposlenika kao samostalni mehanizam nedovoljne su za sigurno omogućavanje novih i novih aplikacija. Uz politike i obuku, IT trebaju alati i sposobnost

praćenja i upravljanja tim aplikacijama. Na primjer, kako bi spriječili korisnike da prenose privatne podatke o kupcima ili osjetljive podatke, umjesto da takve odluke prepusti korisniku.

Kada uzmemo u obzir da se moderniji kibernetički napadi većinom vrše na mrežu, mreža postaje jedna od kritičnih točaka za zaštitu. Segmentaciju mreže treba implementirati firewalls, na granicama različitih korisničkih ili podatkovnih podjela, kako bi se osiguralo da se promet može pregledati dok prolazi različitim segmentima mreže. S uspostavljenim politikama za omogućavanje aplikacija, IT može preusmjeriti pozornost na pregled sadržaja dopuštenog prometa. Ova inspekcija često uključuje traženje poznatog zlonamjernog softvera, obrasce upravljanja i upravljanja, eksploatacije i opasne ili rizične vrste datoteka. Kad god je to moguće, politike koje se usredotočuju na sadržaj prometa trebaju se koordinirati kao dio jedinstvene objedinjene politike, gdje se pravila mogu vidjeti. Ako se politike sadržaja šire kroz više rješenja, modula ili monitora, sastavljanje koordinirane logičke politike provođenja postaje sve teže za IT sigurnosno osoblje. Također će biti teško razumjeti rade li ove politike nakon što se provedu.

Izgradnja dosljednosti u arhitekturi mreže zahtijeva pažljivo planiranje i nužna je za svaku sigurnosnu politiku kako bi se riješila stvarnost suvremenog računanja. Slično tome, sigurnosne politike moraju se baviti upotrebom krajnjih uređaja koji nisu standardna oprema koju izdaje organizacija. Korisnici koji rade kod kuće mogu koristiti vlastita osobna računala za koja je sve veća vjerojatnost da koriste Apple OS X kao i za Windows. Ostali uređaji koji se koriste za daljinsko povezivanje s mrežama organizacije uključuju pametne telefone, tablete i iOS uređaje, kao što su iPhone i iPad. Svi ovi uređaji moraju se također adresirati kako bi se spriječile mrtve točke u sigurnosnim politikama organizacije. [9]

5.2.1.Cloud zaštita

Kako raste i kako napreduju tehnologije Cloud poslužitelja tako dolazimo i do potrebe za napredovanjem zaštite istih tih Cloud poslužitelja. Raspoređena zaštita tradicionalnih odnosno naslijeđenih zaštita nema pregled čak 60% ukupnog mrežnog prometa. Time napadači i njihovi malwari mogu se kretati bočno bez opasnosti od otkrivanja. Pošto u svijetu postoji vrlo malo čistunaca, koriste se hibridne metoda Cloud okruženja koje kombiniraju ono najbolje ali i najgore od javnog i privatnog Cloud okruženja. Stoga sigurnosna rješenja se moraju primjenjivati i na javni i privatni sektor Cloud okruženja kako bi se osigurala sveobuhvatna zaštita sustava i podataka.

Samim povećanjem Clouda kod njegovog korištenja došlo je i do povećanja sigurnosti samog Clouda. U većini se slučajeva postavlja pitanje dali je Cloud siguran za korištenje. Odgovor može biti vrlo složen. U stvari, mnogi pružatelji usluga u oblaku sjajno rade integrirajući sigurnost

u Cloudu infrastrukturu i čineći je sigurnijom od mnogih drugih organizacija. Međutim, nije svaki pružatelj usluga u oblaku ovakav, pa mora biti oprezan pri pregledu sigurnosnog položaja davatelja usluga u oblaku. Sigurnost u računalstvu u oblaku ovisi i o korisnicima. Nepridržavanje ispravnih sigurnosnih standarda i pravovremeno rješavanje sigurnosnih rizika može dovesti do kibernetičkog napada ili kršenja podataka koji se inače može spriječiti. To zahtijeva da tvrtke učinkovito razumiju i ublaže sigurnosne rizike u oblaku. Većina sigurnosnih problema u oblaku usredotočena je na podatke i pristup jer većina modela podijeljene odgovornosti u uslugama računalstva u Cloudu ta dva aspekta u potpunosti prepušta kupcima. Kao rezultat toga, napadači su usmjerili svoj fokus na ovu potencijalnu sigurnosnu ranjivost. Nekoliko je izazova povezanih sa sigurnošću u Cloudu. Najčešći problemi za sigurnost računalstva u Cloudu uključuju: identificiranje i održavanje potrebnih sigurnosnih kontrola, balansiranje zajedničke odgovornosti održavanja sigurnosti između davatelja usluga u Cloudu i korisnika, pridržavanje regulatornih zahtjeva za zaštitu podataka u Cloud okruženju. Sigurnost u Cloudu prilično je dinamična, uglavnom ovisno o tome koliko dobro krajnji korisnik razumije i rješava sigurnosne rizike i ranjivosti računalstva u Cloudu. Srećom, sigurnosni rizici u Cloudu mogu se u velikoj mjeri ublažiti slijeđenjem najboljih praksi u Cloudu. [9]

SL.5.3.Cloud serveri [6]

6. ZAKLJUČAK

Ovim završnim radom opisan je IoT sustav kroz njegovu arhitekturu, mogućnosti te podsustave od kojih se sastoji. IoT je jedan složeni sustav koji kreće od senzora koji na sebe primaju informacije te te tražene informacije šalju gatewayu koji te informacje sortira u dobre za sustav ili ih odbacuje ako nisu potrebne. Tada prelazi na Edge uređaj koji je ključni podsustav između informacija i njihovog mjesta za skladištenje odnosno Clouda. Sav taj sustav je pronašao svoju svrhu u raznim industrijama poput automobilske i farmaceutske te u medicini putem EKG uređaja i mnogih drugih bez kojih današnji život ne bi bio isti. Predstavljene su platforme za upravljanje informacija poput Google Cloud IoT koji ima mogućnost obrade velikog broja informacija i njihove analitike. Te Amazon Web Service koji je pokriva razmjenu informacija između uređaja raznih proizvođača i time olakšalo njihovo međusobno povezivanje. Telemetrijske tehnologije koje su zastupljene u Republici Hrvatskoj koje su omogućile dijeljenje i razmjenu informacija između udaljenih uređaja poput Sigfox IoTNET, LoraWan, NB-IoT koji rade na principima slanja više gatewaya u primarni centar za obradu podataka. Dolazi se i do Cloud poslužitelji su moćna fizička ili virtualna infrastruktura koja izvodi pohranu za obradu aplikacija i informacija te je dostupna svima koji imaju pristup putem interneta. Spoj IoT tehnologije te skladištenje na Cloud primamilo je napadače na krađu informacija i njihovu ucjenu u razmjenu za novac ili druge interese. Neki od najvećih napada koji su zadesili svijet su se dogodili 2014. godine kada su ruski hakeri ukrali preko 1.2 milijarde šifri korisnika na preko 450000 stranica, te hakerski napad na Yahoo iste te godine u kojemu su bile komprimirane informacije od 500 milijuna korisnika. Time je došlo do potrebe razvijanja obrane od samih kibernetičkih napadača. Komunikacija je ključ svakog napada ako se ona prekine napad neće moći biti izvršen u potpunosti. Početne kibernetičke zaštite sastojale su se od zaštite pojedinačnih dijelova mreže odnosno filtriranja informacija putem firewalla koji je dijelio informacije na dobre i opasne. Takvi oblici zaštite kasnije su izgubili smisao jer su napadači razvili tehnike za ulazak u sam sustav putem „dobronamjernih informacija“. Moderne zaštite služe se zaštitom početne i krajnje točke sustav konstantnim praćenjem svakog uređaja zasebno ali i sustava u cjelini. Bitna stvar je konstantan napredak zaštite odnosno razmišljanje unaprijed kako bi uvijek bili korak ispred napadača. Sustav IoT sa Cloudom dopušta nam razmjenu informacija i mogućnosti koje su nam pomogle u različitim situacijama života .Donijele su napretke u svim poljima od industrije do medicine ,ali i sa sobom donijele probleme očuvanja tih informacija. Kibernetička zaštita je u velikom razvitku i to je pozitivna stvar za IoT u globalu.

LITERATURA

[1]Chapter01-Overview of Internet-of-Things

[2] DIREKTIVA (EU) 2016/1148 EUROPSKOG PARLAMENTA I VIJEĆA.,19.7.2016

[3] B. Cannadey, THE FUNDAMENTAL IoT ARCHITECTURE, Losant ,21.8.2019

[4],A. Grieznevich, IoT architecture: building blocks and how they work, ScienceSoft, 1.4.2018

[5], R. Keith, What is IOT Telemetry, A10, 27.03.2019

[6]IBM Cloud Education, Cloud Servers, IBM Cloud, https://www.ibm.com/cloud/learn/cloud-server, (19.04.2019)

[7] L. Stepinac, Što je to zapravo Big Data i gdje se primjenjuje?,12.05.2014

[8]Lawrence C. Miller, Cybersecurity for dummies, John Wiles & Sons ,Inc., Hoboken, New Jersey

[9] Raef Meeuwisse, Cybersecurity for Beginners, Cyber Simplicity Ltd, 14.03.2017

Korištene kratice

IoT-Internet of things

GSM-Global System for Mobile Communication

3G-Treća generacija

LTE-Long term evolution

5G-Peta generacija

SQL-Structured Query Language

PH-potentia hydrogeni

NB-NarrowBand

NFC-Near-field communication

EKG-Elektrokardiogram

MQTT- The Message Queuing Telemetry Transport

CoAP-Constrained Application Protocol

HTTP- Hyper Text Transfer Protocol

HTTPS- HyperText Transfer Protocol Secure

GPS-Global positioning system

DDoS-distrubted deniel of service

APT-Advance persistent threats

IT-Internet Technology

SAŽETAK

U ovome završnom radu opisan je sustav Internet stvari, njegova arhitektura te mogućnosti njegovog upravljanja. Predstavljeni su neki od mnogih Cloud poslužitelja s kojim Internet stvari može doći u kontakt. Predstavljene su telemetrijske tehnologije koje se mogu naći u Republici Hrvatskoj za primanje i obradu podataka. Upoznati smo s Big Datom kao jednim od najvećih i najbržih tehnologija za obradu i filtriranje podataka u realnome vremenu. Objašnjene su metode kibernetičkih napada poput DDoS-a, Dos-a, napada malwara te objašnjene neke od zaštite kojima se brani od mogućih kibernetičkih napada. Po fazama je objašnjen tijek kibernetičkog napada i njihova dugotrajnost.

Ključne riječi: IoT(Internet stvari), Cloud, Big Data, kibernetički napadi, kibernetička zaštita, malwari

ABSTRACT

Title: Cybersecurity of IoT devices connected to the Cloud

This final work describes the Internet of Things system, its architecture and the possibilities of its management. Presented are some of the many Cloud servers with which the Internet of Things can come into contact. Telemetry technologies that can be found in the Republic of Croatia for receiving and processing data are presented. We are familiar with Big Data as one of the largest and fastest technologies for real-time data processing and filtering. Methods of cyber attacks such as DDoS, Dos, malware attacks are explained, and some of the protections used to defend against possible cyber attacks are explained. The course of the cyber attack and their duration are explained in stages

Key words: Internet of things, Cloud, Big Data, Cybernetic attacks, Cybersecurity, malwars

ŽIVOTOPIS

Domagoj Balent rođen je 22.04.1999. u Našicama, a stanuje u selu Beničanci nedaleko od Našica. Osnovnu školu završava u Osnovnoj školi „Matija Gubec“ Magadenovac s odličnim uspjehom.2013. u Našicama upisuje opću gimnaziju „Isidora Kršnjavog“ Našice koju završava 2017.godine, s vrlo dobrim uspjehom.

2017.godine upisuje preddiplomski stručni studij elektrotehnike, smjer elektroenergetika na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija Osijek.

Slobodno vrijeme provodi igrajući nogomet i sudjelujući u Dobrovoljnom Vatrogasnom Društvu. Sudjelovao na natjecanjima iz prometa u osnovnoj školi na kojima dospijeva do županijskih natjecanja dvije godine za redom, ali bez većih uspjeha

Dobro poznaje engleski jezik ali ima znanja i u njemačkom jeziku